EDGE COMPUTING FOR CRITICAL ENVIRONMENTS: VISION AND EXISTING SOLUTIONS

Ijaz Ahmad[1], Andrea Gentili[1], Rupender Singh[1], Juhani Ahonen[2], Jani Suomalainen[1], Seppo Horsmanheimo[1], Heikki Keranen[3], Erkki Harjula[4]

[1]VTT Technical Research Centre of Finland, Finland, [2]Nokia, Finland, [3]Satel, Finland, [4]University of Oulu, Oulu, Finland

NOTE: Corresponding author: Rupender Singh, rupendersingh04cs39@gmail.com

Abstract – *With the increasing connectivity of critical infrastructures through wireless technologies, the importance of edge computing is increasing manyfolds. Edge computing has become an important phenomenon combining the strengths of distributed computing technologies with those of telecommunication technologies. Therefore, new technological breakthroughs are happening in the realm of edge computing for critical environments, such as the next generation underground and open-pit mining. Since the mining technologies are moving at a faster pace towards digitization leveraging connectivity technologies, edge computing plays a crucial role in bringing computing and connectivity into mines to provide latency- and security-critical services on site. In this article, we study how edge computing fulfills the needs of critical environments, focusing on mining environments, and provides important insight into future research directions.*

Keywords – 5G, connectivity, critical environments, edge computing, mining

1. INTRODUCTION

Edge computing brings traditional Information Technology (IT), mainly computing and storage, near to the data sources and users in communication technologies [1, 2]. In telecommunications, edge computing converges technologies of IT with cellular communication networks. In edge computing, server capacity is deployed locally, such as at a base station in a cellular network, so that selected services provided by cloud platforms can be deployed at the edge of the cell and near the users, thus the term edge computing originates from here. Multi-access Edge Computing (MEC) is the standard under the umbrella of the European Telecommunications Standards Institute (ETSI) for providing high computing and storage facilities for Internet of Things (IoT) or Industrial IoT in the vicinity of the IoT near the new generation Radio Access Networks (RANs) [3].

On one hand, edge computing facilitates industrial systems and processes through local storage and processing, and, on the other hand, it facilitates connectivity to other industrial systems, as well as local and external networks [4]. With localized capacity, edge computing facilitates bringing novel services into industrial systems by extending cloud-based systems and workflows to the working environment. Diverse machinery in industrial systems with time-varying requirements will need edge resources due to limited on-board processing and storage, and possibly limited or no external connectivity. Therefore, edge computing can be very useful for real-time support and monitoring in critical environments. Critical environments refer to spaces where sensitive machinery, technology, or processes are located that require optimal conditions through control procedures. In this article, a Next Generation Mining (NGMining) environment is considered as a critical environment.

A mining environment can be either underground (subsurface) or open-pit (surface), or in the sea. The NGMining environment considered in this article is depicted in Fig. 1, which consists of underground and open-pit mining environments. Edge platforms, connected to base stations, operate in both mining environments for the necessary services, such as providing computing facilities to monitoring devices mounted to various equipment. Since the NGMining environment is an extremely complex space with geological, mechanical, and electrical complexities, the edge platform must help to ensure safe, secure, reliable, and continuous operations. Therefore, in this article, we attempt to study what edge computing can offer in such critical environments, what are the most suitable existing solutions, and what needs to be done to fulfill the unique requirements of critical environments. For example, novel concepts of Artificial Intelligence (AI)/machine learning must be coupled with existing proven technologies used for improving edge platforms or MECs to not only automate the mining processes and services, but to mitigate the need for human involvement in all critical process. Hence, a zero-touch security and management framework leveraging MEC, and AI needs to be developed to not only operate autonomously in normal situations, but also adjust itself in unforeseen or unpredicted events. Therefore, we also elaborate on how edge computing complements zero-touch security and services in critical environments such as NGMining.

This article is organized as follows: Section 2 provides a background on the use of edge computing in NGMining environments. Section 3 describes how edge computing meets the unique requirements of NGMining. Section 4 briefly elaborates on secure zero-touch connectivity in NGMining using edge computing, and section 5 concludes the article. For smooth readabilty, the acronyms with corresponding full forms are presented in Table 1.

Table 1 – Expansion of acronyms and abbreviations

Acronym	Expansion
3GPP	Third Generation Partnership Project
5G	Fifth Generation
AI	Artificial Intelligence
API	Application Programming Interface
ARPKI	Attack Resilient Public Key Infrastructure
CPS	Cyber-Physical System
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
EI	Edge Intelligence
ENISA	European Network and Information Security Agency
ETSI	European Telecommunications Standards Institute
FL	Federated Learning
IoT	Internet of Things
ICT	Information and Communications Technology
IT	Information Technology
KPI	Key Performance Indicator
MPW	Modular Private Wireless
MEC	Multi-access Edge Computing
NDAC	Nokia Digital Automation Cloud
NGMining	Next Generation Mining
PDP	Packet Data Protocol
RAN	Radio Access Network
STC-AOG	Spatial-Temporal-Causal AND-OR Graph
SZTP	Secure Zero-Touch Provisioning
TI	Tactile Internet
TEE	Trusted Execution Environment
VCU	Vehicle Control or Connectivity Units
WEMI	Weak Electromagnetic Intrusion Detection

2. BACKGROUND

2.1 Brief introduction of NGMining

The concept of Next Generation Mining (NGMining) emerged in the Finnish research project called NGMining [5], which seeks to automate the mining operations through the developments in the Information and Communications Technology (ICT) sector, mainly 5G. The NGMining environment consists of underground and open-pit mines. The mining environment is a highly critical one since it comprises sensitive machinery, operations and processes, or spaces that require controlled operations. A typical NGMining environment that is connected through 5G, and operates autonomously, is presented in Fig. 1. It consists of two parts, i.e., the underground mine and the open-pit mine. Machinery, such as excavation vehicles, in the mines are connected to 5G networks either through 5G base stations or WiFi, depending on the mobility and speeds of the vehicles. The vehicles are also connected to each other through vehicle control or connectivity units (VCUs). The VCUs can perform minor processing tasks such as video encoding and situational awareness-related tasks. Tasks that require higher processing and storage capabilities are performed in the edge computing nodes.

NGMining proposes the integration of novel technologies into the mining environment for autonomous and safe operations. Since accidents in mines are extremely dangerous in terms of human and capital resources [6], automation of processes, machinery, and vehicles is inevitable [7]. Such automation requires connectivity infrastructures, as discussed in [8]. Due to the physical structures of mines with varying radiation and attenuation attributes of signals, specific attention is paid to the communication infrastructures. Since the communication between different entities including static and moving machinery, processes, gates, and humans must always be working, solutions that pave the way towards increased reliability, safety and security, and continuous operations are needed. Edge computing, in this vein, presents an interesting solution as discussed below.

2.2 Intelligent edge for NGMining

Edge computing will be highly useful in the safe and reliable operation of mines, as well as for the controlled operations of the diverse sets of equipment and machinery used in mines. Edge computing has been studied and surveyed in [9] to present an array of opportunities for critical environments. The NGMining environments, underground and open-pit, have distinct requirements. From a wireless connectivity point of view, typical 5G connectivity in underground and open-pit can be provided with field or area-specific extensions. For example, both underground and open-pit networks will involve highly mobile units that require high-precision positioning. Such positioning will require on-board processing coupled with processing, such as MEC units, in nearby base stations, to provide updated information about other mobile or stationary units. Since the information will be highly time-sensitive, real-time, or near-real-time processing provided by the edge platform will be crucial. The underground environment is a complicated one due to weak signal strengths with limited radio propagation caused by complex tunnel structures and rough surfaces [8]. Therefore, edge computing will play a crucial role to provide the necessary services within complex environments that can have partial disconnections to external resources and networks.

