On the Software Architectures for fog-based Secure IOT Deployments

Christos Tselikis[1], Leandros Maglaras[2], Christos Douligeris[1] and Sarandis Mitropoulos[3]
[1]Department of Informatics, University of Piraeus, Piraeus 185 34, Greece
[2]School of Computer Science, Edinburgh Napier University, Edinburgh, UK
[3]Ionian University, Regional Development Department, Lefkada, Greece

ctselikis@unipi.gr
l.maglaras@naier.ac.uk
cdoulig@unipi.gr
sarandis@unipi.gr

Abstract: In this paper, we examine architectural designs for the support of demanding ad hoc IoT applications, such as industrial and large-scale IoTs. First, we examine the traditional software stack of nodes involved in centralized sensory applications. Then, we propose a highly distributed ad hoc architecture with increased node cooperation. Finally, we propose a secure fog-based hybrid model that offers optimizations with respect to performance and security and which facilitates the development of intelligent localized end-user applications with very strict latency requirements. In the three models that we examine we highlight operations at the routing layer and at the clustering sub-layer.

Keywords: IoT, Fog Computing, Security, Trust, AI/ML.

1. Introduction

Optimum architectural designs are essential for the successful deployment of secure Internet of Things (IoT) networks that are involved in modern use cases, such as industrial Internet of Things (IIoT) and massive IoT. It is well-known that time-critical IoT applications impose very strict requirements for latency, reliability and availability. Specifically, according to the IMT-2020 requirements (ITU 2017), the end-to-end latency in industrial IoT (e.g., robotic control in smart factories) should be less than one-millisecond. In addition, the massive IoT deployments generate *big data* which is not trivial to handle with legacy technologies.

For such time-sensitive and large-scale IoT applications, we identified a number of intensive requirements that can only be satisfied with the adoption of novel, efficient and effective automated solutions:

- There is an increasing demand for achieving even better network performance in support of time-sensitive applications. To satisfy very strict performance requirements, the fog architecture (Open Fog Reference Architecture 2017) can be the solution to effectively reduce the network response times.
- There is strong demand for novel applications with local characteristics which can assist to handle contemporary social needs, such as environmental, health-related, and transport-related. To this end, node cooperation is vital in order to be able to perform in-time, informed and automated decision-making at the local vicinity of interest (e.g., a parking lot, a shopping mall or a historical city sector).
- There is an intensive need to efficiently handle the *big data* inside mobile content delivery networks. This *Big data* is generated especially by the use of multimedia and geospatial applications, for example by vehicle passengers. Also, very large-scale sensory data is generated in the massive Internet of Things. Computing and storage capacity to perform automated AI/ML processing of the *big data* is vital to tackle this requirement.
- There is a need for adaptive network management. ML-based network design, resource management and control with AI/ML have already been successfully implemented in various networked IoT deployments.
- There is a strong need for stronger security (for example, certificate-based mutual authentication between devices as well as between users and the network) and for privacy enhancing mechanisms such as layered use of pseudonyms. We propose the integration of cooperation mechanisms into the wireless communications system in order to increase the array of attacks that can be handled effectively.

To tackle these challenges, the existing communications models and software architectures need optimization if not complete adaptation. As we will see in the next sections, we have to utilize and effectively integrate the

new computing models (such as fog computing) in the deployments of Internet of Things which nowadays expand at very large scale.

This paper is organized as follows. After this first introductory section, which identifies the contemporary challenges for modern IoT applications., Section 2 presents the work related to the topic of security and privacy in novel fog-based architectures used in wireless ad hoc networks. In Section 3, we analyze three architectures and provide the details of the software stacks of the nodes involved in ad hoc IoT applications. The fourth section presents the proposed security solutions, while Section 5 draws the main conclusions and states the directions for future work.

2. Related Work

In this section, we examine and present related work on fog-based security solutions that have been recently proposed. These works fall into several categories, ranging from pure fog computing to combinations integrating blockchain techniques and advanced authentication methods.

