IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 4, 2022, accepted May 9, 2022, date of publication May 18, 2022, date of current version May 27, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3176385

A Survey on Trusted Distributed Artificial Intelligence

MUHAMMED AKİF AĞCA[1,2], (Member, IEEE), SÉBASTIEN FAYE[1], (Member, IEEE), AND DJAMEL KHADRAOUI[1], (Member, IEEE)

[1]Luxembourg Institute of Science and Technology (LIST), L-4362 Esch-Sur-Alzette, Luxembourg
[2]Computer Engineering Department, TOBB University of Economics and Technology (TOBB ETU), 06560 Ankara, Turkey

Corresponding author: Muhammed Akif Ağca (akif.agca@etu.edu.tr)

This work was supported in part by the Luxembourg Institute of Science and Technology (LIST) Ph.D. Grant.

ABSTRACT Emerging Artificial Intelligence (AI) systems are revolutionizing computing and data processing approaches with their strong impact on society. Data is processed with automated labelling pipelines rather than providing it as input to the system. The innovative nature increases the overall performance of monitoring/detection/reaction mechanisms for efficient system resource management. However, due to hardware-driven design limitations, networking and trust mechanisms are not flexible and adaptive enough to be able to interact and control the resources dynamically. Novel adaptive software-driven design approaches can enable us to build growing intelligent mechanisms with software-defined networking (SDN) features by virtualizing network functionalities with maximized features. These challenges and critical feature sets have been identified and introduced into this survey with their scientific background for AI systems and growing intelligent mechanisms. Furthermore, obstacles and research challenges between 1950-2021 are explored and discussed with a focus on recent years. The challenges are categorized according to three defined architectural perspectives (central, decentral/autonomous, distributed/hybrid) for emerging trusted distributed AI mechanisms. Therefore, resiliency and robustness can be assured in a dynamic context with an end-to-end Trusted Execution Environment (TEE) for growing intelligent mechanisms and systems. Furthermore, as presented in the paper, the trust measurement, quantification, and justification methodologies on top of Trusted Distributed AI (TDAI) can be applied in emerging distributed systems and their underlying diverse application domains, which will be explored and experimented in our future related works.

INDEX TERMS Trusted AI, distributed systems, software defined networking (SDN), trusted execution environment (TEE).

OUTLINE

The associate editor coordinating the review of this manuscript and approving it for publication was Hiram Ponce.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

I. INTRODUCTION

Intelligent systems are able to adapt to change dynamically in varying contexts by keeping the trustworthiness of a system within the limits of available resources. However, increasing computational and storage capacities require the decentralization of resources and algorithms. Trusted scalability of analytical functions and resources is still an open issue. Large-scale matrices generated by the novel methods, which are used to formally state the data and context, have to be merged and dynamically fused to be able to scale/train [1] the decentralizing algorithms. Furthermore, an increasing number of nodes in the system cause swarm behavior [2]–[4] due to the use of complex computational systems for co-operative missions of autonomous system units. The components utilized to interact with these units are called edge devices, and have densified storage and computational facilities, which enable them to cover broader additional contexts and a wider spectrum. This is a key enhancement for running novel machine-learning algorithms at the edge by ensuring trust and security [5]. Nevertheless, the dynamic context exponentially triggers data/transaction flows in the system. The flows lead recent challenges for intelligence valorization in a dynamic context.

Valorizing the swarm intelligence and keeping the system resilient require real-time updates and predictions in different system layers [6], [7]. Ledger-based chain structures and big-data technologies can accomplish transaction scalability and memory-speed analytic performance to a certain extent. Despite this, mission/safety/operation-critical applications, such as tracking a moving object, monitored by a swarm, require trust to be verified at the critical checkpoints while maintaining the performance of the overall system. Extending data locality to the edge in a trusted scalable manner with holistic views can help to manage the complexity of the data/transaction-flow and maintain the memory speed performance of the total system and analytical transactions [5]. Furthermore, holistic abstraction can maximize the trust factor of the system while enabling trusted scalability of the transactions and keeping the memory speed of large-scale trusted analytics on massive-systems.

Co-operation between these units can be maximized with micro-service architectures, which have innovative approaches for layer-wise structures. Thereby, trust can be verified at critical checkpoints to maximize the targeted throughputs of these units. The approaches can help to dynamically define user feature sets and the management of these features can be enabled at run-time to maximize the performance of the co-operative mission, and the trust factor of a resilient system. Therefore, the system can consider the trust indicators that can give confidence concerning the predictions processed by the distributed AI/ML algorithms at a massive scale by ensuring trusted scalability with the justified features. Thereby, resiliency and robustness can be assured in a dynamic context with an end-to-end Trusted Execution Environment (TEE) for the growing intelligent mechanisms and systems. These critical feature sets are explored in the rest of the paper as components of a distributed computing system with novel trusted distributed AI-driven approaches with a comprehensive scientific background definition. In this way, the trust justification features can be explored and identified for the emerging intelligent systems and mechanisms.

TABLE 1. Keyword definitions.

Trust	- Belief in Reliability, Truth, Ability, Strength, Reliance, Dependence, Faith, and Confidence. - In the computing domain, it is defined as the behavioural integrity of a system, which behaves as expected for all transactions [37,14,15,28].
Distributed System	Set of nodes with decentralized/distributed memory and processing resources, which operates coherently [14,15].
Autonomous System	In a general context, a network or set of networks under one organization. In systems and computing science, it can be defined as a component or a unit, which can operate independently [13,38,15].
Resilient Swarm	Set of fully connected nodes.
Artificial Intelligence - AI	Ability to make the right decision in a mathematically well-defined context.
Smart System	A system with a set of nodes, which can behave intelligently [14,15].

As a main target in this survey, we introduced the concept of **Trusted Distributed AI (TDAI)**, which is the ability to make the right decision in a mathematically well-defined context within the critical, distributed, autonomous system constraints [15]. Main contribution of such benchmarking is to help to understand the new concept of TDAI, with a comprehensive review of the major related contributions in the current literature. So that, we can obtain comprehensive view on emerging AI systems concepts and its' critical components like SDN, TEE etc. Table 1 introduces selected keyword definitions that will be used in the rest of the paper. Section. II introduces the general scientific background and definitions of AI vs Distributed AI and intelligent systems, Section. III introduces related use-case specifications and descriptions, Section. IV includes a comparative analysis of the literature and gives details about the security, privacy, and trust metrics considered in this study, Section. V includes the discussion, current challenges, and a comparative analysis of the literature. Section. VI concludes the paper and introduces future directions.