The visual representation in Fig. 1 shows mobile equipment which is connected to other mobile units or other resources in the mine through radiocommunications. Edge platforms located underground are connected to mobile units through radio resources and can be connected to other edge platforms either through radio interfaces or wired lines. These edge platforms can provide various applications to mobile units even if external connectivity is lost. Such applications can be related to monitoring,

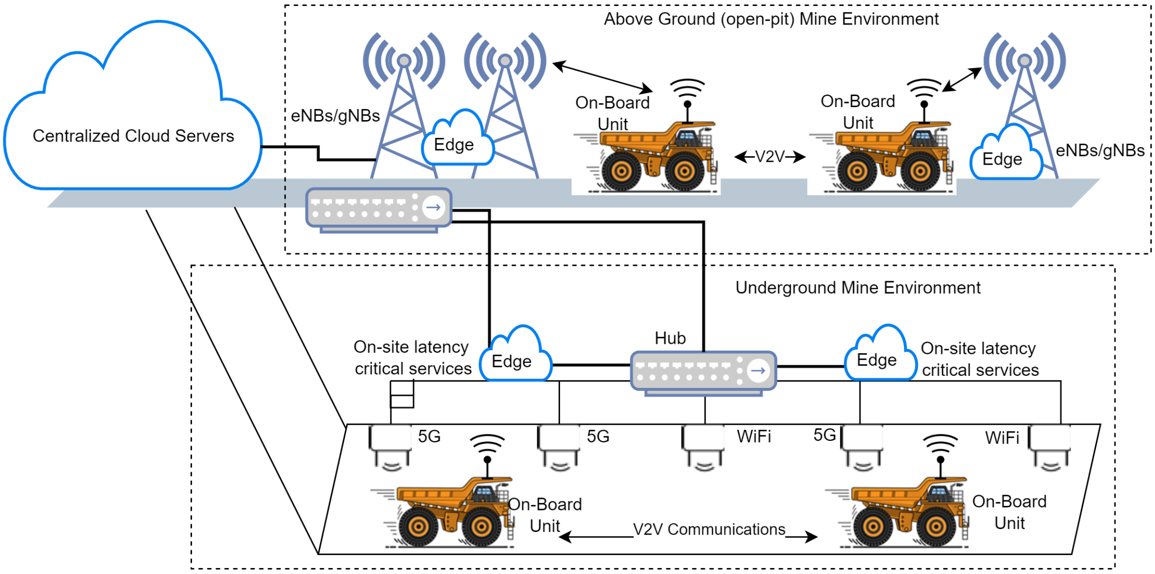
Above Ground (open-pit) Mine Environment
Centralized Cloud Servers
eNBs/gNBs
Edge
On-Board Unit
V2V
On-Board Unit
Edge
eNBs/gNBs
Underground Mine Environment
Hub
On-site latency critical services
Edge
Edge
On-site latency critical services
5G
5G
WiFi
5G
WiFi
On-Board Unit
V2V Communications
On-Board Unit

Fig. 1 – Sample underground and open-pit NGMining environments

control, and protection including situation awareness, safety zone alerting, and on-site data analytics, among others. Edge computing platforms deployed in underground mines can also enable the autonomous operation of mining equipment with remote assistance.

Data gathered from the mining site from various sensors, mobile equipment, and monitoring devices can help in localized decision-making for autonomous operations, leveraging Artificial Intelligence (AI). Edge computing and AI have recently become highly complementary [10, 11, 12], enabling diverse services, resulting in Edge Intelligence (EI). Edge platforms, thus, offer unique opportunities for localized AI-based operations in NGMining. EI can be further pushed, creating a sink and information processing base, into equipment or machinery where localized storage and processing can take place on-board equipment. Such a unit can be called, e.g. a local edge or a micro-MEC unit, which is synchronized with the MEC hosted by the access network. Such a hierarchical edge platform for NGMining is discussed below.

2.3 Hierarchy of cloud platforms (multi-level edge)

The NGMining environment necessitates a hierarchy of computing and storage platforms to support each other for different use cases. In practice, there will be a processing/storage platform on the machinery and mining vehicles. These platforms have limited capabilities and, thus, require computational capacity from edge hosts in proximity for computationally-intensive and/or latency-limited tasks[13]. Since edge resources are limited as well, there will be a need for cross-edge and cloud coordination [14]. We call this **edge-cloud continuum**. Looking at the constraints of the environment (availability of resources) and services (e.g. latency boundaries), the edge-cloud continuum will need to work in a functionally-synchronized manner. The functionality in terms of performing tasks in the existence of such constraints is presented in Fig. 2 and Fig. 3.

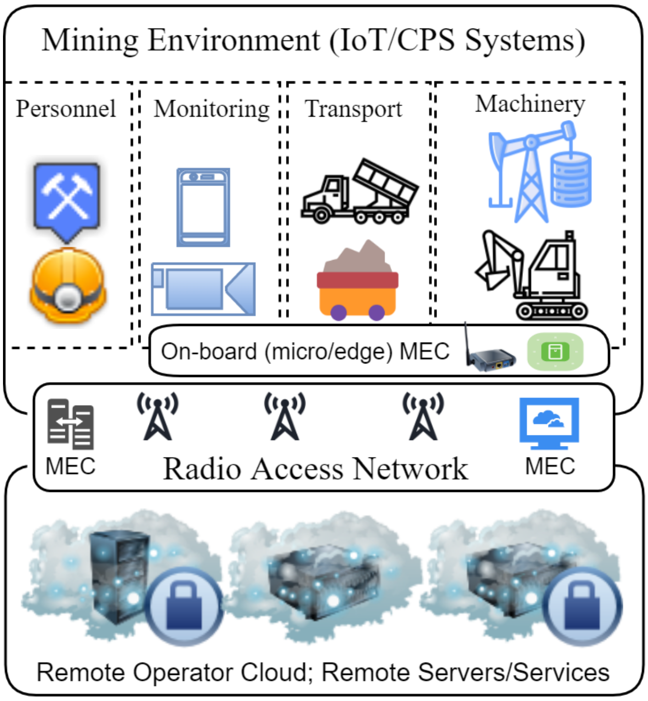
Mining Environment (IoT/CPS Systems)
Personnel
Monitoring
Transport
Machinery
On-board (micro/edge) MEC
MEC
Radio Access Network
MEC
Remote Operator Cloud; Remote Servers/Services

Fig. 2 – Micro-edge, MEC, and centralized clouds

In Fig. 2 it is shown that different equipment will host their own processing unit, termed as micro-edge. These micro-edge platforms are connected to the MEC platforms at the edge of the cell, typically with a 5G base station. The edge devices are connected to centralized or remote cloud platforms with higher processing and storage capabilities. How resource allocation or handling of processing requests are carried out is shown in Fig. 3. Actions like video encoding, suitable for local processing, are managed on-site, while tasks such as vehicle monitor-

