# Internet of Mobile Things: Reliability and Security Issues and Solutions

**Ghadah Aldabbagh[1,2], Nikos Dimitriou[3], Samar Alkhuraiji[1], Omaimah Bamasak[1,2], Samar Babrouk[1]**

[*]Corresponding author E-mail address: galdabbagh@kau.edu.sa

[1]Computer Science Department, Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia. galdabbagh@kau.edu.sa
{galdabbagh, salkhuraiji obamasek, Sbabrouk}@kau.edu.sa

[2] Department of Mechanical Engineering, Massachusetts Institute of Technology,
Cambridge, MA 02139-4307, USA
{ghadah, obamasag}@mit.edu

[3]Institute of Informatics and Telecommunications, NCSR "Demokritos", 15341 Athens, Greece.
nikodim@iit.demokritos.gr

**Abstract**
The paper will focus on the reliability and security challenges in mobile IoT network architectures and will highlight their effects in related vehicular use cases. It will then present representative solutions based on secure routing, blockchain trust management and secure edge cloud processing, along with their tradeoffs.

***Keywords:***
*IoT, security, reliability, routing, blockchain, edge processing*

## I. Introduction

Internet of Things (IoT) involves the combined use and interaction of various sensors and actuators for collecting sensing information from the physical world and for directing appropriate decisions based on processing outcomes of this information and on various requirements and constraints posed by the respective applications. New and emerging IoT applications drive the development of Wireless Mobile Sensor Networks; this requires the consideration of new complex network topologies involving heterogeneous IoT nodes with various sensing, networking, and processing capabilities, enabling them to create ad-hoc mesh formations and to perform information storage and processing in a localized and distributed manner, allowing also autonomous operation and decision making. Various research problems are related to the operation of such a heterogeneous IoT networks. They include the study and design of reliable communication protocols that will allow efficient and safe information flow among the heterogeneous IoT nodes, considering the network topology dynamics and the possible threats that may compromise the safe operation of the network. energy efficient nodes that will sense, transport and process heterogeneous and multimodal information and measurements; each sensor node should have a secure and reliable path (either single-hop or multi-hop) for transmitting the sensed information to a respective receiver node. This involves the evolution of the study of different categories of techniques such as ad-hoc network path establishment/routing, congestion control, self-healing, etc. having also security in mind.

The development of Internet of Things technologies and standards (e.g. NB-IoT, LoRaWAN, IEEE 802.11p/bd, LTE-M, IEEE 802.15.4) addresses the need for integrating cyber-physical networks of interconnected devices and for enabling their interaction via Internet in order to enhance their capabilities and optimize their performance and make them thus suitable for introducing novel services in areas such as environment protection, weather forecasting, industrial automation, autonomic vehicles, precision agriculture, smart cities etc.

One basic challenge for IoT is related to the secure integration of heterogeneous devices (sensors and/or actuators) to perform actions on the physical world based on information/measurements related to the environment (that is collected by sensors), using appropriate applications for processing the sensed information and for considering related constraints and requirements. The deployment scenarios of WSNs involve the use of a large number of deployed sensors within the observation area to gather a high spatial granularity of measurements that could be then centrally processed and thus provide advanced situation awareness. The high number of sensors ensures also

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.90

knowledge extraction reliability even in cases that some sensors are disabled, by using self-healing properties of the WSN communication network. Another important feature that could enhance the capabilities of a WSN is related to the introduction of clusters of mobile-vehicular sensors (i.e. on board of manned or unmanned vehicles - UxVs) for enhanced information collection of specific areas according to triggers and alarms set off by the measurements of the fixed WSN infrastructure. To do that, the heterogeneous WSN will have to employ different network connectivity topologies (e.g. star, mesh) and radio access network interfaces) that will allow the required connectivity of all sensor nodes and the optimum transport of the sensing information (that may range from low rate measurements to high rate real time video) from the remote nodes (fixed or airborne) towards the information processing entities of the WSN.