In (Vaquero 2014), based on the readings aggregated from the sensors, the reputations of the sensors are calculated and then these reputations are classified differentially with the use of adaptive rather than fixed reputation levels. Data sets are trusted only from high reputation nodes. Fortino et al. (Fortino 2020) examined several architectural options in the integration effort of IoT with fog computing. Security and privacy issues of fog-based architectures have been extensively examined recently in several survey papers (Mukherjee 2020), (Mukherjee 2017), (Rani 2022).

In (Alzoubi 2022), the authors analyzed several blockchain-based fog computing solutions and how these solutions can achieve a distributed and trusted system, identity management, secure data, reputation, and payment systems. According to their findings such convergence would take several years and a great deal of work to be accomplished. The authors in (Katsikogiannis 2018) propose a policy-based management scheme utilizing the Service Oriented Architecture (SoA) for machine-to-machine communications.

The secure authentication of devices and users in a complex system that consists of end nodes, fog nodes, cloud providers, and several hardware and software platforms is a rather difficult problem to solve. The solution must be kept simple and computationally efficient while at the same time offering a high level of security. In a recent article that focuses on the security of healthcare architectures, the authors propose an efficient and authenticated key establishment scheme that resists common attacks and reduces computation overhead (Li 2022). Focusing only on the authentication of end users, another recent work proposes a combination of honeywords and authenticators that can offer protection against several attacks, while keeping the process simple and platform-agnostic (Papaspirou 2021).

Fog computing is mostly related to data that are collected from the end devices and sent to the fog nodes for computation, aggregation or analysis. In several domains, like the healthcare sector, these data may be sensitive and sometimes it is crucial to be able to correctly classify them before deciding to send them to a nearby fog node or to the cloud. The authors in (Sarrab 2022) proposed a framework for the classification of streamed data according to their criticality level. This framework can be used in order to reassure better protection of sensitive data and can be applied to other domains. Privacy preservation of data in fog computing is a critical matter that has been extensively researched recently (Sarwar 2022).

3. Architectural Designs

In this section we examine three different architectural designs, namely the centralized, the fully distributed and the hybrid ones under IoT scenarios. We examine if and how each one of the three different software architectures can address the challenges we identified in our introduction regarding time-sensitive, large-scale and secure localized applications. In each case, we focus on the operations at the routing layer and at the clustering sub-layer.

3.1 Centralized architecture

We examine the centralized IoT model based on the use case of an environmental application. In this scenario, there exist sensor nodes that forward their readings (e.g., moisture reports) to a sink point which is the networked base station with Internet connectivity. The base station performs the main information processing requested by the sensory application, makes the results available to the Internet and also sends commands or queries to manage the deployed sensors. We assume here that the gateway runs a clustering application to hierarchically organize the sensor nodes in clusters.

Initially, the base station assigns to the registered wireless small devices (sensors, PDA/smart phones) their configuration settings over the radio interface (e.g., IEEE 802.15.4). Figure 1 shows the sensors' software stack consisting of the physical/node discovery, the routing and the application layers and also highlights the clustering module installed at the gateway node. Physical parameters include the environmental data, the sensor location, the velocity, the connectivity degree and the energy which along with each sensor's neighbour list are periodically forwarded and passed to the clustering module at the gateway node. The base station executes a number of clustering runs to determine the cluster head set which defines the sensor network structure. Once the network structure has been determined, the base station broadcasts the cluster head list to the sensors via the radio control channel. The sensors can now forward their readings encrypted to the known local cluster heads. The latter can use default routing to reach the base station in one hop. Distance vectors are usually preferred for ad hoc routing in multi-hop scenarios (Sheng 2013). Alternatively, geographical routing can be utilized (Aznaoui 2021).