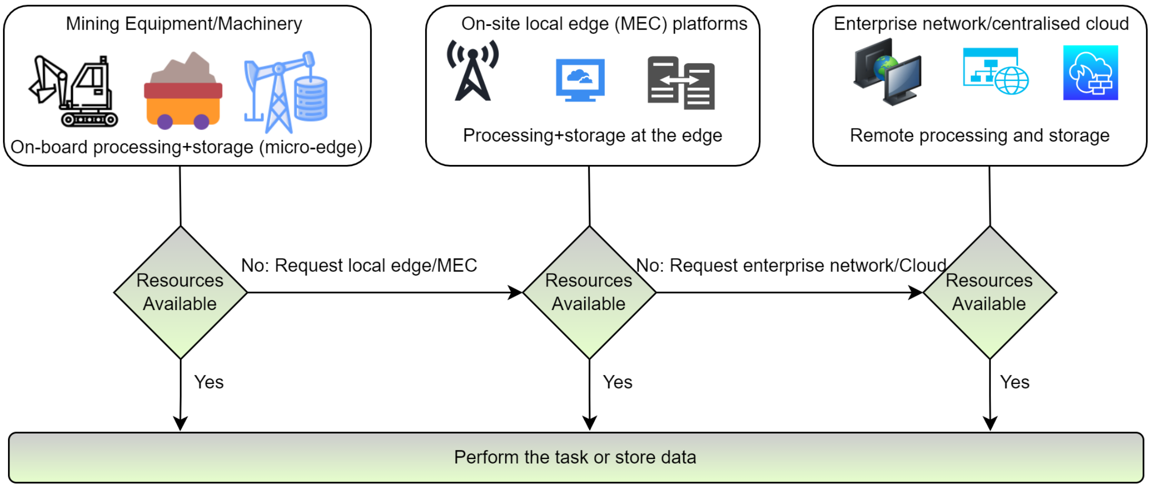
Mining Equipment/Machinery
On-board processing+storage (micro-edge)
On-site local edge (MEC) platforms
Processing+storage at the edge
Enterprise network/centralised cloud
Remote processing and storage
Resources Available
No: Request local edge/MEC
Resources Available
No: Request enterprise network/Cloud
Resources Available
Yes
Yes
Yes
Perform the task or store data

Fig. 3 – Generic architecture showing the working of resource allocation between micro-edge, MEC, and centralized cloud platforms

ing occur at the edge. Actions that require further higher processing, such as AI-based operations, are carried out in the centralized clouds. Such synchronized edge-cloud architectures can increase the performance of the overall system, as evaluated in [15].

3. HOW INTELLIGENT EDGE MEETS THE NGMINING REQUIREMENTS?

In this section, we discuss the most important requirements of NGMining that can be met through edge computing. The list of requirements can be large, however, we focus on the most important ones that can be solved technologically through the combination of enabling communication infrastructure and distributed processing and storage units, such as MEC platforms.

3.1 Reliability

Mining environments are sensitive and critical infrastructures that require highly reliable digital and manual operations [16]. Since the operations of current mining environments rely on communication technologies to connect diverse machinery, reliable communications infrastructures must be in place [17]. Thus, edge computing can play a critical role in increasing the reliability of mining environments from many perspectives. To elaborate on the increased reliability, consider an emergency situation as an example. Emergency situations in the mining environment can be caused by many factors, including accidents and natural hazards, such as malfunctioning machinery or leakage of hazardous gases, respectively. In such situations, localized edge computing nodes get monitoring data from actuators and sensors can quickly guide the workers and other equipment for the right actions. For example, the edge computing nodes can immediately calculate the risk and inform the workers to move to safe locations, ask the mobile machinery to stop moving, and ask other machinery to halt functioning. Relying on external or distant computing or monitoring can be dangerous in situations where connectivity from actuators and sensors in the working environments is disrupted due to accidents and natural hazards.

In normal situations, edge computing offers services to latency-critical services, and thus increases the reliability of maintaining routine operations as well as meeting stringent requirements of critical services. The concepts of MEC have already been evaluated for highly dynamic environments comprising extremely low-capacity IoT devices that require extremely low latency [14]. Similarly, the concepts of edge computing have also been coupled with other technologies, such as blockchain, for environments that require high reliability and security such as industrial IoT [18]. As another example, through AI-enabled edge computing, a proactive maintenance service is established involving the prediction of equipment maintenance by gathering data from edge points. This approach contributes to the enhancement of equipment reliability [19]. This will help in saving the lives of mining workers, as 90% of mining deaths are caused by machine malfunctions [20].

3.2 Continuous and secure operation

Continuous operation and support of ICT-based services will require ensuring continuity of operations through fail-proof and secure connectivity. Edge-based digital twins can ensure visible operation continuity, thus ensuring the support of digital twins through the edge platforms will be important. Furthermore, a visual analysis through edge platforms that integrate the digital twin and proprietary devices (specifically the on-board processing units on machinery and equipment) can provide a way forward for a fully functional system for the whole environment. The existing commercial and open source edge platforms already provide such functionalities, as discussed in Section 3.6. From the perspectives of integration of different types of edge nodes and services, open

Application Programming Interfaces (APIs) that are easily interoperable, such as those developed with Swagger [21] for instance, can provide a way forward in integration.

To enable security and reliability, two approaches can be considered. One, the security of the edge platform itself, and two, the security of the operating environment. Security resources, both human and computing-wise, are typically more limited when compared to security operation capabilities in centralized cloud services. Consequently, edge services may be more vulnerable to security incidents than cloud-based services. The security of the edge platform requires strong authentication and authorization. In [22], the security of a function-specific edge platform, that is miniature in nature, is considered. The security of services in edge platforms can be secured through a combination of techniques ranging from slice-based isolation to authorization, and authentication techniques. Certificate-based authentication, also supported by existing commercial platforms, for instance, and adopting security layer-based approaches can provide promising solutions to security. The security of the whole ecosystem will play an important role, such as the security of the enabling 5G infrastructure [23], and operating machines such as vehicles [24].

3.3 Situation awareness

Situation awareness encompasses the convergence of a number of technologies and technological concepts, including the digital twin, precision location, visual input and analysis, data analytics, and AI techniques. Edge platforms will play a crucial role in hosting these technologies in the NGMining sites. The digital twin can show and map different cyber and physical systems and the interactions between them. Precision location information will be needed to track the exact and precise mobility of different machines, vehicles, and personnel in the mining environment. The location information must be provided to the edge resources, and thereby shared with other platforms for analysis for situational awareness. Since there will be huge amounts of data from sensors and video/surveillance cameras, it can be filtered and discovered for only useful data using edge analytics which cuts down the resources [25]. The AI-assisted edge platform can help in situational predictions or estimations and real-time analysis based on dynamic decision-making and dynamic resource allocation [26], [27].

3.4 Safety zones and alerting

Dynamic safety zones will require connectivity of all resources and personnel in the NGMining environment. Edge platforms can play a critical role in enabling the connectivity of different machinery, equipment, and personnel in the environment [28]. For this, first, a safety zone should be defined, and then, location technologies need to be embedded into user equipment and machinery [29]. This will also require leveraging precision location technologies. The edge platform will provide the necessary computation in the user environment for processing the location information, matching the safety zones and locations of machinery and personnel, and creating alerts based on the outcome of the processing [30]. Thus, edge computing will play a crucial role in creating dynamic safety zones and informing machinery and personnel through creating alerts in real time.

3.5 Data analytics at the edge

Due to the higher number of sensing devices and autonomous machines and personnel involved, the mining environment will generate huge amounts of data. Real-time data analytics will therefore require an edge platform to perform data analysis and provide feedback in shorter times to latency critical services. Generally, data can be categorized into three main categories based on time-sensitivity as described in [31], and summarized below:

- ***Hard real time:*** has a strict predefined latency. For example, industrial control systems, autonomous vehicles, drones, etc.
- ***Soft real time:*** has predefined latency, yet can tolerate some bounded latency. For example, live voice and video calls.
- ***Non-real time:*** has no time sensitivity and can tolerate latency. For example, batch and continuous haulage.

Utilization of data analytics extends to enhancing edge performance within a collaborative multi-edge framework, as elucidated in [32]. Within the NGMining context, specifically in subterranean settings, the deployment of multiple edge platforms is envisaged, necessitating inter-platform communication to facilitate resource and task distribution. This situation inherently leads to the inevitability of cross-edge platform communication and collaborative resource sharing. Notably, industrial systems like the Nokia Digital Automation Cloud (NDAC) exhibit processing resource limitations, necessitating either inter-platform resource sharing or the incorporation of supplementary resources such as accelerators. The strategic implementation of data analytics assumes paramount importance across several domains, encompassing the establishment of safety zones, activation of alert mechanisms, fault diagnosis, tolerance and analysis procedures, along with cybersecurity fortifications.