IoT systems are based on collecting and processing information as well as on generating specific actuation commands. This collection, exchange and flow of information and commands has to be done in a reliable manner in order to meet the specifications and requirements of the applications and of the infrastructures that utilize them, which in some cases involve considerable long-term capital investments such as smart buildings, factories, hospital, power plants and distribution networks, etc. In most cases the IoT networks need to have self organizing capabilities in order to reconfigure themselves against failure events and malfunctions or in order to adapt the information collection and sensing parameters according to updated application specifications. Reliability is a key requirement for the operation of such complex networks; it includes the following properties [1]: (a) Self-configuration and ability to withstand changing environmental conditions, (b) Long-term usability, (c) Application robustness in the face of uncertain information and (d) Resistance to security problems. In order to achieve the reliable operation of an end-end IoT system and of the supporting applications, it is important to break down the possible issues that may arise in different parts of the end-end connection, or of the information transport/storage and processing subsystems and functionalities, in order to assess the reliability threats and to design efficient countermeasures. These threats may be either caused by occasional malfunctioning of parts of the system or software or may be related to the malicious operation of outside users that aim at compromising the IoT system's operation and gathered information. Therefore, the objective is to identify solutions that will ensure the IoT network operation reliability resilience and cyber-security. The paper will examine representative techniques and will present their trade-offs in terms of efficiency, overhead and complexity. The paper is organized as follows: Section II provides the analysis of the concepts related to IoT privacy, resilience and cybersecurity. Section III then identifies the main issues and challenges that are related to cybersecurity threats in different points of an IoT system architecture. Following that, in Section IV the paper focuses on specific security threats related to Vehicular Networks and mobile IoT use cases, whereas section V provides representative solutions related to three different categories, namely secure routing, blockchain trust management and secure edge cloud processing and discusses their tradeoffs. Finally, section VI concludes the paper.

## II. IoT Privacy, Resilience and Cybersecurity concepts

***IoT Privacy:*** Privacy concerns the information related to sensed data, location, and node identity. IoT systems enable the generation and exchange of large volumes of privacy-sensitive data which makes them attractive targets of various attacks that may exploit the data for user profiling, behavior recording and user surveillance. Such attacks can involve the following [2]: (a) DNS or device fingerprinting to identify specific devices from the monitored network traffic and (b) inference of user activities and behavior based on changes in (even encrypted) device traffic rates.

***IoT Resilience:*** Resilience can be interpreted as the capability of a system to respond to external disturbances without experiencing regression or internal perturbations. The key objective of resilience mechanisms is robustness against external attacks, using proactive measures for prevention and effective reactive schemes to recover from any potential damages that may have happened due to the attacks [3]. Resilient IoT frameworks must have increased degree of context and situation awareness in order to effectively monitor all parts of the IoT ecosystem (nodes, networks) for any externally induced malfunctions and misbehaviors. In this context, trust management is also important for ensuring the validity of shared and collected information from different parts of an IoT network. Thus, resilience is closely related to the social dimension of IoT networks, that has been highlighted as one of the most important enablers for IoT evolution [4]. Cyber attacks effectively target the reputation and established trust within an IoT network infrastructure in order to cause instabilities and perturbations and to thus compromise the network's operation.

***IoT Cybersecurity:*** Cybersecurity involves all security and privacy features that can be implemented (by design) in any system of connected things, involving decision making intelligence. According to [5], the main cybersecurity threats are the following: (i) Nefarious activity/abuse (e.g. malware, involving malware, exploit kits, DDoS), (ii) Eavesdropping/Interception/hijacking (e.g. 'man in the middle' attacks, session hijacking, network reconnaissance), (iii) Outages (e.g. intentional network or device interruptions or failures), (iv) IT Damage/Loss (e.g. leakage of sensitive information), (v) Failures/malfunctions (e.g. software vulnerabilities, weak passwords, elements' misconfiguration), (vi) Disaster (e.g. equipment failures due to environment or natural disasters), (vii) Physical attacks (e.g. device modification or destruction due to intentional tampering or sabotage). According to the same report, the most critical attack scenarios are the following: (i) Against the administrative IoT systems, (ii) Against sensors, by falsifying their readings and other threshold settings , (iii) Against devices, by directing false commands to them, (iv) Against the communication links among devices and controllers, (v) Against the information flows within the IoT network, (vi) Against actuators, by falsifying their settings, (vii) Exploiting protocol vulnerabilities, (viii) By sequentially compromising multiple mutually interconnected nodes (Stepping stones attacks), and (ix) Power source compromise and manipulation.