II. BACKGROUND AND DEFINITIONS

A. DISTRIBUTED SYSTEMS VS TRUSTED DISTRIBUTED SYSTEMS

In order to characterize a distributed system, it is useful to use the **logical functional distribution** of the processing

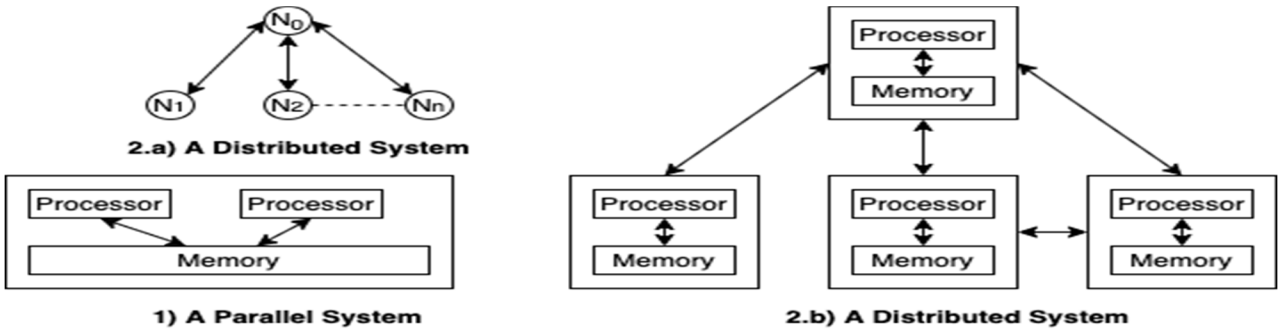

FIGURE 1. Parallel and distributed systems.

capabilities of a given system composed of a set of computers. The logical distribution of such capabilities is based on the following criteria like: Multiple processes, Inter-process communication, Shared memory and Collective goals. Some examples of distributed systems can be related to Peer-to-peer networks, Process control systems, Sensor networks and Grid computing.

The computers in these systems are identified as system units, which are generic components called **nodes**. A distributed system is a system with set of nodes N_i : $\{N_o, N_1, N_2, \ldots, N_n,$, which can operate coherently as a single system. Depending on the memory system design, it is called (1) a parallel system with shared memory resources or (2) a distributed system with decentralized/distributed memory resources in each system node N_i, as illustrated in Figure 1.

The systems can be designed for specific purposes or as **generic mechanisms** for multi-purpose implementations. Examples of this are: (1) Distributed computing system, which can be a cluster computing system or a grid computing system; (2) Distributed information system for a transaction-processing system (mainly database applications) or enterprise applications; and (3) Distributed pervasive systems with mobile and embedded computing devices. This category can include wireless nodes as networking devices for low latency communication, such as emerging 1/2/3/4/5/6G communication and networking technologies [14].

Features for networking and communication technologies and current research challenges for distributed systems will be discussed in Section. IV, but we can already say that emerging communication and networking technologies together with system abstraction approaches enable us to categorize that as a fog layer with novel holistic view approaches [5], with a feedback controller mechanism. Some examples of emerging wireless communication technologies such as 5/6G can be defined as a network component for distributed pervasive systems with a set of interacting nodes $N_i \ldots n$, which have very low latencies for real/near real time critical systems. It is a core mechanism for emerging Software Defined Networking (SDN) and virtualized network functionalities (NFV), as well as for the growing intelligent systems.

The concept of trust is very subjective, having been used by many researchers in many domains for different purposes. The generic definition of trust is as follows:

"trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before [we] can monitor such action (or independently of his capacity of ever to be able to monitor it) and in a context in which it affects [our] own action".

Trust can then be defined as the belief that a rational entity will resist malicious manipulation or that a passionate entity will behave without malicious intent [40].

If we look at the distributed systems from a service point of view, the emerging digital environments and infrastructures, such as distributed security and computing services, have together generated new means of communication, information-sharing, and resource utilization. However, using these distributed services results in the challenge of how to trust service providers to not violate security requirements, whether in isolation or jointly. Answering this question is crucial for designing trusted distributed systems and selecting trusted service providers [41].

When designing distributed systems, trust has to be considered as a major factor in all development stages. Therefore, the trust-based design and development would need a framework to guide system developers towards identifying a set of comprehensive requirements and simultaneously preventing any possible conflicts [42]. These conflicts are observed via layering and logical operations with a multi-layer design principle and paradigm approach, as illustrated in Figure 2, which interacts via data between the layers. Thereby, data can be the key components to track the states and critical knowledge regarding the required framework.

In [5], authors propose the Markov chain Monte Carlo (MCMC) method, which can be analytically considered as an inference problem, i.e. computing the posterior distribution via prior distribution information. Given a dataset $D = \{x_1, x_2, \ldots, x_N\}$, the posterior probability of $P(x^* \mid D)$ for the excess state x^* can be calculated using the Bayesian Rule with a probabilistic distribution. Knowing the probability distribution of the initial state $P(x^0)$ and the transition kernels $T(x^* \leftarrow x)$, the marginal probability of the Markov chain at the specific state x^* is computed dynamically. If the prior states are likely to link to the posterior states, then, the

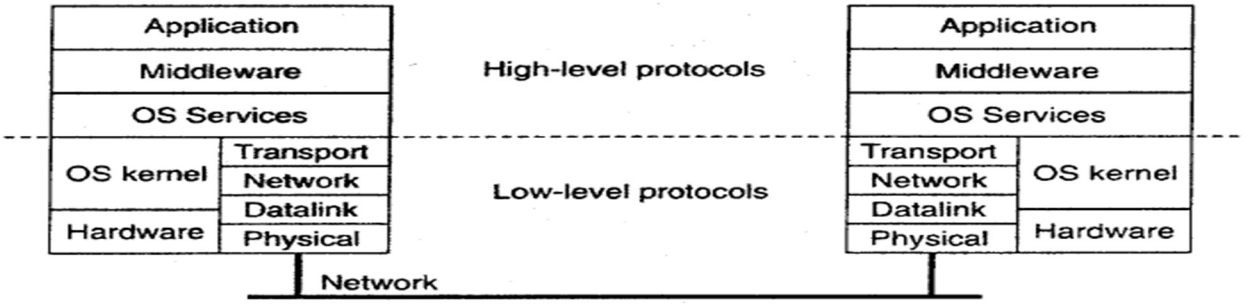

FIGURE 2. Layering and logical operations of a distributed system [14].

Markovian chain is ergodic and converges to an invariant distribution. So that, trust can be transferred between the contexts. This approach can be considered for a dynamic context with a rational agent function to obtain a well-defined context to elaborate on the challenges.

In order to formulate interactions with the environment within the well-defined dynamic context, the behavior of a given node can be described as a dynamic system node in the environment E, which produces a sequence of states or snapshots of that environment. A performance measurement U () evaluates this sequence. Let $V(f, \mathbf{E}, U)$ denote the expected utility according to U () of the agent function f() operating in E{}. Each Environment has a set of nodes, $N_E\{N_1, N_2, N_3, \ldots, N_n\}$ and can be monitored with a set of trusted agents or nodes. Each node can be defined as a trusted agent, which can be defined as system nodes depending on their context. We can identify the rational agent with a function as follows:

$$f_{opt} = arg \max_{f} V(f, \mathbf{E}, U). \tag{1}$$

Throughput of each Node X(N) is monitored via trusted Agent A{} as well as via other nodes N{}. A trusted Agent is formulated as follows:

$$A\{\} = \{iN_i \text{ and with activation function } a_i\}. \tag{2}$$

The goal of the set of agents A{} and nodes N{} is to maximize the expected utility V() of the set of environments E{} by monitoring behaviors with $f_{opt}()$ function via trusted channels. The interactions with the environment and identified trust **justification features** can be observed dynamically with (1) centralized, (2) decentralized and (3) distributed system design paradigms within an architectural design perspective. Thereby, the trust factor of the system, $P(x^*) \propto t$ with the set of nodes; N_E:$\{N_1, N_2, N_3, \ldots, N_n\}$ can be aggregated in order to **maximize** the throughput in the well-defined dynamic context.