3.6 Existing relevant platforms

There are many types and variants of edge computing, as discussed in [61], [62], and [63]. The main aim of such platforms is converging telecommunication and IT services mainly by providing a cloud computing platform at the radio edge of the network, i.e., radio access network. Due to its overarching importance, many companies have developed service or solution-specific platforms such as edge platforms for industrial, manufacturing, Cyber-Physical Systems (CPS), and transportation systems, etc., as elaborated in [64], [65], and [66], for instance. Some examples of the most relevant platforms are presented in Table 2. For brevity, only the names of the platforms with respective references, and brief descriptions are provided. The selected platforms are the most relevant to the next generation mining technologies. Furthermore, the list is not exhaustive, but provides a glimpse of existing offerings by a diverse vendor base.

4. EDGE FOR SECURE ZERO-TOUCH CONNECTIVITY

Zero-touch services play a crucial role in safeguarding critical environments against the need for manual setup of essential services and technologies. According to the European Union Agency for Cybersecurity, ENISA, [67], around 90 percent of the connectivity loss in 2021 by European telecommunication operators was due to human errors. The criticality of the environment such as NGMining requires automated deployment of new services, updates of parameters, and configurations to avoid human-introduced errors and latency. The benefit of zero-touch network management is that the mining operative personnel do not need to do (but only minimum) parametrization and configuration of devices and machinery. This saves time (and thus, money) as well as helping to avoid human error in local configuration.

In the NGmining case, the most pertinent use case is that of automated vehicles also mounted with routers to provide connectivity to onboard units or temporary connectivity to on-location devices. The zero-touch functionality starts when the vehicle where the router is installed is started and turned on, or the vehicle enters the network for the first time. According to standard 3GPP network operation, the router will request Packet Data Protocol (PDP) context, or bearer activation, and receives 5G network-related configuration from the 5G network. After this, the vehicle reports to the mining operation center or similar central service (or even the cloud, should Internet access be available). This will notify the central management about vehicles coming online. This event also enables central zero-touch services to push this vehicle-specific configuration to the router, for example, routing configuration. Furthermore, information about possible software updates is pushed. Zero-touch configuration could also be utilized by applications running in the vehicle network, such as video stream endpoints. Zero-touch operation requires successful authentication. Edge computing will have a very consequential role in providing the necessary cloud resources within the environment. Thus, the chances of mishaps due to Internet disconnection will be reduced. Building a secure zero-touch network environment requires a purpose-built server running and reachable within the vicinity, and thus the role of edge computing is amplified.

- **Zero-touch network management:** Considering the cost of down time in the mining environment, the connectivity from the mining equipment should be done in invisible or seamless manner, so that the mine IT should not need to manually configure each vehicle control unit (VCU) separately. This leads also to significant savings on the personnel cost and overall efficiency. Similarly, all VCU related operations and performance should be reported to fleet management, central monitoring systems such as NDAC.
- **Security:** Zero-touch architecture requires strict application on cyber security principles: access to the zero-touch must be secured and authenticated. After secure access to zero-touch, process control related Cyber Security settings can be retrieved from central configuration database. This would be for example IPSEC / OpenVPN parameters.
- **Intelligent IP Connectivity:** While the connectivity from the Vehicle to the 5G network is very varying, for example video, remote control, configuration traffic, positioning related connections etc., it is very important to manage the prioritization of the traffic. The 3GPP 5G radio interface has separate QoS management, which the 5G modem should conform to. Furthermore, the VCU can affect and apply the QoS on IP (OSI layer 3) level and for the vehicle internal Ethernet, on Ethernet (OSI L2) level.

The edge computing platforms enable plug-and-play installation around ISA/IEC 62443 standards to support the secure zero-touch automated edge environment [30]. The edge devices authenticate the servers remotely using stored private device keys and a combination of certificates. This enables easy installation of edge devices at one location or multi-location in under-resourced areas such as NGMining. Recent advancements in zero-touch automation and its security, as listed in Table 3, indicate that zero-touch automation has several use cases in NGMining. For instance, the 5G connectivity between the server and router mounted on the automated vehicles serving under the mines. These vehicles keep reporting to the mining operation center or similar central service (or even the cloud, should Internet access be available).

5. FUTURE RESEARCH DIRECTIONS

Machine learning techniques that are proposed for embedding intelligence in edge environments also have security limitations and challenges, as discussed in [78]. Therefore, before deploying machine learning techniques in a critical environment it is important to evaluate its security implications. Along with the transition towards 6G systems, both added flexibility of increased software components to be used as virtual resources, as well as increased security and resilience of those elements towards

Table 2 – Existing relevant MEC Platforms

Platform	Details
Nokia Digital Automation Cloud (NDAC) [33]	An end-to-end wireless edge platform designed to serve the industrial sector as well as governments, cities, and webscale businesses. It integrates reliable high-bandwidth, low latency 4G/5G connectivity with local edge computing capabilities and a plethora of ready-made applications.
Nokia's MX Industrial Edge [34]	High-performance edge architecture for asset-intensive industrial environments. The platform permits the flexibility to choose the NDAC or Modular Private Wireless (MPW) network architecture to meet industrial connectivity needs.
Siemens Industrial Edge [35]	Mobile edge computing industrial platform that brings AI applications to the field devices.
Verizon 5G edge [36]	Designed to enable developers to build applications for mobile end users and wireless edge devices providing low-latency communication. The synergy with the AWS platform provides solutions such as AWS Wavelength [37] that bring the advantages of the world's leading cloud closer to the edge.
Microsoft Azure Stack Edge [38]	Fully managed private MEC platform that brings compute and storage services on premises. Matched with on-site 5G connectivity [39] can enable increased efficiencies and a higher level of security.
IBM [40] [41]	IBM's edge and telco cloud solutions ecosystem support enterprises to deploy their cloud platforms and to leverage edge computing advantages. IBM Edge Application Manager [42] is an intelligent and flexible application that provides autonomous management for edge computing.
Advantech WISE-EdgeLink [43, 44]	It is a cross-platform and edge-computing gateway that enables to transmit the equipment data to the cloud and to third-party environments, permitting the management of systems utilizing handheld devices.
AlefEdge [45]	Leading-edge Internet platform that enables 5G applications through open APIs at the edge. Alef's edge API platform enables enterprises to deploy their own private mobile networks leveraging the benefits of edge computing.
Affirmed Networks [46]	Affirmed's Cloud Edge (ACE) solution hosts applications and keeps data locally on the customers' premises (for increased latency and efficiency), and can also be deployed and utilized at the edge of the mobile operator's network or used as part of the cloud edge offerings from AWS, Microsoft Azure, or Google Cloud.
ClearBlade [47]	Running in the cloud, and on premises at the edge, ClearBlade's middleware platform is designed to connect various parts of IoT, being the only software platform that can deploy a common software stack across the board.
Mutable [48]	Provides edge technology to application providers, cable operators, and cloud providers. Mutable's software platform operates on operators' existing servers, automatically prioritizing the owner's workloads, and selling the computing capabilities not utilized to unlock more potential revenues.
MobiledgeX [49]	Software platform provider in the mobile edge computing space, uniting operators, developers, and cloud providers with edge resources to foster edge applications.
Section [50]	DevOps focused-based edge computing platform, which integrates with application engineers' workloads. The solution permits having full control over how, when, and where data processing occurs.
EdgeX Foundry [51]	Highly flexible and scalable open-source software framework that facilitates interoperability between devices and applications at the IoT Edge. It enables architectures that meet specific requirements of the edge IoT.
Project EVE [52]	Permits building an open, curated, and universal operating system for solution deployments at the distributed edge. Project EVE enables lifecycle management and remote orchestration of any application and hardware, and incorporates a zero-trust security model.
Fledge [53]	Scalable and secure IIoT open-source platform for building and operating industrial applications for condition monitoring, predictive maintenance, increased efficiency (Overall Equipment Effectiveness, or OEE), higher quality, situation awareness, and safety.
Home Edge [54]	Edge computing open-source framework, platform, and ecosystem that provides an interoperable, flexible, and scalable edge orchestration and computing services platform, with APIs that can also be used with libraries and runtimes to enable various user scenarios for the home.
Baetyl [55]	General-purpose platform for edge computing that manipulates different types of hardware facilities and device capabilities into a standardized cloud-native runtime environment and API, enabling the efficient management of application, service and data flow through a remote console both on cloud and on premises.
Nokia SEP [56]	Supports innovative RAN use cases implementing O-RAN standardized near-real-time RIC capabilities together with ETSI-defined MEC Application Programming Interfaces (APIs).
MiTAC [57]	MiTAC actively participates in 5G infrastructure development in O-RAN Alliance, OCP (Open Compute Project), and ODCC (Open Data Center Committee) to create an open 5G environment with the utilization of COTS hardware.
Aether [58]	Aether is the first open-source 5G connected edge platform that provides 5G mobile connectivity and edge cloud services for distributed enterprise networks. It represents a complete and open 5G solution addressing RAN through Core, democratizing the availability of a robust and complete software-defined 5G platform for developers.
Adlink [59]	ADLINK provides a scalable and cost-effective white-box solution to encourage the deployment of 5G RAN and private networks, enabling 5G DU/CU in open RAN. [60]