Even though there have been numerous efforts to develop common cybersecurity standards, there are still considerable open security issues related to the operation of cyber-physical systems and IoT, due to the continuous evolution of application scenarios that widen the scope of IoT domains and promote the development of networks with increased complexity and distributed autonomy [6].

## III. Identification of main issues & challenges

Reliability and security threats can be considered to target the following IoT network requirements [7]: (i) Data Confidentiality, that is related the data packets interception, examination and corruption by unauthorized parties/nodes, (ii) Data Integrity, that has to do with the undetected modification of the circulated or stored information by malicious third parties and (iii) Availability, which involves all the cases of devices functioning in a ways different from the predefined ones (e.g. nodes malfunctioning, disabled, compromised, exploited by malicious third parties).

Also, such threats can be taxonomized according to the actual IoT architectural layer to which they belong. The following figure depicts the classification of main IoT reliability and security issues into different IoT architectural layers.

.

.

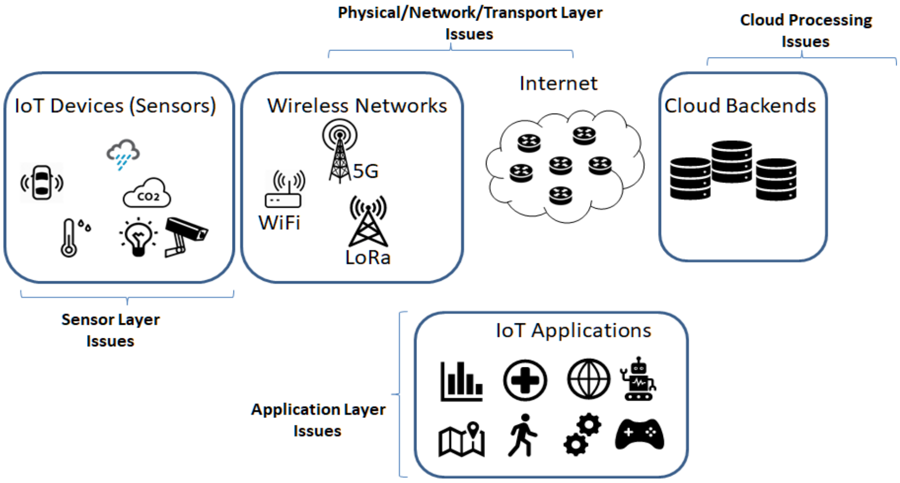

**Figure 1:** Mapping of reliability and security issues on IoT architecture

***Sensor/ Perception Layer:*** IoT and Cyberphysical systems depend heavily on information collected from sensors. Therefore, these systems are vulnerable to spoofing attacks that inject fabricated stimuli to the sensors that cannot be detected, affecting the sensor outputs and the whole system operation.

***Physical Layer:*** The physical layer incorporates all the mechanisms and protocols for the collection, framing and transmission of the sensed information via proper wireless or wireline signals between the sensors and information collection nodes. These signals are vulnerable to malicious interception, jamming or even forgery. Also, Denial of Service Attacks can be performed exploiting the wireless interface between the sensors and the IoT network gateways.

***MAC Layer:*** Typical threats in the MAC layer are related to 'Man in The Middle' (MITM) spoofing the address resolution protocol (ARP) at the MAC layer and linking an attacker's MAC address to an IoT device's legitimate IP address. This is done via ARP poisoning which uses the fact that each ARP request-response is considered to be trusted and also that network clients can always accept server responses, without distinguishing whether they are legitimate or malicious.

***Network Layer:*** In the network layer a common security threat is IP Spoofing in which attackers forge the source IP addresses in IP packets (using legitimate IP addresses of IoT nodes) to perform Distributed Denial of Service (DDoS) attacks. These attacks may be twofold; they are related either to forming clusters of compromised IoT devices (botnets) to generate massive IP traffic floods towards specific target servers or to generate fake requests on behalf of a target and trigger huge amounts of server responses, or to isolate parts of the network by not forwarding incoming traffic (blackhole attacks). In all cases such attacks aim at causing servers' downtime, network saturation and outage.