The dynamic context and environment in which the set of nodes N_E interacts, require an **optimal** level of trust in the context in order to be able to ensure the interactivity of the nodes and system components. Depending on this level of trust, the system can be identified as a trusted distributed system with the hard constraints of a critical system in real time. This set of features can be mainly identified and measured with dynamic metrics such as the latency, throughput, and power values of the nodes. The values have to be set up accurately for the context dependencies and adapted dynamically to the changing context. Next chapter introduces the background of these AI principles and paradigms with a comparative analysis on centralized and distributed perspectives.

B. CENTRALIZED AI VS DISTRIBUTED AI

Artificial/computational intelligence has been described from many aspects in literature. The main challenge is finding the abstract and numeric definitions of thinking, learning, and intelligence. In this chapter, we will provide the major definitions of machine intelligence, computing, and AI, in order to emphasize the roots of our conceptual and abstract basic definition for trusted AI mechanisms available in the literature. This section articulates and discusses state-of-the-art conceptual definitions of artificial intelligence.

In spite of not having a standard definition for artificial intelligence, most accepted definitions can be categorized into four main groups. (1) behavior, acting humanly; (2) thought processes and reasoning, thinking humanly, cognitive modeling; (3) success measurement respective to human performance, thinking rationally; and (4) the ideal performance measure, rationality; acting rationally is a combination of mathematics and engineering [13]. The remainder of the section briefs on the four main categories and introduces the state-of-the-art definitions. Current challenges will be addressed with a comparative analysis of the state of the art.

The first category is behavior, acting humanly and is initiated by the Turing test approach. Natural language processing methods enable computers to communicate with other computers like humans. A computer passes the test if a human interrogator cannot differentiate whether the sender of the message is a human or machine. Knowledge representation stores heard or known data. Automated reasoning uses stored information to answer questions and inference new conclusions.

Machine learning adapts a system to new contexts and detects/extrapolates patterns. There is no direct physical interaction between the computer and the interrogator, since the physical simulation of a person is unnecessary for intelligence. A video signal is included to test the subject's perceptual abilities and pass physical objects through a hatch.

Computers need computer vision to perceive objects and robotics that manipulate/move objects in order to be able to pass the test. AI researchers prefer studying the underlying principles of intelligence rather than duplicating exemplary scenarios. Therefore, little effort is needed to pass the Turing test.

The second category is the thought processes and reasoning, thinking humanly, cognitive modeling approach. Cognitive science merges computer models from AI and experimental methods from psychology to imitate the human mind. Each field is growing rapidly and fertilizing the other. One of the most popular definitions of intelligence is the ability to adapt to change (Hawking, 1992), which has inspired most AI systems. Neuropsychological evidence supports computer vision to develop innovative computational models. However, the systems used in real life have mission/safety/operational critical system constraints. Rational and formally proven methods are preferred by AI researchers.

The third category is rational thinking, success measurement with respect to human performance. Logicians develop precise notations for statements about all kinds of objects in the world and relationships among them. Logic-based computational reasoning systems are applicable to some extent. However, formalizing and stating informal knowledge in formal terms with uncertainty factors is not an approach that is fully applicable. Furthermore, an insufficient number of facts make the use of problem-solving methods impossible and would exhaust computational resources. Reasoning steps can be added to increase the performance of a computational reasoning system, but it would remain limited due to uncertainty and informal knowledge resources.

The fourth category is the acting rationally, rational agent approach, a combination of mathematics and engineering, based on an ideal performance measure known as rationality. A computer agent operates autonomously, perceives the environment, persists in a defined time period, adapts to change, reasons logically, and generates and pursues goals. A rational agent operates/acts under uncertain conditions to achieve the best expected outcome. All skills are required for the Turing test enable agent to act rationally. Knowledge representation and reasoning skills enable agents to reach good decisions. Comprehensible sentences in natural language need to be generated to communicate with the environment. Continuous learning is needed to improve the ability to generate effective behavior with the agent function $f_{opt}()$. This category of AI can enable us to obtain a mathematically well-defined context to interact with the environment. In this way, we can extend a definition for trust to AI systems as illustrated in Figure 3, where we have a dynamic context and where we see the AI based categories and trust impact. For instance, in IV part of the figure we can have mathematically well-defined context, where we can extend, quantify and qualify the trust with precise definitions of rationality principles.

Based on the comprehensive view of AI system methodologies, we can see that the rational agent approach is preferred by AI researchers. The standard of rationality is mathematically well-defined and completely general. It can enable an agent to be generated for any well-defined context. Achieving perfect rationality and always doing the right thing is not feasible with the uncertainty factors intensive environments. Computational requirements cannot be satisfied in the context. A computer system that has (1) storage, (2) an executive unit, (3) control units does not have to be a central mechanism. Decentralized and distributed system design approaches can enable us to get closer to achieving perfect rationality.

Architectural views and perspectives can be used to differentiate and categorize the features of emerging AI systems. The categories can be named as (1) centralized AI (2) decentralized AI (2) and (3) distributed/hybrid AI.

The centralized approach is not considered feasible with the current state-of-the-art approaches, since the emerging intelligent environments are data-intensive and they have limited agent cooperation interactivity features due to the bandwidth limits of interaction channels. Thereby, the number of nodes in the limited context inflates exponentially. The agent functions $f_{opt}()$ also grow exponentially and the systems exceed the limits of computational scalability [5].

As the second alternative, decentralized design features can help to control the independent nodes with limited capabilities of the autonomous agents, mainly with limited knowledge storing and processing features to make the right decision in uncertainty-intensive contexts and environments. However, decentralized design is also limited due to the capacities of the independent node, which is only feasible for a well-defined limited context.

Fortunately, distributed design paradigms can help to merge critical feature sets of centralized and decentralized design paradigms within a hybrid design approach for cooperation and interaction with the agent function $f_{opt}()$ under uncertainty-intensive conditions. Thereby, we can define the distributed AI as the ability to make the right decision in a mathematically well-defined context within the critical, distributed, autonomous system constraints [15]. The main difference between centralized and distributed approaches is the dynamic data-driven cooperation with a set of nodes; $N_{E:}\{N_1, N_2, N_3, \ldots, N_n\}$ in a set of dynamic environments $E\{\}$ to achieve the expected utility V

As cooperation between the nodes increases, system level trust becomes a more critical requirement to ensure the behavioral integrity of a system. The distributed design approach can enable us to maximize the critical feature sets (memory, storage, processing capacities etc.) of distributed AI/ML algorithms for the intelligent systems and mechanisms targeted. The following chapter discusses these feature sets in a dynamic context, where we introduce the need and increasing interest for Trusted Distributed AI in the literature as the core generic mechanism of the emerging trusted distributed systems. In this way, the agent function $f_{opt}()$ can dynamically control distributed resources to maximize the performance of the expected utility V By this means, the system can cover wider contexts and spectrums with the