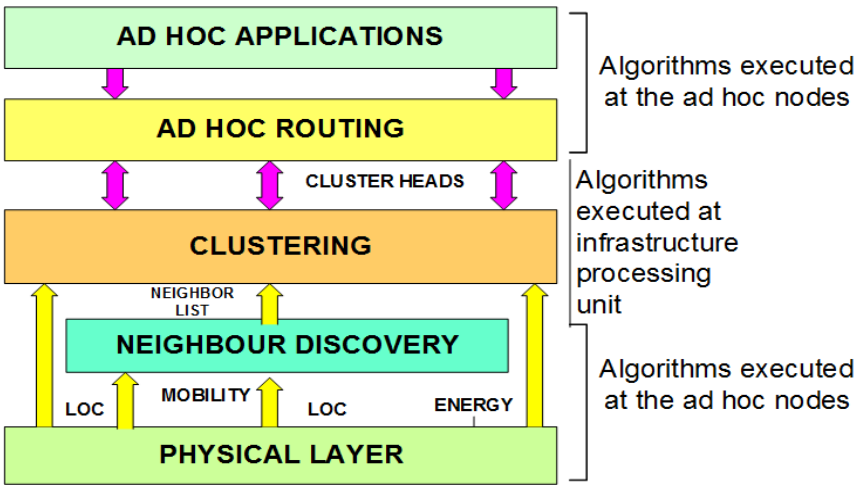

Figure 1: Software architecture for the centralised IoT model.

The above centralized design is more suitable for deploying static sensory applications of a small scale, such as, for example, monitoring of a small agricultural field. It is evident that this kind of processing at the local sink node cannot handle the *big data* that contemporary massive IoT applications generate nor can it address the dynamicity of mobile applications such as vehicle-to-vehicle image/video/data sharing scenarios.

3.2 Distributed cooperative architecture

The second architecture, shown in Figure 2, is a generic cross-layer framework that we propose for ad hoc IoT networks. Not all the components shown in Figure 2 are to be implemented at the network nodes; the actual implementations depend on the specific application's requirements, the capacity of the nodes and the network deployment choices available to the operator. This architecture differs from the centralized design in that now highly distributed interactions exist amongst peer ad hoc devices. The distributed components reside at the middleware layer providing a number of services to both end-user and management applications, including trust-security services, brokered publish-subscribe messaging services, service discovery, and energy and load management.

The devices now take autonomous decisions by participating in cooperative distributed protocols, such as in clustering protocols for the selection of local cluster heads or for the selection of local Certificate Authorities that establish trust. Every ad hoc node, due to the middleware, can become, for example, a local cluster head without the need of a gateway decision, or it may become a responsive intruder detector that broadcasts alerts in the event of malicious actions. Note that the malicious nodes, either external or internal, may launch various types of network attacks. Such attacks may target to harm a) the operations of the network protocols, b) the integrity of the data exchanged inside the network, and c) the users' privacy, mainly their identity, location and content of personal communications.