Also, in the network layer wormhole attacks may be performed, that involve two malicious nodes intruding in an IoT network and setting up a tunnel for re-routing the ordinary traffic generated among the legitimate IoT nodes

***Transport Layer***: In the transport layer, TCP is used for ensuring packet transmission reliability and congestion control. It has a mechanism for ensuring error detection of the transmitted data but does not have any security provisions to prevent unauthorized data reception or 'Man in The Middle' attacks. Security can be provided by Secure Sockets Layer SSL and Transport Layer Security TLS protocols, that introduce cryptographic mechanisms, message authentication, key generation, and cipher suites. Traditional 'Air Gap' isolation of SCADA and WSN networks is diminishing or even not possible in current and emerging networks of interconnected objects. There are also many cases of cyber threats in 'air gapped' systems in which attackers may use various means to access remote devises via removable storage media, compromised personal devices or embedded sensors.

***Application Layer:*** Message Queue Telemetry Transport (MQTT) relies on TCP and is unencrypted (in the absence of TLS) is vulnerable to Man-In-The-Middle attacks, DDoS attacks and buffer overflow attacks. Also, messages in MQTT are formed using clear text, therefore may include sensitive information and credentials such as usernames and passwords [8]. Also, another threat is related to application 'privilege escalation'; IoT platforms may be compromised to grant to IoT applications excessive access rights to devices and to the messages those devices generate, that may result in attackers gaining control of remote devices and exploiting target IoT networks for performing other attacks such as botnets, DDoS, etc.

***Big Data and Cloud processing:*** The Cloud is part of the IoT architecture and usually supports the remote control of the IoT nodes, handling also some resource consuming tasks on their behalf. Attackers may compromise the Cloud authentication system and may get access to IoT control functionalities, taking over the management of the IoT devices and orchestrating various malicious operations, related to either exploiting the collected information or to using the underlying networks for DDoS attacks [8].

## IV. Threats related to Vehicular Networks and mobile IoT use cases

This section will present how the aforementioned issues can affect real-time mobile IoT use cases and applications, focusing on smart transportation and vehicular networks. In general, cyber attacks target specific parts of an IoT network. They can try to affect an end node in order to take over its functionalities, download its stored data and information, intercept its network authentication credentials and even affect its actuation commands. They can also try to use an effected node in order to perform similar actions in other neighboring network end nodes or even to gain access towards centralized access points or gateways, for gaining control of the whole network or for compromising the data that are stored and processed in edge or remote cloud facilities.

In smart transportation use cases, the attacker may attempt to block the physical link connection between vehicles and Road Side Units (RSUs) by causing excessive interference on their respective wireless control channels. Additionally, the attacker may exploit vulnerabilities at the link and network layer to intervene between two communicating nodes (either vehicles or a vehicle and an RSU) in order to obtain real time vehicular awareness information (e.g. motion and on-board sensor data) and also to take over a vehicle's Controller Area Network (CAN) that regulates critical driving functionalities such as engine control, the braking system, the throttle regulation and the steering wheel manipulation, as well as vehicular environment and comfort settings, as for example the air-conditioning system [9]. As the developing trend is to move from level 0 - where the vehicles will just have embedded automated systems for generating warnings, performing brief interventions (e.g., emergency braking)- towards level 5 robotic vehicles where steering wheel will be optional, one crucial factor will be the degree of the actual resilience of the developed systems in cases of security and privacy attacks. Existing protocols such as IEEE 802.11p and 3GPP C-V2X have to address various threats related to availability, integrity and confidentiality. Indicatively, IEEE 802.11p is susceptible to flooding attacks that may affect the CSMA/CA exponential backoff scheme. LTE-V2X can also be affected by a flooding attack by malicious nodes impersonating legitimate LTE nodes. Additionally, both standards cannot prevent jamming attacks or coalition attacks that affect mainly victim nodes close to the edge of coverage. Also, in the case of both standards various broadcast messages and network information are transmitted without encryption for reducing transmission and processing latency (e.g., time-critical safety information, vehicle location and mobility status information), thus it is feasible for an eavesdropping attacker to access this information and target specific network nodes and resources. Device-Device links are more sensitive to the attacks, due to the absence of authentication control from the base station [11].