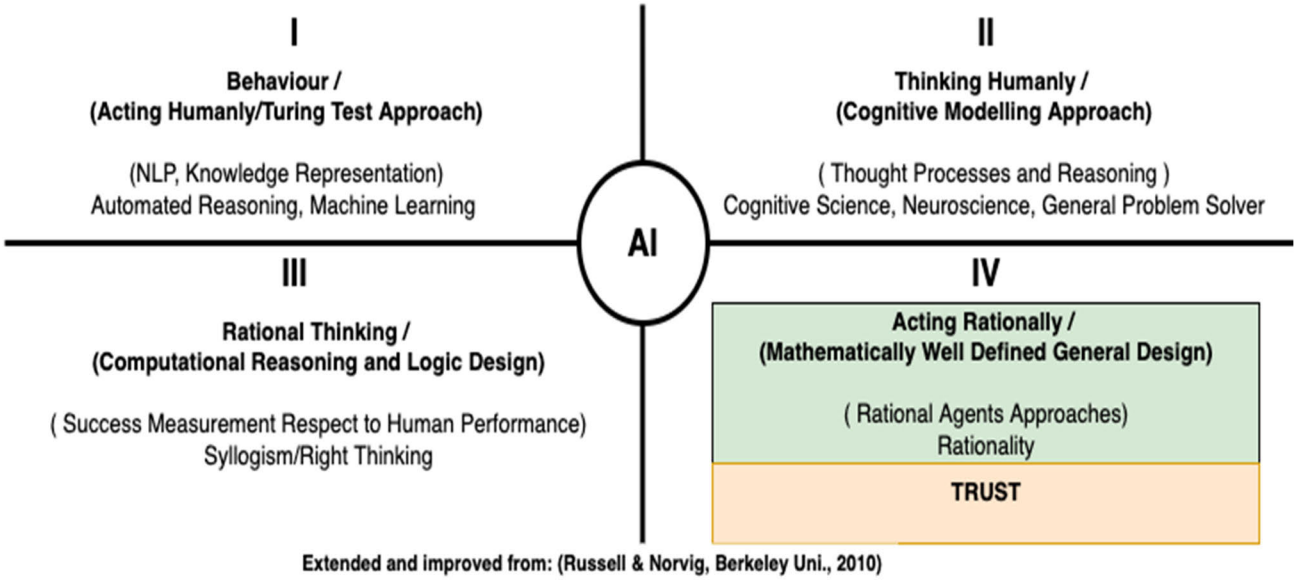

FIGURE 3. Main categories of artificial intelligence.

TABLE 2. Artificial intelligence system state-of-the-art targeted feature summary (✓: Yes, X: No).

ARCHITECTURE	Trust Measurement and Quantification	Trusted Scalability	Trust Assurance	Swarm Manipulation	System and User Behaviour Monitoring
Decentralized (Autonomous/ Embedded/Local)	✗	✗	✗	✗	✓
Centralized/ (Fully connected)	✗	✓	✓	✗	✓ Limited with end-to-end latencies.
Distributed (Edge/Hybrid/Hierarchical/Multi-layer)	✗	✓	✓	✓	✗
Trusted Distributed AI	✓	✓	✓	✓	✓

distributed features of trusted distributed AI, as explained in the next chapter.

C. TRUSTED AI VS TRUSTED DISTRIBUTED AI

In a broader context, Trusted Distributed AI (TDAI) can be defined as the ability to make the right decision in a mathematically well-defined context within the critical, distributed, autonomous system constraints. The constraints can be observed with agent function $f_{opt}()$ to reach ultimate rationality in uncertainty-intensive environments. In order to identify these features, the rest of the section introduces basic definitions of (1) distributed systems, (2) security, privacy, and trust, (3) distributed AI and multi-agent systems, (4) end-to-end paradigms, and swarm mechanisms to maximize cooperation between the agents and thus maximize the performance measure U () in a set of environments E {}.

Table 2 introduces selected critical feature set comparisons between trusted AI and Trusted Distributed AI with the architectural perspectives. The rest of the section explains the key features of TDAI and its advantages with decentral and hybrid design approaches, which enables us to maximize the performance of the agent function $f_{opt}()$ and overall system.

1) SECURITY, PRIVACY, AND TRUST FEATURES

Security, privacy, and trust are the key elements of growing intelligent distributed systems. The scientific principles and paradigms are investigated in all design lifecycles with hardware/software co-design approaches. These features can make systems more flexible and undertake the necessary configurations to tackle the challenges of hardware dependencies.

Scientific views and challenges can be categorized into many perspectives, such as the authors [14] roughly divide the issues of security in a distributed system into two parts. (1) concerns the communication between users or processes, possibly residing on different machines that have

secure communication channel mechanisms. The mechanisms are more specifically designed for authentication, message integrity, and confidentiality. (2) concerns authorization, which deals with ensuring access rights to the resources with an access control mechanism. The mechanism can manage the user access level, system node confidentiality classification, and data protection policies with cryptographic keys and certificates.

In a broader context, the security of a computer system is strongly related to the notion of dependability, which means that the computer system must have justifiable trust to deliver its services. Dependability includes availability, reliability/liability, safety, maintainability, and robustness. Furthermore, recently emerging concepts like anti-fragility can also be a notion of the resilience and dependence of the system. The authors include the confidentiality and integrity of the computer system as a prerequisite of trust.

Confidentiality feature can be ensured by the security mechanisms in some manner with a layered logical and security mechanism. However, the integrity and coherency of the system require holistic views and end-to-end transaction monitoring approaches within the limits of critical system constraints [15]. In this way, alterations and state changes can be detected and rectified in real or near real time at massive scale. By this means, Alice can trust the computer system and interact with Bob via trusted channels in real or near real time. Trust features, metrics, and measurement/quantification approaches will be discussed in detail in Section. IV after the brief background definitions of end-to-end paradigms and swarm mechanism feature sets in the next chapter.

2) END-TO-END PARADIGM AND SWARM MECHANISMS

The data-intensive nature of emerging AI systems and context-dependent programs makes the problem much more complicated due to the increasing complexities of the transactions. Nevertheless, a generalization approach is possible. Distributed caching policies and system abstractions have recently been tested. Performance improvements are observed with distributed file systems and different configurations for memory bottlenecks and congestions as an improvement to the Turing and McCarthy abstraction models [3], [29]. The studies prove that the end-to-end implementations of machine-learning pipelines with modern cloud systems, which have browser-based interface architectures, can be implemented in real time or near real-time. The authors define the diversity of emerging data growth as big data concept. It is 3V (Volume, Variety, Velocity) data, which cannot be processed with classical database systems.

A proof-of-concept study was experimented with basic machine-learning use cases for an opinion-mining application to understand social polarization and convergence features. The proposed distributed file system-based design enables us to overcome the memory bottleneck with a 90% true clustering performance [29] for designed scoring algorithms.