Table 3 – Recent advancements in zero-touch networks

Focus	Proposed algorithms/approaches	Details
Secure zero-touch networks	Distributed Ledger Technologies (DLTs) coupled with AI-driven operations [68]	Creation of a secure zero-touch environment for 5G through AI, DLT, and cloud native technologies. Architecture aims for cross-domain security and trust orchestration via DLTs and AI-driven operations. Validation through three use cases at 5GBarcelona and 5TONIC/Madrid. Key challenges: Pervasive networking limitations in current 5G standards. Need for automated end-to-end operations and distributed AI for cognitive orchestration. Contribution: Zero-touch security and trust architecture. Future research: Multi-stakeholder service chains, efficient service delivery.
	pi-Edge Platform [69]	Establishment of secure zero-touch automation via core security services and support security services. Innovative mechanism for automated network operations. Detailed algorithmic insights, performance metrics, and system design constraints to be provided. Impact: Enhanced security in zero-touch environments. Future research: Algorithm refinements, integration with AI.
	Gradient boost algorithms for Distributed Denial of Service (DDoS) attacks [70]	Gradient boost-based DDoS attack detection and mitigation. Proactive defense against similar future attacks. Detailed algorithms, innovation in DDoS prevention, performance metrics, and potential challenges to be elaborated. Contribution: Proactive DDoS protection. Future research: Advanced attack vectors, algorithm robustness.
	Various approaches including API, intent, AI and machine learning for security [71]	Implements authentication, authorization, encryption, and input validation for secure access and manipulation. Assessed using security assessment tools, evaluated in terms of attack success rate, and verified against industry standards.
	Attack Resilient Public Key Infrastructure (ARPKI) schemes [72]	Integrates Attack Resilient Public Key Infrastructure (ARPKI) with Secure Zero-Touch Provisioning (SZTP) for secure bootstrapping of edge devices. Provides accountability, prevents impersonation attacks. Mutual authentication using TLS 1.3 handshake.
Zero-touch management	Hierarchical language framework based on Spatial-Temporal-Causal AND-OR Graph (STC-AOG) [73]	A hierarchical language framework proposed for a zero-touch network where grammar structure of STC-AOG was adopted to express the network constraints of the language system.
	Network slicing for zero-touch networks [74]	Overview of challenges of virtualization of zero-touch networks.
	Deep learning-based Weak Electromagnetic Intrusion Detection (WEMI) [75]	A method proposed to detect the WEMI attacks on industrial IoT nodes by exploiting the fingerprints of the node.
	eXplainable AI-powered Federated Learning (FL) framework [76]	XAI-powered FL-enabled framework proposed for zero-touch network, had the ability to interpret the critical predictions of latency Key Performance Indicators (KPIs).
	Tactile Internet (TI) architecture [77]	A TI-based architecture proposed to convert a network into zero-touch by eliminating communication between the master and slave nodes using AI algorithms.

malicious attacks in the network and system malfunctions are needed. For example, very limited work exists on integrity verification of data that is used in training machine learning algorithms. One of the most common types of attacks against distributed AI systems is the poisoning attack [79], where the intruder injects false training data to corrupt the learning model itself. Since in edge-cloud architectures, the upper tiers in the network usually receive the learned parameters, but not the raw data itself, detecting false data and behavior of functional components through e.g. anomaly detection is needed already on local and edge tiers.

Furthermore, machine learning may also consume huge amounts of, not only computational but also communication, resources in case the learning algorithm is run far from data sources. New machine learning techniques that combine network semantics can minimize the sole reliability of the gathered data, as evaluated in [80] and can be helpful for critical environments.

A single MEC platform may become a single point of failure. Hence, multiple MEC platforms synchronized with each other and hierarchical MEC platforms will be useful. However, such synchronization and hierarchy of MEC platforms can also result in cascading failures if proper load-balancing techniques are not in place. Therefore, research on such scenarios of MEC including horizontal (cross-platform), and vertical (hierarchical) synchronization along with load-balancing supervision is needed. Moreover, techniques for minimizing the chances of loss of information during the handover from MEC to MEC, i.e., primary to secondary, as discussed in [81] should also be investigated.

The edge infrastructure can be shared between different users who may not fully trust each other nor the platform provider. For instance, in the mining scenarios, we can foresee situations where the public safety authorities are given access to communication and information services on the edge of a private mining company, but authorities could also utilize the edge as a computing platform to deploy authorities' mission-critical services. The concept of confidential computing has been proposed [82, 83], to increase edge security in these situations. The concept isolates critical data and code with cryptography, when stored or transmitted, or with hardware-based Trusted Execution Environments (TEEs) or homomorphic cryptography when processed. Examples of TEEs include Intel SGX, ARM TrustZone, or AMD Secure Encrypted Virtualization. Utilization of confidential computing requires rethinking the application architectures, specifying new trust models, and recognizing the critical minimal assets that require additional protection. Research is needed also when offloading and orchestrating critical functions between cloud, edge, and devices.

6. CONCLUSION

Edge computing plays a pivotal role in connected services due to its numerous advantages in providing distributed and low-latency service availability. Since AI-based data analytics and automation are becoming increasingly important for critical services, edge computing provides an opportunity to leverage on-site computing and storage facility for AI. Moreover, edge services can utilize AI for improving the service offering, and thus edge intelligence or intelligent edge has emerged as an important technological concept. In this paper, we have studied the importance of intelligent edge in the realm of NGMining environments. First, we have studied the relation of intelligent edge with mining environments and then elaborated on various approaches related to the integration of intelligent edge and mining technologies. The paper also provides a study of existing industrial edge solutions that are relevant to NGMining. Furthermore, important concepts and technologies related to zero-touch networking for the NGMining are provided. In summary, this article provides important research insights into the future of using edge in critical environments.

ACKNOWLEDGMENT

This work was supported in part by the Business Finland through the NGMining, AI-NET-ANTILLAS, and the SUNSET-6G projects.

REFERENCES

[1] Pedro Garcia Lopez, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino, Adriana Iamnitchi, Marinho Barcellos, Pascal Felber, and Etienne Riviere. *Edge-centric computing: Vision and challenges*. 2015.

[2] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. "Edge computing: Vision and challenges". In: *IEEE inter. of Things J.* 3.5 (2016), pp. 637–646.

[3] Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher, and Valerie Young. "Mobile edge computing—A key technology towards 5G". In: *ETSI white paper* 11.11 (2015), pp. 1–16.