## V. Description of candidate solutions and related tradeoffs

In order to address the challenges of the aforementioned IoT reliability and security threats, various solutions have been proposed in literature. These solutions can be taxonomized in the following categories:

**Secure Communication and Routing:** The wireless medium allows for performing various attacks to IoT nodes. By adding security layers on the peer-peer and multi-hop communication among the IoT nodes, such vulnerabilities may be addressed, at the cost of increased overhead. Emphasis is given on enhanced cryptography features for user authentication and secure routing also considering path diversity. The architecture assumed by secure routing protocols should involve additional modules performing authentication, encryption, key management and neighbor node trust monitoring. These modules, as show in **Figure 2**, should have an efficient interplay with ordinary routing and forwarding protocols for efficiently securing proactive or reactive routing tables and for assisting in the detection of possible security vulnerabilities and events. Specific nodes may be chosen to perform additional security monitoring tasks according to their resource constraints and mobility patterns [12], to assist in securing the whole network that may consist of nodes with variable energy, storage, computation, mobility, and communication capabilities. Routing procedures rely heavily on the integrity and accuracy of the distributed routing tables that are used by each network node to forward incoming packets towards the appropriate neighboring node. Any malicious nodes that may intervene in the network and advertise incorrect routes may impact the network performance and also the route maintenance mechanisms. Such routing attacks may not be efficiently addressed by protocols running on the link layer (hop-by-hop such as IEEE 802.15.4 link layer security) or on higher -than the network- layers (end-end such as CoAP's DTLS protocol). One method for adding security in routing is to force network nodes joining a network to first authenticate, that may add overhead, considering a large IoT network size. Another security feature may involve the inference of trust metrics for each network node, either based on information exchange among neighboring nodes or with the assistance of third party nodes or even nodes assuming the task of a cluster head, which again involve additional computation and signaling requirements, that have impact on the network scalability, throughput and energy performance [13]. Key issues that need to be addressed are related to the adaptation of authentication, encryption, key generation and management on IoT protocols running on resource-constrained devices employing light protocols matching their application features (e.g. 6LowPAN frame header compression and fragmentation).

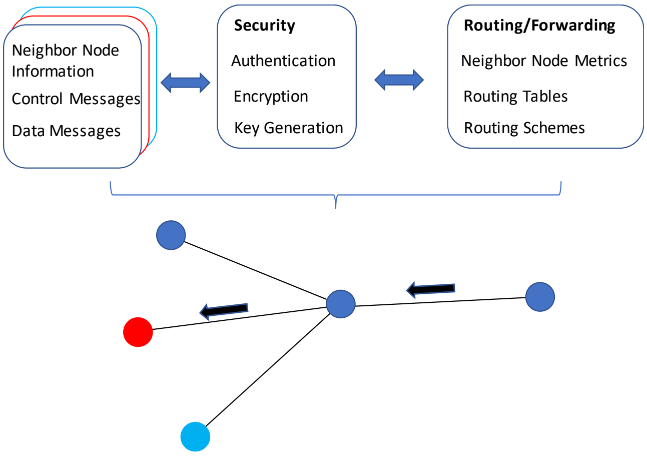

**Figure 2: Adding security on top of forwarding/routing functionalities**

**Trust Management**: This is related to the establishment of suitable mechanisms with which all nodes within an IoT network will be validated in order to securely share security features (e.g. cryptographic keys), transmit and receive sensed information elements and actuation commands. This is also related to collective consensus and decision mechanisms as promoted by Blockchain Technologies.

Centralized IoT security solutions are not considered to be capable of addressing the requirements posed by various cybersecurity attacks and by the increasing diversity within heterogeneous IoT networks. In centralized IoT cloud-based systems IoT devices must be identified, authenticated, and connected via cloud servers, therefore all related signaling must be performed via Internet, even if it is related to proximal nodes. This may increase substantially the IoT network rollout cost, may also lead to cases of single points of failure and may as well allow for malicious system manipulation [14]. In contrast, Blockchains can ensure identity security (e.g. addressing identity theft, the cases of rogue public key certificates and man-in-the-middle threats), data security (e.g. addressing unauthorized access of data via access control schemes) and communication security (e.g. by shielding domain name system services and countering attacks such as DDoS) [15].