System-level innovations and new conceptual definitions and abstractions have enabled us to develop advanced computational systems to automate many manual processes. Thereby, trusted distributed AI methodologies can be implemented with end-to-end machine learning pipelines and trusted execution of transactions with holistic views to the total system. Baydin *et al.* [1] propose automatic differentiation for machine-learning applications to build end-to-end pipelines. The approach can enable end-to-end machine-learning models/knowledge bases to be merged and trained in different contexts. Emerging AI systems and computational/storage resources can support the end-to-end design of AI systems. Data can be managed and fused with knowledge bases within reasonable latency thresholds for many applications to keep the rationality of the agents in a well-defined dynamic context [30].

Machine learning and statistical techniques can help to transform big data into actionable knowledge with a simple user-interface via an efficient distributed system design approach [2]. End-to-end differentiable pipelining frameworks can support the automatic composition of a learning framework within acceptable latency thresholds [3]. The innovations enable cooperation between diverse contexts for the tasks, and trigger novel trust modeling approaches. Cohen *et al.* [4] propose a multi-agent-based trust model to be able to ensure the expected behaviors of system units. In order to increase cooperation between system-level transactions, swarm-based coherence is proposed as a collective adaptation for swarm intelligence with artificial neural networks [31].

The emerging technologies associated with swarm mechanisms enable trusted distributed AI to be developed, with an increase in processing capacity together with the distribution/decentralization of resources (data units, AI processes, etc.). Real-time management/exploitation of such systems and consideration of them from a holistic point of view becomes much more critical. [5] is an example of holistic system abstraction proposed for end-to-end transaction flow monitoring of trusted AI systems. In addition to this, some research work focuses on transaction management considering the X-AI concepts together with the lineage aspects (data locality and tracking) [32]–[35]. In terms of the development and engineering of AI-based systems, cloud-based lifecycle-based trust modeling and monitoring approaches are also proposed by the authors [8], [9].

As a brief overview to the explored background, the challenges can be categorized into three main architectural design views with a system level perspective. (1) Decentralized (Autonomous/ Embedded/Local) (2) Centralized/ Fully connected (3) Distributed (Edge/Hybrid/Hierarchical/Multi-layer). Within these, the interactivity and cooperation of the agents and dynamic system components can be observed in the dynamic context within a holistic point of view.

The features in the literature targeting trustworthy mechanisms for either centralized AI or Distributed AI can be

summarized as illustrated in Table. 2. These categories and main feature sets can be listed as follows:

- trust measurement, quantification, and justification
- trusted scalability
- trust assurance
- swarm manipulation
- system and user/agent behavior monitoring

From this initial literature survey, we can see that there is little research work that is related to the field of TDAI. Indeed, this research field requires all five key features dedicated to pure distributed AI-driven systems, as mentioned above, to be considered. The next chapter describes the novel feature sets of TDAI with a use-case focus for the growing intelligent systems. Section. IV analyses the literature comparatively with comprehensive tables.

III. USE-CASE SPECIFICATIONS AND DESCRIPTIONS

The scenario targeted in this work is related to mobility use-cases and considers a mix of connected autonomous (SAE level 5) and non- or semi-autonomous vehicles. Each vehicle is deployed with a sensing unit as system node that has a processing and reasoning capability – to process the raw data collected from a vehicle's sensors and subsequently interpret them into useful outcomes of emerging AI systems. In this context, we can imagine a given number of vehicles on the road moving from a starting point to a destination with all vehicles connected to each other and sharing some data measured and/or interpreted locally, using their sensing capabilities, or collaboratively, using each other's knowledge. In such a situation, each node could implement its own AI module to estimate/predict or learn, not only from what has happened in the past, but also from what the other nodes are sharing with it (using its reasoning capability).

We can also assume that for some tasks, a given node might rely on the processing power offered (vs allowed) by a remote node due to the lack of processing power or learning capability of the original node. In other words, vehicles that are not equipped with this AI feature or with a too weak computing capability can potentially rely on other vehicles' modules by using low-latency communication capabilities provided by P2P or cellular communication networks. This can be achieved via a collaboration feature that a distributed system can offer to give all mechanisms for the ability to run in real time. This heterogeneity (in the nature and capacities of vehicles) makes this collaborative approach particularly efficient, allowing a single node to benefit from the overall knowledge and processing capabilities. In such a scenario, we see a double (win/win) benefit, where a local node can profit from neighboring nodes to help make decisions locally and anticipate decisions for the next steps.

The resulting distributed architecture can become complex and may involve self-organizing techniques with multiple hierarchical layers to better manage the decisions between several nodes. A node which might play the role of master would benefit from an overall view for global decision-making. Many applications might be related to this, especially those related to mobile, edge and ubiquitous computing where vehicles are equipped with context-aware and user-centric technologies.

Applications that cover this could be related to driver behavior profiling, with different possible outcomes, like low-emission driving where the user or the car (if fully autonomous) would need to follow precise instructions depending on the way that is driving and, on the environment, (i.e. other vehicles).

One challenge of particular interest is when a mix of fully autonomous and semi-autonomous vehicles are collaborating. This specific scenario involves different behaviors and ways of sending, processing, and reacting to a given situation. This might of course lead to conflicting decisions, with semi-autonomous vehicles, still operated by a driver, sending requests or information that might be badly interpreted by the other vehicles. This type of scenario, when coupled with the complexity of the underlying distributed architecture, can lead to trust issues. This is even more true when AI algorithms are distributed over several disparate entities, since one of them may misinterpret an outcome interpreted by another vehicle. Another possible scenario is a complementary mobility application being related to an emergency where an ambulance can process data (related to early medical diagnosis) of the patient being transported, to be transmitted in real time before arriving at the hospital. In such a case, a patient's mobile device (e.g., smartphone or smartwatch) could be used for such a transmission via a roadside unit node (like a 5G edge node), which is utilized for transmitting the packets to the destination.

This process involves low latency and a high quality of service, as well as cooperation. Sometimes, it might indeed occur that we rely on such a node to request ad hoc computation if an edge node (hospital edge node) is not available or not trusted anymore. In such a scenario, the main challenge is ensuring that the actors in the value chain trust the services at the top of such a distributed system since they mainly rely on AI systems capabilities: sensing, processing and reasoning features. In other words, what are the measurable trust indicators that can be considered to gauge confidence and correlate with trust in the overall services offered by such a distributed system?

Looking at the trusted conceptual background provided by the literature, we can already specify the following key trust indicators that are specific to the distributed nature of a given intelligent and growing system:

- AI and the underlying distribution/architecture (versus organization) of its analytics functions: local learning (like in centralized systems), federated learning (like in distributed systems), etc.
- Processing over the nodes: processing power and organization within the distributed system
- Reputation of the distributed nodes, meaning how can we exclude any of the nodes if the overall reputation is degraded and how can we detect such a failure?