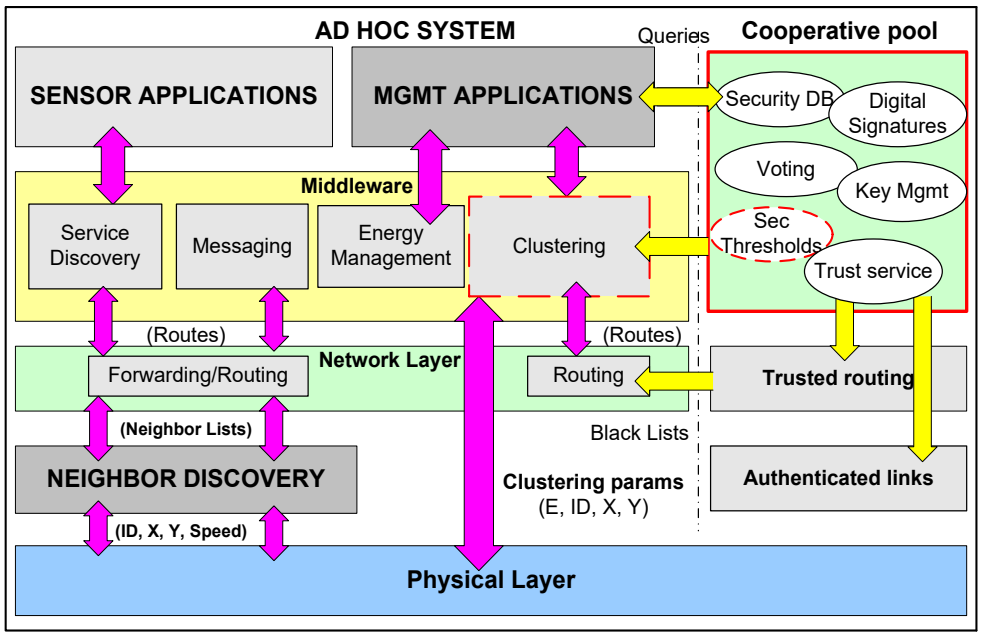

Figure 2: Software architecture for the distributed IoT model.

We enhance the IoT middleware layer with a pool of distributed components which are implemented as software libraries and which provide additional cooperative services to the end-devices. For example, a re-clustering process running at the ad hoc IoT plane can make a remote procedure call to the service of a distributed voting protocol which is based on security thresholds (Tselikis 2012). According to this scheme, the local nodes can securely reach an agreement regarding the identities of the IoT nodes that have the capacity to act as local Cluster Heads (or as local Certificate Authorities).

As another example of using the pool of cooperative components shown in Figure 2, the re-clustering procedure can trigger the execution of a Group Key Agreement protocol to establish, on-the-fly, a symmetric secret key. This key can be utilized as input to a symmetric algorithm to encrypt the messages exchanged inside an ad hoc group of nodes, such as industrial sensors or vehicles (Tselikis 2020). Alternatively, the routing protocol can call the services of a trust-based mechanism in order to resolve the next hop node based on the level of the nodes' reputation (Zahariadis 2010).

In our opinion, the distributed architecture shown in Figure 2 although is suitable for dynamic ad hoc IoT deployments, it lacks provisions for handling with analytics the big data generated in the massive IoT and also imposes computing overhead on the restricted IoT nodes. In addition, tight synchronization guarantees must be satisfied to successfully conduct the compound distributed operations present in this architecture.

3.3 Hybrid architecture

We propose the use of a hybrid architecture to meet the IoT requirements for small latency, big data handling, robust automated analytics processing with AI/ML, redundancy, scalability, privacy and security. It was made evident before that neither the centralized nor the distributed architecture can tackle the requirements in massive IoT and those in industrial environments. To this end, we propose to integrate the infrastructure-less wireless IoT networks with the cellular network adopting novel models, namely the fog computing paradigm and the disaggregated software-based architectural design of the Open Radio Access Network initiative (O-RAN Alliance 2023).

The fog architecture inserts a robust distributed layer, namely the fog tier, between the IoT devices and the centralized infrastructure at the cloud tier. The communication with fog nodes decreases the end-to-end latency and saves bandwidth since there is no need to contact the remote cloud for services. The end-devices generate a large number of data reports relating to local area information (e.g., images/video of road conditions). This data is hierarchically stored in the fog nodes or it can be optionally sent to the cloud.

In this context, new end-user applications can be designed and served by local servers installed at the vicinity of events of interest. For example, fog nodes installed at Road Side Units (RSU) may serve user queries regarding a free parking space (Ni 2017). On the other hand, local organizations or commercial entities can apply advanced processing to the data stored in the fog nodes in order to predict conditions and, therefore, make better

decisions (e.g., a transport entity can deduce knowledge for excessive pollution levels of a city area and then can re-route the traffic accordingly).

The IoT devices can communicate directly with each other or via the cellular network. In such a hybrid model, we can place the local servers which are envisaged in the fog model at the local infrastructure of the cellular network, i.e., at the 4G/5G base stations. Having more computational, communication and storage resources, the base stations can operate not only as local access points (traffic aggregators) but as intelligent estimators/predictors by utilizing AI/ML algorithms. The latter can run (or move) as virtualized/containerized components in the fog. In addition, in this way, processing-intensive tasks, such as intruder detection and routing optimizers, can be offloaded to the robust fog nodes.