Blockchains have been under increased interest and research over the past years as means for providing data integrity and decentralized trust in various transactional sectors. They are based on block lists that are cryptographically linked and contain information about the transaction data, block ownership and certification. These lists are distributed among all network nodes (on a peer-peer fashion) and thus are considered as distributed ledgers or databases, whose validity and resilience is based on the consensus of the majority of the participating nodes. Thus, it is very difficult for blockchains to become altered, compromised or modified from malicious parties and therefore they are considered suitable solutions for securely storing, accessing and transferring data. Blockchains involve a series of procedures for establishing peer-peer connectivity, consensus schemes, validation mechanisms that require specific levels of overhead and therefore affect the overall system complexity and computation requirements. Therefore, the actual implementation parameters of Blockchain protocols (e.g. their focus range within a network, their operation on subsets of nodes, the enforcement of consensus algorithms) depend on the actual IoT application requirements and on the specific computation and communication capabilities of the respective IoT nodes.

In [16] the authors propose the use of public Blockchains that store and manage the event messages' sequence and the trust indicators of the vehicles in a reliable and indisputable way. Specific Location Certificates, which play the role of Proofs of Location, are provided to vehicles by legitimate RSUs using corresponding public and private key pairs. Thus, by using the blockchain, all vehicles within an area can verify the trustworthiness of their neighboring peers and can exchange securely their respective messages, with controlled overhead sizes and blockchain growth scalability. Also, assuming that vehicular nodes create individual blocks and exchange them with their neighbors when they are within the same coverage range, as shown in **Figure 3**, it is very challenging to ensure that the blockchain can be maintained due to the topology dynamicity and the intermittent connectivity due to node mobility. The work investigated the stability that can be achieved in vehicular blockchains and identified that it depends on the actual CSMA contention window size (e.g. for based IEEE 802.11p or IEEE 802.11bd), on the coverage range of each node and on the node speeds, that all determine the effectiveness of node connectivity and of the exchange rate of blocks for validation and for including them in the common widespread blockchain.

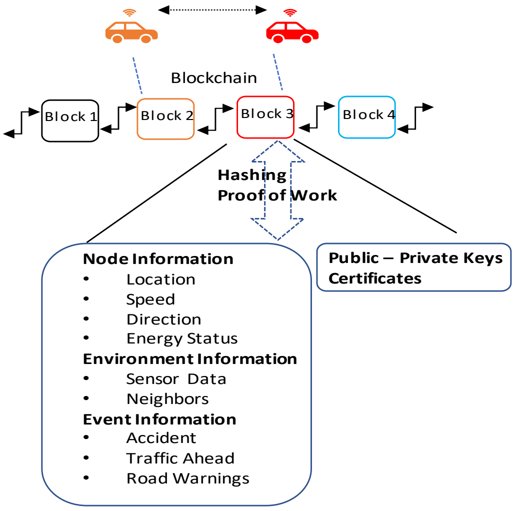

**Figure 3: Blockchain concepts for vehicular IoT networks**

**Secure edge cloud processing**: Novel decentralized architectures involve the use of nodes performing edge cloud processing tasks close to the IoT access networks for improving the network performance and minimizing end-end latency. This trend can be seen as an opportunity and as threat since the introduction of resource unconstrained devices may allow the offloading of security mechanisms of individual resource constrained nodes, but on the other hand such edge/fog nodes may be targeted due to their advanced network monitoring and control capabilities. In IoT architectures it is of great importance to achieve efficient processing of the collected information in order to generate the required control and actuation commands and to address the delay requirements of the respective applications which in some cases may be very demanding (e.g. collision avoidance in autonomous cars, precision manufacturing in smart factories, remote operations in telemedicine etc.) In order to achieve the end-end delay minimization, distributed architectures are being developed, introducing edge processing nodes that are close to the IoT access networks, leading to mobile edge clouds and fog architectures. Security is a major issue also in such system realizations and appropriate mechanisms should be in place to achieve it. The existence of edge nodes with more computation, storage, communication, and energy capabilities, as well as with a wider scope over the access network, compared to simple IoT devices, may be exploited to implement strong and effective security enforcement as well as intrusion detection schemes. Edge-based security architectures can be taxonomized into *user-centric*, where the user security mechanisms are offloaded to the edge node via a trusted virtual domain and are device-independent, *device-centric* , where edge nodes undertake specific security tasks tailored to each individual of IoT device and *end-to-end IoT security*, where secure middleware at edge nodes is used to abstract the IoT devices' heterogeneity and to enable their secure end-end connection [18].