[4] Jude Okwuibe, Juuso Haavisto, Erkki Harjula, Ijaz Ahmad, and Mika Ylianttila. "SDN Enhanced Resource Orchestration of Containerized Edge Applications for Industrial IoT". In: *IEEE Access* 8 (2020), pp. 229117–229131. DOI: 10.1109/ACCESS.2020.3045563.

[5] VTT Technical Research Centre of Finland. *Next Generation Mining (NGMining) Project*. 2022. URL: https://www.vttresearch.com/en/news-and-ideas/vtt-nokia-sandvik-collaborate-5g-powered-research-project-next-generation.

[6] "Accident analysis of two Turkish underground coal mines". In: *Safe. Sci.* 42.8 (2004), pp. 675–690. ISSN: 0925-7535. DOI: https://doi.org/10.1016/j.ssci.2003.11.002.

[7] Jonathon Ralston, David Reid, Chad Hargrave, and David Hainsworth. "Sensing for advancing mining automation capability: A review of underground automation technology development". In: *Inter. J. of Mining Sci. and Tech.* 24.3 (2014). Special Issue on Green Mining, pp. 305–310. ISSN: 2095-2686. DOI: https://doi.org/10.1016/j.ijmst.2014.03.003. URL: https://www.sciencedirect.com/science/article/pii/S2095268614000469.

[8] Serhan Yarkan, Sabih Guzelgoz, Huseyin Arslan, and Robin R. Murphy. "Underground Mine Communications: A Survey". In: *IEEE Commun. Surv. Tut.* 11.3 (2009), pp. 125–142. DOI: 10.1109/SURV.2009.090309.

[9] Francesco Spinelli and Vincenzo Mancuso. “Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility”. In: *IEEE Commun. Surv. Tut.* 23.1 (2021), pp. 596–630. DOI: 10.1109/COMST.2020.3037674.

[10] Yuanming Shi, Kai Yang, Tao Jiang, Jun Zhang, and Khaled B Letaief. “Communication-efficient edge AI: Algorithms and systems”. In: *IEEE Commun. Surv. Tut.* 22.4 (2020), pp. 2167–2191.

[11] Tiago Koketsu Rodrigues, Katsuya Suto, Hiroki Nishiyama, Jiajia Liu, and Nei Kato. “Machine learning meets computation and communication control in evolving edge and cloud: Challenges and future perspective”. In: *IEEE Commun. Surv. Tut.* 22.1 (2019), pp. 38–67.

[12] Ella Peltonen, Ijaz Ahmad, Atakan Aral, Michele Capobianco, Aaron Yi Ding, Felipe Gil-Castiñeira, Ekaterina Gilman, Erkki Harjula, Marko Jurmu, Teemu Karvonen, Markus Kelanti, Teemu Leppänen, Lauri Lovén, Tommi Mikkonen, Nitinder Mohan, Petteri Nurmi, Susanna Pirttikangas, Paweł Sroka, Sasu Tarkoma, and Tingting Yang. “The Many Faces of Edge Intelligence”. In: *IEEE Access* 10 (2022), pp. 104769–104782. DOI: 10.1109/ACCESS.2022.3210584.

[13] Ivana Kovacevic, Erkki Harjula, Savo Glisic, Beatriz Lorenzo, and Mika Ylianttila. “Cloud and Edge Computation Offloading for Latency Limited Services”. In: *IEEE Access* 9 (2021), pp. 55764–55776. DOI: 10.1109/ACCESS.2021.3071848.

[14] Erkki Harjula, Pekka Karhula, Johirul Islam, Teemu Leppänen, Ahsan Manzoor, Madhusanka Liyanage, Jagmohan Chauhan, Tanesh Kumar, Ijaz Ahmad, and Mika Ylianttila. “Decentralized IoT edge nanoservice architecture for future gadget-free computing”. In: *IEEE Access* 7 (2019), pp. 119856–119872.

[15] Jude Okwuibe, Juuso Haavisto, Ivana Kovacevic, Erkki Harjula, Ijaz Ahmad, Johirul Islam, and Mika Ylianttila. “SDN-Enabled Resource Orchestration for Industrial IoT in Collaborative Edge-Cloud Networks”. In: *IEEE Access* 9 (2021), pp. 115839–115854. DOI: 10.1109/ACCESS.2021.3105944.

[16] “Study On Key Technologies Of Internet Of Things Perceiving Mine”. In: *Procedia Engin.* 26 (2011). ISMSSE2011, pp. 2326–2333. ISSN: 1877-7058. DOI: https://doi.org/10.1016/j.proeng.2011.11.2442.

[17] “Intelligent Mining Technology for an Underground Metal Mine Based on Unmanned Equipment”. In: *Engineering* 4.3 (2018), pp. 381–391. ISSN: 2095-8099. DOI: https://doi.org/10.1016/j.eng.2018.05.013.

[18] Tanesh Kumar, Erkki Harjula, Muneeb Ejaz, Ahsan Manzoor, Pawani Porambage, Ijaz Ahmad, Madhusanka Liyanage, An Braeken, and Mika Ylianttila. “BlockEdge: blockchain-edge framework for industrial IoT networks”. In: *IEEE Access* 8 (2020), pp. 154166–154185.

[19] Baotong Chen, Yan Liu, Chunhua Zhang, and Zhongren Wang. “Time Series Data for Equipment Reliability Analysis With Deep Learning”. In: *IEEE Access* 8 (2020), pp. 105484–105493. DOI: 10.1109/ACCESS.2020.3000006.

[20] *Accelerating mining safety and smart mines with limitless connectivity*. Ericsson. URL: https://www.ericsson.com/en/blog/2021/11/accelerating-mining-safety-and-smart-mines-with-limitless-connectivity.

[21] *API Development for Everyone*. Swagger. URL: https://swagger.io/.

[22] Ijaz Ahmad, Sergio Lembo, Felipe Rodriguez, Stephan Mehnert, and Mikko Vehkaperä. “Security of Micro MEC in 6G: A Brief Overview”. In: *IEEE 19th Annual Cons. Commun. Netw. Conf. (CCNC)*. IEEE. 2022, pp. 332–337.

[23] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila. “Security for 5G and Beyond”. In: *IEEE Commun. Surv. Tut.* 21.4 (Fourthquarter 2019), pp. 3682–3722. ISSN: 2373-745X. DOI: 10.1109/COMST.2019.2916180.

[24] Diana Pamela Moya Osorio, Ijaz Ahmad, José David Vega Sánchez, Andrei Gurtov, Johan Scholliers, Matti Kutila, and Pawani Porambage. “Towards 6G-Enabled Internet of Vehicles: Security and Privacy”. In: *IEEE Open J. of the Commun. Soci.* 3 (2022), pp. 82–105. DOI: 10.1109/OJCOMS.2022.3143098.

[25] Wenbin Chen, Yuxin Chen, Yishuo Jiao, and Quanchun Liu. “Security Awareness Scheme of Edge Computing in IoT Systems”. In: *IEEE 4th Inter. Conf. on Comp. and Commun. Engin. Tech. (CCET)*. 2021, pp. 332–335. DOI: 10.1109/CCET52649.2021.9544267.

[26] Rongbin Xu, Wangxing Lin, Zhiqiang Liu, Menglong Wang, Yuanmo Lin, and Ying Xie. “Real-time Situation Awareness of Industrial Process based on Deep Learning at the Edge Server”. In: *20th IEEE/ACM Int. Symp. on Cluster, Cloud and Inter. Comp. (CCGRID)*. 2020, pp. 823–826. DOI: 10.1109/CCGrid49817.2020.000-3.

[27] Pratik Baniya, Gaurav Bajaj, Jerry Lee, Ardeshir Bastani, Clifton Francis, and Mahima Agumbe Suresh. “Towards Policy-aware Edge Computing Architectures”. In: *IEEE Int. Conf. on Big Data (Big Data)*. 2020, pp. 3464–3469. DOI: 10.1109/BigData50022.2020.9377982.