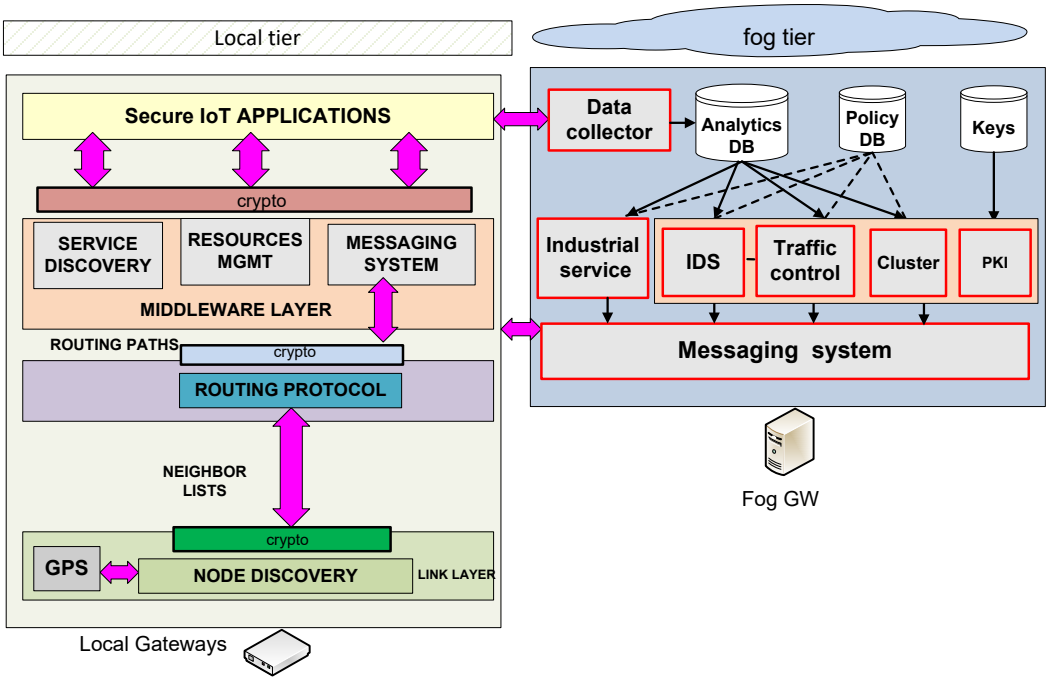

Figure 3: Fog-based hybrid IoT architecture.

As shown in Figure 3, with our proposal the network operator has the ability to utilize location-aware AI/ML-based controllers and analytics databases, as those are hierarchically envisaged in the Open RAN architecture, however at the fog tier. In more detail, an ML-based IDS component is shown in Figure 3. IDS agents monitor in real-time the end-user traffic collected and stored in a fog database and detect anomalies (e.g., DoS/DDoS attacks) or other suspicious user actions based on the classification made by a pre-trained ML model. The IDS agents also react in the event of such attacks by utilizing the messaging subsystem to broadcast alerts inside the network.

Further functionality can be achieved in case the agent interfaces with the Traffic Controller (TC). The traffic controller is another component used for the purposes of policy-based network management. This controller can act as a policy engine that loads the policies from a fog database and interfaces with the ad hoc messaging system. It is vital that TC can send (re)configuration commands to the IoT devices, or to other components that belong to the fog tier, based on the input fed by the IDS agent, as previously explained. If such an interface between the IDS agent and the TC is supported, the IDS agent, in the event of an attack, can trigger a signal to the TC containing information on the type of the launched attack. Then, the TC engine based on this input, can select new actions policies (security-wise or performance-wise) sending appropriate configuration commands to the devices and network elements.

The third architectural scheme can cope with a mixture of network models, e.g. with 4G/5G cellular IoT and with Vehicular to Infrastructure (V2I) applications. More specifically, it is proposed that the fog components and their interfaces shown in Figure 3 can be implementations compliant with the specifications of the Open RAN disaggregated architecture which introduces open and standardized interfaces between the network elements in the Radio Access Network.