There are obvious challenges in edge-based secure architectures, since edge nodes may be targeted for advanced attacks in order to compromise their network control capabilities and also to exploit the rich information that they acquire from the underlying IoT nodes. Since edge nodes may allow for more resource intensive algorithm and task executions, it is possible to consider the implementation of sophisticated edge cloud-based schemes based on machine learning and data mining, exploiting a reduced volume of collected information and data. This concept is illustrated in **Figure 4**. Also, hierarchical structures consisting of multiple edge nodes communicating with centralized cloud facilities, as suggested in [16], may enhance the effectiveness of edge-based security, shifting towards the cloud a reduced set of operations and minimizing thus the overhead and delay due to centralized processing and control.

Table 1 highlights some properties and issues related to the three abovementioned security enhancements for IoT.

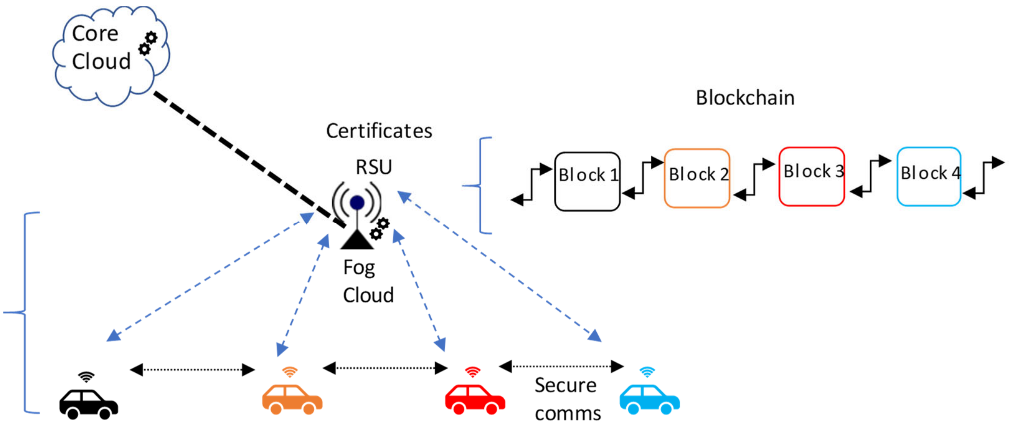

**Figure 4:** Secure mobile IoT communications using Blockchain and fog computing mechanisms

**Table 1** Key Reliability and Security Solutions' tradeoffs

| | |
|---|---|
| **Secure Routing** | **Pros:**<br>• Reliable and Secure message forwarding<br>• Resilience to DoS, MITM, Black/Grayhole attacks<br>**Cons:**<br>• Need for centralized coordination/asymmetric key generation<br>• Increased overhead for establishing secure channels<br>• Increased delay (also depending on the centralized cloud architecture |
| **Blockchain Trust Management** | **Pros:**<br>• Distributed Trust Management based on distributed consistent ledger<br>• Architecture matching peer-peer IoT networks<br>• Resilience to malicious node attacks based on prevailing node consensus<br>**Cons:**<br>• Need for processing power for each miner node hashing functions<br>• Increased overhead for establishing secure channels and for distributing blockchain updates<br>• Increased delay (also depending on the centralized cloud architecture |
| **Secure Edge Processing** | **Pros:**<br>• Architecture allowing for lower delays due to the closer placement of fog nodes to the IoT access nodes<br>• Increased processing functionalities and power for supporting advanced encryption and trust management mechanisms (e.g. Blockchain)<br>• Support for latency-critical applications<br>**Cons:**<br>• Increased functionalities in a fog node constitute it as a target for advanced security attacks compromising its operation and stored information<br>• Node mobility may require frequent handovers (session migrations) among neighboring edge fog nodes<br>• More complicated hierarchical network architecture (remote cloud-edge cloud-access network levels) |

## VI. Conclusions

The paper addressed the need for enhancing the reliability, privacy, resilience and security in cyber-physical networks of mobile interconnected devices and identified key related challenges within vehicular use cases, based on specific security threats. Furthermore, the paper highlighted key mechanisms in secure routing, blockchain trust management and secure edge cloud processing that can address these challenges and discussed their tradeoffs.