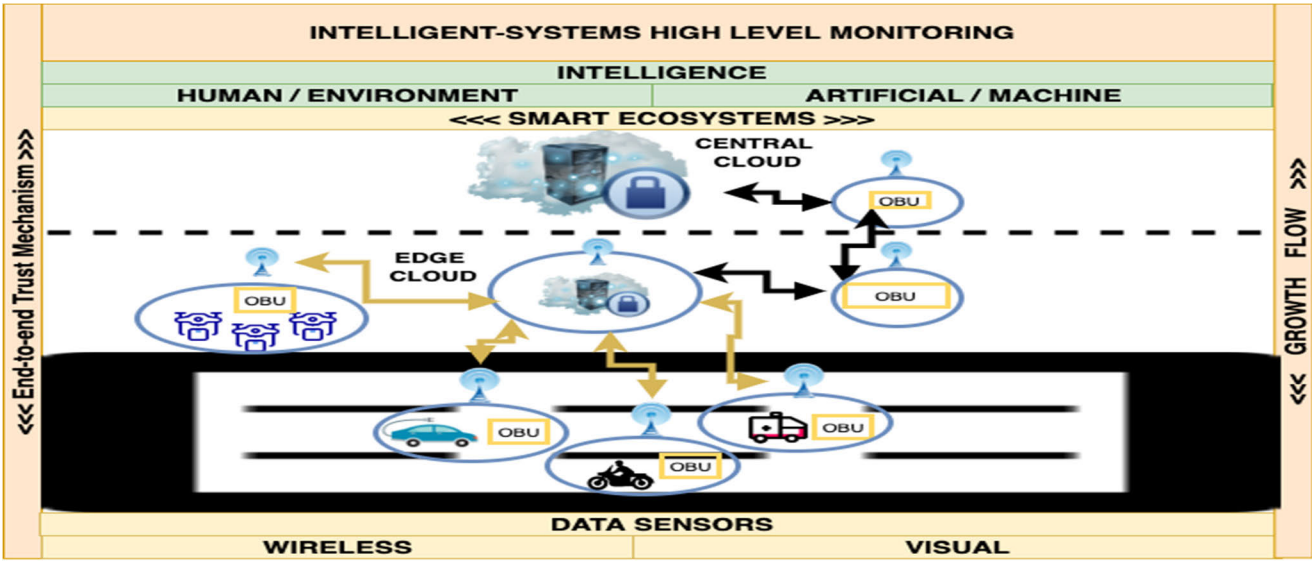

FIGURE 4. Intelligent system intelligence flow mechanism.

- Impact assessment of the overall trust value at both the node and global level.
- Measure/quantify/justify the trust factor coefficient of each node and the context dynamically in different time spans by observing the throughput levels expected for them.

All these indicators may require simulation tasks to understand and measure the ability of a distributed system solution to solve complex (near) real-time mobility problems compared to conventional centralized approaches. Figure 4 illustrates an intelligence flow mechanism in this dynamic context, in which the learning and growth is correlated with an end-to-end trust mechanism. Thereby, the high-level monitoring dashboards of intelligent systems can have a holistic view of the growing mechanisms in a dynamic context. The next chapter comparatively analyses the state of the art for the identified principles and paradigms and introduces the emerging challenges and potentials in detail.

IV. COMPARATIVE ANALYSIS OF LITERATURE

A. AI SYSTEM CATEGORIZATION

Continuously growing intelligent systems can enable massive-scale AI support for many critical systems. However, challenges also increase, mainly in terms of complexity, inflation of size/volume, reaching limits of resource centralization, and an increased need for decentralized/distributed mechanisms due to non-deterministic alterations and uncertainties in system components. In this chapter, we will discuss related studies, which categorize the challenges and introduce the main features to be targeted for a trusted distributed AI methodology as a core mechanism of growing intelligent systems.

Data is the most valuable digital dynamic asset of the intelligent systems. Since computing machines have existed, the most interesting challenge has been to tackle the computational complexities in a timely manner and access the system resources with the right credentials. [42] Proper identifies the current state of the data as fuel for the digital age. Business analytics, statistics-based AI, digital twins, etc. are defined as ''data-hungry'' applications, which are components of complex systems, and which can be thought of as data ecosystems. The research challenges below are defined as the main categories:

- Data as a key resource
- Trust at the core
- Regulation of data ecosystems
- Data need semantics
- From data to information

The challenges within the identified categories can help define the role of data in the current context of smart systems. However, data is not fully separated concern from computation, it has to be mapped to computation. Trust has to be measured and quantified. Novel holistic system abstractions are required to track the transaction flow at the system level and to assign trust values to each category. Furthermore, semantic web-based ontology modeling approaches with RDF (Resource Description Framework, Subject-Predicate-Object) [43], [44], scenario-based strategy planning tools [45], or any other system design tools can help to model a lifecycle with a conceptual modeling perspective to better interact with intelligent system components at run time or (near) real time. Thereby, explainability and justifiability features with socio-dynamical perspectives can also be tracked more coherently to contribute to the continuous growth of the emerging intelligent mechanisms.

Within the digital-dynamics perspective, system-level end-to-end transaction monitoring can be succeeded by a holistic view [5], which enables data-state and lineage tracking in a trusted manner with a robust core mechanism. System-level trust features, metrics, and measurement approaches will be

discussed later in this chapter to indicate the justification of trust prerequisites, such as robustness, reliability/liability, resiliency, and integrity.

The digitization of everyday life, cause the amount of data to grow exponentially, and the challenges emerging from this have made the need for system reconfigurability more critical. Hardware-dependent designs are replaced with software-driven mechanism and hardware/software co-design approaches are utilized when necessary. The software-driven approaches also adapted the software challenges to the current intelligent system context with software-intensive mechanisms. Aksit [46] has summarized these challenges/research directions into six categories with a focus on smart-city systems and presents them in a single list as briefed below;

1. Developing models for smart cities;
2. Designing a framework for managing and optimizing the configurations of clusters;
3. Designing models, methods and tools for critical infrastructures;
4. Optimizing the necessary quality attributes through system adaptation at run-time;
5. Integrating software systems;
6. Designing a smart infrastructure with a high degree of interoperability, configurability, adaptability, and evolvability.

The challenges can help to synchronize coherency between the related research studies. However, new software and hardware co-design principles are emerging. System-level hardware/software integrated views, which can interact with all verticals at run-times, are required for emerging smart city systems. Trust is not only required for dependability, which already ensures the security, robustness, resilience, integrity, and coherency of a system [46], but must be measured and quantified for smart systems, in order to inspire confidence in system architectural level disruptive innovations.

The next chapters will identify these architectural design differences to emphasize the need for distributed design and the potential benefits of hybrid mechanisms. Thereby, we will be able to introduce the methodology to be used for the concept of SDN to ensure the interactivity of trusted agents in near/real-time for smart systems. Hybrid approaches also define a core mechanism for emerging networking/communication methodologies for close-to-long-range systems as the generic IT core, which can be implemented in emerging software intensive systems, such as 5/6G. In order to be able to focus the identified features on the TDAI, these system-level paradigms can be categorized as architectural (1) and (2) networking/communication perspectives. Thereby, we can obtain the trust justification features of novel computing systems with a focus on distributed computing concerns for the targeted trust frameworks. Rest of the section introduces these identified system-level features and explains them as the trust-justification features of emerging AI systems.

1) ARCHITECTURE

Architectural modeling and the models are the basic methodology and critical feature for system-design paradigms. These are mainly considered with hardware and software-level design concerns. The approaches can be limited to board-level architecture-design paradigms for computing and intelligent system mechanisms [47]. Chip-level designs can enable us to implement computing facilities on any system components as an integrated unit, such as edge devices and mobile units. However, increasing amounts of the data manipulated by the systems require major updates of the hardware and software abstraction principles.