[28] Liangcai Fang, Chungui Ge, Guolin Zu, Xinkun Wang, Weiguo Ding, Changliang Xiao, and Liang Zhao. "A Mobile Edge Computing Architecture for Safety in Mining Industry". In: *SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI*. 2019, pp. 1494–1498. DOI: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00269.

[29] *AI in industrial automation (white paper)*. ZVEI. URL: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2021/April/AI_in_Industrial_Automation/AI-in-Industrial-Automation-White-Paper-NEU.pdf..

[30] Michal Wisniewski, Bartlomiej Gladysz, Krzysztof Ejsmont, Andrzej Wodecki, and Tim Van Erp. "Industry 4.0 Solutions Impacts on Critical Infrastructure Safety and Protection–A Systematic Literature Review". In: *IEEE Access* 10 (2022), pp. 82716–82735. DOI: 10.1109/ACCESS.2022.3195337.

[31] Najmul Hassan, Kok-Lim Alvin Yau, and Celimuge Wu. "Edge Computing in 5G: A Review". In: *IEEE Access* 7 (2019), pp. 127276–127289. DOI: 10.1109/ACCESS.2019.2938534.

[32] Hai Jin, Lin Jia, and Zhi Zhou. "Boosting edge intelligence with collaborative cross-edge analytics". In: *IEEE Inter. of Things J.* 8.4 (2020), pp. 2444–2458.

[33] *Nokia Digital Automation Cloud*. Nokia. URL: https://dac.nokia.com/.

[34] *MX Industrial Edge*. Nokia. URL: https://www.nokia.com/networks/industry-solutions/mx-industrial-edge/.

[35] *Industrial Edge*. Siemens. URL: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-edge.html.

[36] *Harness the power of 5G Edge*. Verizon. URL: https://www.verizon.com/business/solutions/5g/edge-computing/.

[37] *AWS Wavelength*. Verizon. URL: https://www.verizon.com/business/solutions/5g/edge-computing/aws-wavelength-5g/.

[38] *Verizon debuts private mobile edge cloud computing for enterprises with Microsoft Azure*. Verizon. URL: https://www.verizon.com/about/news/verizon-debuts-cloud-computing-microsoft-azure.

[39] *On Site 5G. High capacity. Highly secure.* Verizon. URL: https://www.verizon.com/business/products/networks/connectivity/on-site-5g/.

[40] *Edge Computing Solutions*. IBM. URL: https://www.ibm.com/cloud/edge-computing.

[41] *IBM 5G and edge computing*. IBM. URL: https://www.ibm.com/downloads/cas/0WOR6ORJ.

[42] *IBM Edge Application Manager*. IBM. URL: https://www.ibm.com/cloud/edge-application-manager.

[43] *Advantech Edge Computing Platform*. Advantech. URL: https://campaign.advantech.online/en/global/intelligent-systems/edge-computing/.

[44] *Realize the Real Industrial IoT with Data Management via WISE-EdgeLink*. Advantech. URL: https://select.advantech.com/wise-paas-edgelink/?utm_medium=technology_highlight&utm_source=landing_page&utm_campaign=edge_computing_portal.

[45] *The Edge Your Enterprise Deserves*. Alef Edge. URL: https://www.wearealef.com/.

[46] *Affirmed Cloud Edge – Mobile Edge Computing*. Affirmed Networks. URL: https://www.affirmednetworks.com/products-solutions/mec-solutions/.

[47] *Clearblade Edge Platform*. Clearblade. URL: https://www.clearblade.com/clearblade-edge-platform/.

[48] *The Sharing Economy For Servers*. Mutable. URL: https://mutable.io/.

[49] *Edge Services*. MobileedgeX. URL: https://mobiledgex.com/.

[50] *Edge Compute Solutions*. Section. URL: https://www.section.io/iot/.

[51] *Why EdgeX?* EdgeXFoundry. URL: https://www.edgexfoundry.org/why_edgex/why-edgex/.

[52] *Project EVE*. LF Edge. URL: https://www.lfedge.org/projects/eve/.

[53] *Fledge*. LF Edge. URL: https://www.lfedge.org/projects/fledge/.

[54] *HomeEdge*. LF Edge. URL: https://www.lfedge.org/projects/homeedge/.

[55] *Baetyl*. LF Edge. URL: https://www.lfedge.org/projects/baetyl/.

[56] *Nokia SEP integrates RIC and MEC into a single solution*. Nokia. URL: https://www.nokia.com/networks/mobile-networks/service-enablement-platform/#single-solution.

[57] *5G RAN / Edge Computing*. MiTAC. URL: https://www.mitacmct.com/EN/solution/5G_edge_computing_solution.

[58] *ONF's Private 5G Connected Edge Platform Aether™ Released to Open Source*. IEEE. URL: https://techblog.comsoc.org/2022/02/23/onfs-private-5g-connected-edge-platform-aether-released-to-open-source/.

[59] *Unlock 5G Value with Open Standards-based COTS Edge Servers*. ADLINK. URL: https://www.adlinktech.com/en/Edge_Server.

[60] *Solution Brief - ADLINK Edge Servers Enable Rapid 5G Open RAN Deployment*. ADLINK. URL: https://www.adlinktech.com/Products/DownloadPublication?ID=1387.

[61] Pavel Mach and Zdenek Becvar. "Mobile edge computing: A survey on architecture and computation offloading". In: *IEEE Commun. Surv. Tut.* 19.3 (2017), pp. 1628–1656.

[62] Yaqiong Liu, Mugen Peng, Guochu Shou, Yudong Chen, and Siyu Chen. "Toward edge intelligence: multiaccess edge computing for 5G and internet of things". In: *IEEE Inter. of Things J.* 7.8 (2020), pp. 6722–6747.

[63] Tarik Taleb, Konstantinos Samdanis, Badr Mada, Hannu Flinck, Sunny Dutta, and Dario Sabella. "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration". In: *IEEE Commun. Surv. Tut.* 19.3 (2017), pp. 1657–1681.

[64] Yehan Ma, Chenyang Lu, Bruno Sinopoli, and Shen Zeng. "Exploring edge computing for multitier industrial control". In: *IEEE Trans. on Comp.-Aided Design of Integr. Circ. and Syst.* 39.11 (2020), pp. 3506–3518.

[65] David Hästbacka, Jari Halme, Laurentiu Barna, Henrikki Hoikka, Henri Pettinen, Martin Larrañaga, Mikael Björkbom, Heikki Mesiä, Antti Jaatinen, and Marko Elo. "Dynamic edge and cloud service integration for industrial iot and production monitoring applications of industrial cyber-physical systems". In: *IEEE Trans. on Indust. Inform.* 18.1 (2021), pp. 498–508.

[66] Fei Tao, Dongming Zhao, Yefa Hu, and Zude Zhou. "Resource service composition and its optimal-selection based on particle swarm optimization in manufacturing grid system". In: *IEEE Trans. on indust. inform.* 4.4 (2008), pp. 315–327.

[67] *TELECOM SECURITY INCIDENTS 2021*. The European Union Agency for Cybersecurity, ENISA. URL: https://www.enisa.europa.eu/publications/telecom-security-incidents-2021.

[68] Gino Carrozzo, M Shuaib Siddiqui, August Betzler, José Bonnet, Gregorio Martinez Perez, Aurora Ramos, and Tejas Subramanya. "AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture". In: *Euro. conf. on netwo. and commun. (EuCNC)*. IEEE. 2020, pp. 254–258.

[69] Alexandros Valantasis, Nikos Psaromanolakis, and Vasileios Theodorou. "Zero-touch security automation mechanisms for edge NFV: the π-Edge approach". In: *18th Inter. Conf. on Netw. and Servi. Manag. (CNSM)*. IEEE. 2022, pp. 317–323.

[70] Redouane Niboucha, Sabra Ben Saad, Adlen Ksentini, and Yacine Challal. "Zero-touch security management for mMTC network slices: DDoS attack detection and mitigation". In: *IEEE Inter. of Things J.* (2022).