## Acknowledgement

This paper has been funded by the National Plan for Science, Technology and Innovation (MAARIFAH) – King Abdulaziz City for Science and Technology - the Kingdom of Saudi Arabia – award number 12-INF 2723-03. The authors also, acknowledge with gratitude the Science and Technology Unit in King Abdulaziz University for technical support.

## References

[1] J. Kempf, J. Arkko, N. Beheshti, K. Yedavalli, "Thoughts on reliability in the Internet of Things", *Proc. Interconnecting Smart Objects Internet Workshop*, pp. 1-4, 2011. [online] https://www.iab.org/wp-content/IAB-uploads/2011/03/Kempf.pdf

[2] N.Apthorpe, D.Reisman, S.Sundaresan, A.Narayanan, N.Feamster "Spying on the Smart Home: Privacy Attacks and Defenses on

Encrypted IoT Traffic”, *Computer Science*, 1708.05044v1, 16 Aug 2017

[3] R.Rogers, E.Apeh, C.J.Richardson, "Resilience of the Internet of Things (IoT) from an Information Assurance (IA) Perspective", *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, 2016, 110-115.

[4] L.Atzori, A.Iera, G.Morabito, M.Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization*", Computer Networks,* Vol.56 (2012) 3594–3608

[5] ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures November 2017, [Online] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[6] A.Burg , A.Chattopadhyay, K-Y Lam, "Wireless Communication and Security Issues for Cyber– Physical Systems and the Internet-of-Things", *Proceedings of the IEEE*, Vol. 106, No. 1, January 2018, DOI 10.1109/JPROC.2017.2780172

[7] D.Minoli, B.Occhiogrosso, "Blockchain mechanisms for IoT security", *Elsevier Internet of Things*, 1–2 (2018) 1–13

[8] J. Cynthia, H. Parveen Sultana, M. N. Saroja and J. Senthil, "Security Protocols for IoT", *Ubiquitous Computing and Computing Security of IoT,* Studies in Big Data, Jeyanthi N., Abraham A., Mcheick H. (eds)., vol 47. Springer, 2019

[9] ENISA Towards secure convergence of Cloud and IoT, September 2018, [Online] https://www.enisa.europa.eu/news/enisa-news/towards-secure-convergence-of-cloud-and-iot

[10] K.B.Kelarestaghi, K.Heaslip, M.Foruhandeh,R. Gerdes, "Intelligent Transportation System Security: Impact-Oriented Risk Assessment of In-Vehicle Networks", *IEEE Intelligent Transportation Systems Magazine*, January 2019, DOI: 10.1109/MITS.2018.2889714

[11] A.Alnassera, H.Sunb, J.Jiang, "Cyber Security Challenges and Solutions for V2X Communications: A Survey", *Computer Networks*, Vol. 151, 14 March 2019, Pages 52-67

[12] Deebak B.D., F.Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks", *Ad Hoc Networks*, 97 (2020).

[13] D.Airehrour, J.Gutierrez a, S.Kumar Ray, "Secure routing for internet of things: A survey", *Journal of Network and Computer Applications*, 66(2016)198–213

[14] N. Kshetri, “Can blockchain strengthen the Internet of Things?”, *IEEE IT Professional*, vol. 19, pp. 68–72, 2017. doi: 10.1109/MITP.2017.3051335.

[15] N.Kolokotronis, K.Limniotis, S.Shiaeles, R.Griffiths, "Secured by Blockchain: Safeguarding Internet of Things devices", *IEEE Consumer Electronics Magazine*, May 2019.

[16] R.Shrestha, R.Bajracharya, A.P.Shrestha, S.Y.Namb, "A new type of blockchain for secure message exchange in VANET", *Digital Communications and Networks*, (2019), doi.org/10.1016/j.dcan.2019.04.003.

[17] S.Kim, "Impacts of Mobility on Performance of Blockchain in VANET", *IEEE Access*, June 2019, DOI: 10.1109/ACCESS.2019.2918411

[18] K. Sha, T.A. Yang, W. Wei, S. Davari, “A survey of edge computing-based designs for IoT security”, *Digital Communications and Networks* (2019), doi: https://doi.org/10.1016/j.dcan.2019.08.006.