Existing approaches can enable us to process and manipulate data with virtualization and caching policies [48]. Chip-level interconnection [49] mechanisms can enable us to transfer the data between the processes with available scheduling policies [50]. These design approaches are limited with 3D-Stack board/memory design principles [51] and network interconnection issues [52], such as scalability, performance, energy consumptions, and most of all, with bandwidths of the transmission and buffering channels.

Emerging intelligent computing architectures [53] can enable us to process and manipulate data with more intelligent approaches. For instance, caching performances [54] can be optimized and streaming buffers can be designed more coherently and adaptively [55] to interact more efficiently with the system components. The interactions can be designed with online approaches with an event-based trigger mechanism [55] with data-center networking [56] protocols. The architectural concerns can be modeled as generic core mechanisms with the holistic abstraction and end-to-end system design paradigms with throughput maximization approaches [5].

Interactions with the environment and the dynamic state changes of the components also trigger behavioral complexities. These require the dynamic modeling of system view points and snapshots of the states, and can be succeeded by available system engineering architectural frameworks [57] up to the specific requirements of the dynamic context changes. In addition, business processes can also be modeled conceptually [58] to interact more efficiently with the environment. Therefore, system resource modeling and management paradigms can be improved with novel learning heuristics [59]. Furthermore, system resource-management knowledge bases can be trained for continuous growth and the heuristics can be improved with holistic abstraction [5] paradigms. These architectural features can be categorized into three main groups with centralized (fully connected), decentralized (autonomous/embedded/local), and distributed (edge/hybrid/hierarchical/multi-layer) system design approaches.

- **Centralized/**(Fully connected)**:** Processing and memory resources are fully centralized

Centralized architecture can enable to build smart systems with intelligent mechanisms, which have centralized

processing and memory/storage components. Furthermore, robust networking/communication channel-based abilities are supported with strong back-end units, such as quantum computing mechanism, to interact with the environment and dynamic context efficiently. However, these architectural design paradigms are limited by system integration and performance issues [60]. Fortunately, parallelizable portions of these issues can be identified with trust factor maximization principles, and integrity concerns can be minimized with holistic interfaces [61], and holistic total system throughput maximization methodologies [5]. Nevertheless, the design/manufacturing costs and physical limits of these designs require decentralized and distributed approaches, which are explained briefly in the next chapters.

- **Decentral/**(Autonomous/Embedded/Local): Processing and memory resources are fully de-centralized

The decentralization of the mechanisms requires trusted computing units [37] on edge devices and secure channels for trusted interactions with the environment. The trust constraints can be ensured to a certain extent, but the edge/mobile components are limited by digital design paradigms and require novel holistic interfaces [61]. 3D-stack digital design technologies can help to improve edge/mobile units as densified system components [15], [62]. These features can dynamically adapt to the context changes with the holistic interface's digital design approaches [61] and end-to-end holistic abstraction and views [5], [14]. Thereby, the available features of edge/mobile devices can be maximized with densified design paradigms, and the overall system performance can be improved with a distributed design approach. Next chapter introduces the basics of distributed design and details are discussed in a comparative matrix in Section. IV C.

- **Distributed/**(Edge/Hybrid/Hierarchical/Multi-layer): Processing and memory resources are distributed

Distributed system design issues can be grouped into (1) algorithm-level and (2) system-level concerns with a focus on distributed computing [14] principles and paradigms. Algorithm-level challenges include learning paradigms with statistical and AI/ML optimization approaches, such as learning cardinality estimator performance maximization [63] with a flow loss model, a source code compiler to minimize algorithmic complexities [64], and other AI/ML challenges to automate the data pipelines of training and test data-sets [65]. One of the most critical concerns of these challenges, estimator performance maximization, can be improved with holistic abstraction paradigms, which can enable the dynamic training of multi-layer data models [5].

However, increasing complexities and uncertainties of the algorithms trigger more system-level concerns and require computational tractability of the processes and transactions. For instance, critical database ACID (Atomicity, Consistency, Integrity, Durability) features need to be extended to edge devices in a trusted, scalable manner [5]. These challenges require updates in logic design and hardware level updates within the polynomial time threshold values

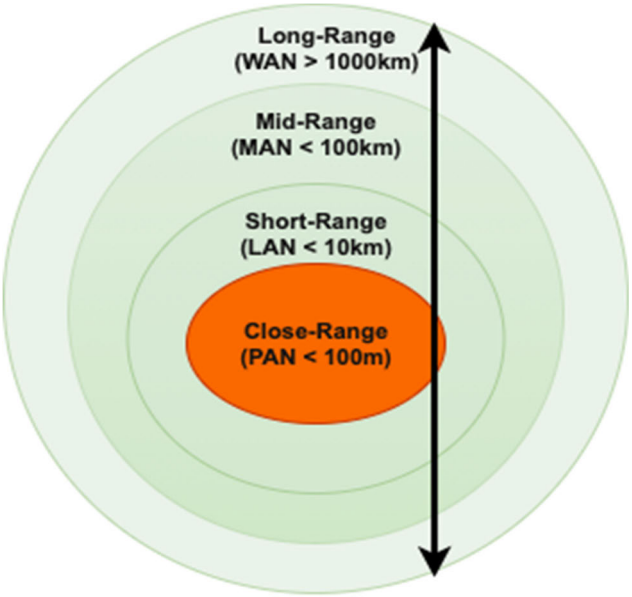

FIGURE 5. Networking and communication systems range-based categorization.

to minimize latency concerns [66]. Holistic interfaces can help to design reconfigurable hardware with a dynamic end-to-end logic structure [61]. However, middleware design paradigms are also critical for software/hardware co-design issues [5], [62]. Fortunately, rational verification methods in polynomial time [66] can help to improve the transaction flow to enable the computational tractability of the processes.

Behavioral strategies of these mechanisms can also be dynamically configured [67] to improve the intelligence mechanism of the intelligent systems. Therefore, AI systems can be improved with novel methodologies, so that we are able to mention trust on these systems, which have more opportunities and challenges than ML features [68], due to their behavioral integrity constraints [5], [62]. Intelligent agents [69] are key components for these intelligently behaving smart systems, and trust measurement and maximization with swarming approaches are promising indicators and features of these paradigms [15]. Comparative analysis matrix in Section. IV B summarizes potential research directions. Discussions in the next chapter will be limited to networking and communication perspectives in order to observe the methodologies that can maximize critical features of an intelligent system with the set of nodes $N_i : \{N_o, N_1, N_2, \ldots, N_n,$, such as connectivity and interactivity paradigms.