[71] Chafika Benzaid and Tarik Taleb. "ZSM security: Threat surface and best practices". In: *IEEE Netw.* 34.3 (2020), pp. 124–133.

[72] Danu Dwi Sanjoyo and Masahiro Mambo. "Accountable Bootstrapping based on Attack Resilient Public Key Infrastructure and Secure Zero Touch Provisioning". In: *IEEE Access* (2022).

[73] Guozhi Lin, Jingguo Ge, and Yulei Wu. "Towards Zero Touch Networks: From the Perspective of Hierarchical Language Systems". In: *IEEE Netw.* (2022).

[74] Imran Ashraf, Yousaf Bin Zikria, Sahil Garg, Yongwan Park, Georges Kaddoum, and Satinder Singh. "Zero Touch Networks to Realize Virtualization: Opportunities, Challenges, and Future Prospects". In: *IEEE Netw.* 36.6 (2022), pp. 251–259. DOI: 10.1109/MNET.001.2200029.

[75] Tingting Wang, Jianqing Li, Wei Wei, Wei Wang, and Kai Fang. "Deep-Learning-Based Weak Electromagnetic Intrusion Detection Method for Zero Touch Networks on Industrial IoT". In: *IEEE Netw.* 36.6 (2022), pp. 236–242. DOI: 10.1109/MNET.001.2100754.

[76] Sabra Ben Saad, Bouziane Brik, and Adlen Ksentini. "A Trust and Explainable Federated Deep Learning Framework in Zero Touch B5G Networks". In: *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. 2022, pp. 1037–1042. DOI: 10.1109/GLOBECOM48099.2022.10001371.

[77] Ismaeel Al Ridhawi, Moayad Aloqaily, Fakhri Karray, Mohsen Guizani, and Merouane Debbah. "Realizing the Tactile Internet through Intelligent Zero Touch Networks". In: *IEEE Netw.* (2022), pp. 1–8. DOI: 10.1109/MNET.117.2200016.

[78] Jani Suomalainen, Arto Juhola, Shahriar Shahabuddin, Aarne Mämmelä, and Ijaz Ahmad. "Machine Learning Threatens 5G Security". In: *IEEE Access* 8 (2020), pp. 190822–190842. DOI: 10.1109/ACCESS.2020.3031966.

[79] Chafika Benzaïd and Tarik Taleb. "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" In: *IEEE Netw.* 34.6 (2020), pp. 140–147. DOI: 10.1109/MNET.011.2000088.

[80] Tianpeng Ye, Gaolei Li, Ijaz Ahmad, Chaofeng Zhang, Xiang Lin, and Jianhua Li. "FLAG: Few-Shot Latent Dirichlet Generative Learning for Semantic-Aware Traffic Detection". In: *IEEE Trans. on Netw. and Serv. Manag.* 19.1 (2022), pp. 73–88. DOI: 10.1109/TNSM.2021.3131266.

[81] Emmanuel A. Oyekanlu, Alexander C. Smith, Windsor P. Thomas, Grethel Mulroy, Dave Hitesh, Matthew Ramsey, David J. Kuhn, Jason D. Mcghinnis, Steven C. Buonavita, Nickolus A. Looper, Mason Ng, Anthony Ng'oma, Weimin Liu, Patrick G. Mcbride, Michael G. Shultz, Craig Cerasi, and Dan Sun. "A Review of Recent Advances in Automated Guided Vehicle Technologies: Integration Challenges and Research Areas for 5G-Based Smart Manufacturing Applications". In: *IEEE Access* 8 (2020), pp. 202312–202353. DOI: 10.1109/ACCESS.2020.3035729.

[82] Sandro Pinto, Tiago Gomes, Jorge Pereira, Jorge Cabral, and Adriano Tavares. "IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices". In: *IEEE Internet Computing* 21.1 (2017), pp. 40–47.

[83] Dalton Cézane Gomes Valadares, Newton Carlos Will, Marco Aurelio Spohn, Danilo Freire de Souza Santos, Angelo Perkusich, and Kyller Costa Gorgonio. "Confidential computing in cloud/fog-based Internet of Things scenarios". In: *Internet of Things* 19 (2022), p. 100543.

AUTHORS

Dr. Ijaz Ahmad is working with VTT Technical Research Centre of Finland, and is an adjunct professor at the University of Oulu, Finland. Dr. Ijaz has been a visiting scientist at the Technical University of Vienna, Austria (2019), at Aalto University Finland (2018), and is the recipient of several awards including the Nokia Foundation, Tauno Tönning and Jorma Ollila grant awards, and the VTT research excellence awards for 2020, 2021, and 2023. Furthermore, Dr. Ijaz has received two best paper awards at IEEE conferences. His research interests include cybersecurity, security of 5G and 6G.

Andrea Gentili received his M.Sc. (Tech.) degree in information and communications engineering at the University of Trento, Italy in 2020. He is currently working with VTT Technical Research Centre of Finland as a research scientist. His research interests include edge computing, video streaming and multipath routing solutions over Wi-Fi and 5G.

Dr. Rupender Singh is working with VTT Technical Research Centre of Finland. He received a Ph.D. degree in wireless communication from the Indian Institute of Technology Roorkee, Roorkee, India, in 2021. Previously, he worked as post-doctoral fellow with Qatar University (2021-2022) and as an assistant professor with the World Institute of Technology, Gurgaon, India (2009-2013). His current research interests include secure 6G networks, terahertz communication, physical layer security, and optical wireless communication.

Juhani Ahonen received his M.Sc.degree from the University of Oulu, Finland, in 1991. He has worked in the telecommunication industry for over 25 years.

Dr. Jani Suomalainen received his M.Sc. (Tech.) degree from Lappeenranta University of Technology, Finland, in 2001 and D.Sc. (Tech.) degree from Aalto University, Finland, in 2022. Since 2000 he has been with VTT Technical Research Centre of Finland in Espoo where he is a senior scientist. Recently, he has been involved in European and Finnish cooperation projects to develop, research, and trial secure next-generation technologies for mobile networks. His research interests include cybersecurity, threat modeling, security architectures, as well as intelligent and active defenses for dynamic and heterogeneous network environments.

Seppo Horsmanheimo received M.Sc. (Tech) degrees from Computer Science department of Michigan Technological University in 1996 and from Information Technology department of Lappeenranta University of Technology in 1997. He is a principal scientist at VTT Technical Research Centre of Finland Ltd working on military, national, and EU funded projects closely related to existing and forthcoming mobile communication and localization solutions applied to critical infrastructures e.g., smart grids, next generation mines, and automated ports. In the NGMining project, he has been involved in design, implementation of 5G proof-of-concept system using joint communication and positioning.

Heikki Keränen received an M.Sc. (Tech) degree from the Networking technology laboratory of Helsinki University of Technology (now Aalto University) in 2006. Heikki has a professional background with varying telecommunication technologies, ranging from mobile operator networks to proprietary private networking over UHF/VHF frequencies. As Head of Technology at Satel, Heikki leads the research of mission-critical connectivity systems and technologies, such as 5G, Wi-Fi Mesh and LEO. In the NGMining project, his research activities focused on 5G and Wi-Fi-enabled vehicle routers and how to achieve maximized reliability, safety, and security for the connectivity in underground mines from the UE point of view.

Erkki Harjula is a tenure-track assistant professor at the CWC-NS research unit, Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu, Finland. He received a D.Sc. degree in 2016, and an M.Sc. degree in 2007 from University of Oulu. Currently he works on wireless system level architectures for future digital healthcare, focusing on intelligent trustworthy distributed computing and communication architectures. He has a background in edge computing, mobile and IoT networks and green computing. He has co-authored more than 90 international peer-reviewed articles. He is also an associate editor of Springer Wireless Networks journal.