4. Security

Fog nodes need to handle a large number of IoT devices or moving vehicles. In several cases, the users' data are exposed due to untrusted components residing on fog nodes, for example compromised nodes with malicious software. Privacy preservation is more challenging in fog computing since fog nodes that are in vicinity with the end users can collect sensitive data concerning the identity, communication pattern or coordinates. This information can be used for profiling and inference. Moreover, since fog nodes can be geographically distributed, centralized control becomes difficult.

In order to be able to secure our hybrid model we propose the combination of several solutions that include cryptographic methods, consistency controls, anti-spoofing mechanisms and intrusion detection systems. To achieve multi-fence protection, we adopted complementary protective solutions as suggested in (Mukherjee 2017). As shown in Figure 3, each ad hoc layer in the stack is protected with cryptographic primitives. Moreover, we exploit the fact that when location knowledge is available to the routing protocol, another layer of protection is offered against malicious nodes who broadcast faulty topology claims, given that the location and the identity of the nodes are cryptographically protected through digital signatures. In order to achieve this goal, we propose to have a fog-based PKI system that creates and stores the long-term keys for every IoT node. These keys are used to encrypt the sent messages and also to digitally sign them. Each node is certified by a Certificate Authority (CA) that issues a digital certificate that includes information about the location of the node.

The proposed model includes an intrusion detection system that constantly monitors, collects and aggregates the packets that are exchanged among nodes in its proximity. When the behaviour of the local neighbourhood of the IDS differs from the normal one that the IDS 'knows' the IDS sends alarms to the administrator of the system that can further investigate the situation similar to the one presented in (Ferrag 2019).

IoT devices must be able to verify whether the fog nodes are secure and, therefore, trust should be established. Our model incorporates the idea of clustering and voting. The nodes create clusters based on their proximity using distributed algorithms like the ones presented in (Maglaras 2012) and elect as cluster head the one that is more stable among the candidates. The cluster head can take over several actions in the neighbourhood, can act as a data collector, or even perform intrusion detection processes among others.

5. Conclusions

In this paper, we described traditional and new proposed software architectures for IoT deployments. We presented operational examples involving some of the ad hoc communications protocols (clustering and routing) that are involved in time-sensitive IoT application scenarios.

The centralized architecture, which is still being utilized in many sensory applications, is suitable for small-scale and mainly static wireless sensor networks. The distributed peer-to-peer architecture has attracted strong interest in the previous years and many middleware systems have been developed and utilized so far in commercial IoT deployments. However, in our opinion, it is doubtful not only whether the peer-to-peer model can tackle the performance and security requirements of the URLLC Use Case, but whether it can satisfy the need to efficiently handle the *big data* that modern large-scale multimedia applications create. In order to strengthen the security guarantees, we proposed cooperative enhancements in the case of the distributed peer-to-peer architecture.

Finally, we proposed a hybrid software framework that integrates the infrastructure-less ad hoc networks with the fog computing paradigm allowing the design of novel localized applications with stronger security (resilience to attacks) and better performance (smaller communications latency). We integrated in this fog-based model certain AI/ML components, namely the IDS agent and the Traffic Controller. By exploiting the robust computing and storage resources available at the fog tier, the IDS can run ML models which facilitate the detection of traffic anomalies inside IoT networks. In addition, the IDS component can be responsive in the event of attacks by applying a new configuration of the things tier.

In future work, we shall investigate further the integration path between wireless IoT networks and 5G cellular networks applying architectural concepts used in the Open RAN specifications. We could further investigate the integration of blockchain into the proposed model in order to further enhance privacy preservation and the integrity of the information but having in mind also the need for keeping a high quality of service in terms of latency and throughput.

Acknowledgements

This work has been partially supported by the European Union through project CybereSecPro (Project No. 101083594).

References

Alzoubi, Y. I., Al-Ahmad, A. and Kahtan, H. (2022) “Blockchain technology as a Fog computing security and privacy solution: An overview”, Computer Communications, Volume 182, pp. 129-152.

Aznaoui H., Ullah A., Raghay S., Aziz L. (2021) “Advanced GAF routing protocol using the goal attainment method in WSN”, NISS (ACM): 11:1-11:7.

Ferrag M. A. and Maglaras L. (2019) “Deliverycoin: An ids and blockchain-based delivery framework for drone-delivered services,” Computers, vol. 8, no. 3, p. 58.

Fortino G. et al. (2020) “Trust and Reputation in the Internet of Things: State-of-the-Art and Research Challenges”, IEEE Access, Volume 8, pp. 60117-60125.

ITU Report (2017), ITU-R M.2410. Available at: https://www.itu.int/pub/R-REP-M.2410, [accessed 28-03-2023].

Katsikogiannis G. et al. (2018) “A policy-aware Service Oriented Architecture for secure machine-to-machine communications”, Journal of Ad Hoc Networks, 80, 208, pp. 70-80.

Li, X. et al. (2022) “An efficient and authenticated key establishment scheme based on fog computing for healthcare system”, Frontiers of Computer Science, 16(4), pp. 1-12.

Maglaras L. A. and Katsaros D. (2012) “New measures for characterizing the significance of nodes in wireless ad hoc networks via localized path-based neighbourhood analysis”, Social Network Analysis and Mining, Volume 2, no. 2, pp. 97–106.

Mukherjee M. et al. (2020) “Security and privacy issues and solutions for fog,” Fog and Fogonomics: Challenges and Practices of Fog Computing, Communication, Networking, Strategy, and Economics, pp. 353– 374.

Mukherjee M. et al. (2017) “Security and Privacy in Fog Computing: Challenges”, IEEE Access, Volume 5, pp. 19293-19304.

Ni J. et al. (2017) “Security, Privacy and Fairness in Fog-based Vehicular Crowdsensing”, IEEE Communications Magazine, pp. 146-152.

Open Fog Reference Architecture for Fog Computing, produced by the OpenFog Consortium Architecture Working Group. Available at:
https://site.ieee.org/denver-com/files/2017/06/OpenFog_Reference_Architecture_2_09_17-FINAL-1.pdf
[accessed 28-03-2023].

O-RAN Alliance. Available at: https://www.o-ran.org/ [accessed 28-03-2023].

Papaspirou, V. et al. (2022) “Security Revisited: Honeytokens meet Google Authenticator”, *7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, Ioannina, Greece, pp. 1-8.

Rani, S., Kataria, A. and Chauhan, M. (2022) “Fog computing in industry 4.0: Applications and challenges—A research roadmap” Energy Conservation Solutions for Fog-Edge Computing Paradigms, Springer, Singapore pp. 173-190.

Sarrab, M. and Alshohoumi, F. (2022) “Assisted Fog Computing Approach for Data Privacy Preservation in IoT-Based Healthcare”, Security and Privacy Preserving for IoT and 5G Networks, Springer, Cham, pp. 191-201.

Sarwar, K. et al. (2022) “Efficient privacy-preserving data replication in fog-enabled IoT”, Future Generation Computer Systems, Volume 128, pp. 538-551.

Sheng, Z. et al. (2013) "A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities", IEEE Wireless Communications, vol. 20, no. 6, pp. 91-98.

Tselikis, C. et al. (2012) "Degree-Based Clustering Algorithms for Wireless Ad Hoc Networks Under Attack," IEEE Communications Letters, Volume 16, no. 5, pp. 619-621.

Tselikis C. et al. (2020) “On the conference key distribution system with user anonymity”, Journal of Information Security and Applications, Volume 54: 102556.

Vaquero L. M. and Rodero-Merino L. (2014) “Finding Your Way in the Fog: Towards a Comprehensive Definition of Fog Computing,” ACM SIGCOMM Computer Communications Rev., vol. 44, no. 5, pp. 27–32.

Zahariadis T. et al. (2010) "Trust management in wireless sensor networks", European Transactions on Telecommunications, 21.4: pp. 386-395.