2) NETWORKING AND COMMUNICATION

As the emerging technologies grow faster, intersections between the fields are also increasing and multi-disciplinary fields are converging with AI systems-driven design paradigms. For example, networking and communication technologies are improved, with the critical features of emerging AI systems and novel functionalities are being enabled with software-driven design paradigms, such as NFV (Network Function Virtualization) and SDN (Software

	Sub-6 GHz	mmWave (30 – 100 GHz)	sub-THz and THz (0.1 – 10 THz)
Distance	High range	Medium to short range ($\leq$ 200 m)	Short range ($\leq$ 20 m)
Bandwidth	Limited	Medium to Large	Large
Data rates	Limited	Medium to High (up to 10 Gbps)	High (up to 100 Gbps)
Interference	Mitigated by techniques like OFDM and OFDMA	Mitigated by beamforming	Mitigated by sharp pencil beamforming
Noise source	Thermal noise	Thermal noise	Molecular absorption noise and Thermal noise
Blockage	Not susceptible	Susceptible	Highly susceptible
Beamforming	Medium to narrow beams	Narrow beams	Very narrow neams
Horizons to explore	Expanding the midband coverage	NLoS communications and long-range sensing functions	Reliable and low latency communications, integrated sensing and communication systems
Viable architectures	Massive MIMO	Ultra massive MIMO, RIS, and UAV-RIS	Cell-free massive MIMO and holographic intelligent surfaces
Significant caveats	Low rates and spectrum inefficient	Susceptibility to mobility and blockages	Susceptibility to micro-mobility, orientation, air composition and blockages
Applications	Low-rate and latency tolerant services	Vehicular networks, radar, UAVs, and IoT	XR, holography, IoE, NTNs, sensing, and nanosensors

FIGURE 6. Advance wireless communication systems emerging features [72].

Defined Networking). In this way, emerging networking and communication technologies like 5/6G technologies can enable massive-scale AI System deployments to be implemented with novel hardware/software codesign paradigms, and the challenges can be explored with AI systems perspectives. The rest of the section explores these critical features with a range-based categorization approach as illustrated in Figure 5.

Networking and communication features, which trigger growth acceleration in the computing paradigms and the densified computing/storage system units, can enable distributed massive data to be processed in real time and help to ensure the connectivity and interactivity of the components within the critical system constraints. These features, which are the key enablers for the SDN mechanisms with virtualized network functionalities, are called NFV. Thereby, the connected mechanisms can help to design software-driven dynamic systems rather than hardware-dependent designs to make the networking and communication systems flexible and adaptive to dynamic context changes. In doing this, the critical networking and communication components of emerging technologies can enable us to ensure the interactivity of the agents within hybrid-cloud mechanisms [49] and Radio-Network technologies, which have multi-layer design with network slicing features [56].

Standard definitions are still on progress of improving signal transmission and edge/mobile processing latencies to meet the critical system constraints [57]. In spite of making good progress with these challenges, distributed computing and system design paradigms [14], [15] still need to be investigated and tested with the critical feature sets of the emerging networking and communication systems. These features are mainly categorized into two groups: (1) beamforming and signal transmission and (2) edge/mobile processing mechanism for networking mechanisms and systems. Figure 6 [72] illustrates the basic characteristics of wireless features, with GHz frequencies and advanced emerging features, which are mmWave and THz waveforms. These signal transmission abilities can help to improve the interactivity of system nodes and edge/mobile units within the limits of total system throughput principles and paradigms [5]. Furthermore, available networking protocols and mechanisms can enable the transmission and processing of [86] packages with multi-layer connectivity paradigms, as illustrated in Figure 7. Transmission latencies and edge/mobile package processing features are promising for ensuring the interactivity and connectivity of an intelligent system with a set of nodes N_i : $\{N_o, N_1, N_2, \ldots, N_n,$. Detailed features are discussed with a focus on end-to-end trust mechanism justification features and indicators. In this chapter, we will limit the discussion to critical networking and communication features with a range-based categorization approach as illustrated in Figure 5, consist of (1) Close (2) short (3) mid (4) long ranges.

- **Close-Range (PAN $<$ 100m):** Bluetooth, Wi-Fi, 802.11p/ITS G5 for V2X, low latency networks etc.

An increasing number of networking and communication technologies can provide a wide variety of options for the connectivity and interactivity maximization of the system nodes and edge/mobile units. However, the growth and diversity of options increase complexity and trigger behavioral anomalies, which require (near)-real-time channel selection mechanisms.

Fortunately, intelligent control mechanisms can enable us to design vision-based control mechanisms [87] or hybrid controllers with a wireless/visual sensor-based [5] control structure inside the edge/mobile units. These challenges trigger the requirement for novel synchronization and concurrency features [88] at the edge/mobile units. Networking and

Name	Category	Special Mechanisms
E2E	end-to-end	standard TCP-Reno
E2E-NEWRENO	end-to-end	TCP-NewReno
E2E-SMART	end-to-end	SMART-based selective acks
E2E-IETF-SACK	end-to-end	IETF selective acks
E2E-ELN	end-to-end	Explicit Loss Notification (ELN)
E2E-ELN-RXMT	end-to-end	ELN with retransmit on first dupack
LL	link-layer	none
LL-TCP-AWARE	link-layer	duplicate ack suppression
LL-SMART	link-layer	SMART-based selective acks
LL-SMART-TCP-AWARE	link-layer	SMART and duplicate ack suppression
SPLIT	split-connection	none
SPLIT-SMART	split-connection	SMART-based wireless connection

FIGURE 7. Networking protocols for package transmission [98].

communication services can also be adapted to the dynamic internet/intranet [89] applications. Energy efficiency of these nodes is also a critical feature for the available wireless/wired communication channels and required wireless communication protocols [90], and wireless sensor network architectures [91] can be adapted to change dynamically. These features can be designed as open-flow mechanisms [92] for a selected region, and adaptive protocols [93] can help to process packages and disseminate information in edge/mobile units with a distributed design approach [93]. Multi-layer topologies [94], such as MAC 802.11 ad hoc protocols, can be maintained dynamically to adapt the physical layers at run-time.

The resiliency of overlay networks [95] is also a critical concern for the edge/mobile device surface [96] signal processing abilities within the critical system constraints. Thereby, advances in edge/mobile device features and abilities like ultrasonic ranging hardware [97], congestion controller mechanisms [98], miniaturized beamforming devices [99] can operate and help to ensure the interactivity and connectivity of the components with ms-scale latency values [100]. On the other hand, these advanced features require hardware-level code management challenges with context-aware computing paradigms. Fortunately, this adaptiveness can be improved with Machine Inferred Code Similarity (MISIM) systems [101], which can be part of a future research challenge in terms of the run-time reconfigurability of the systems. In order to limit discussions on close-range communication in terms of end-to-end trust mechanism and justification features, the rest of the section will only mention short-to-long range paradigms briefly and will focus on the identified trusted computing feature sets.

- **Short-Range (LAN < 10km):** Cellular networks, 4G/LTE, 5G NR etc.

Short-range feature sets and end-to-end networking/ communication mechanisms can maximize the connectivity and interactivity of the system components and edge/mobile units in real/near-real time. Figure 7 illustrates these protocol categories, which include link-layer and end-to-end connectivity features. These features need to be extended to short-range cover, especially for smart-city use cases. For instance, emerging mobility technologies like autonomous cars can behave like a mobile computer device, which can help to implement urban air transport with the cars having a dual functionality as mobile computers.

Connectivity and interactivity of these mobile units can be ensured with emerging systems and methods in order to obtain [102] telematic data with wireless/wired sensor tags. These protocols can be adapted dynamically to the dynamic context changes as explained in the previous section. The discussions can be limited to the V2X (vehicle to everything) domain to explain the most promising feature sets. For instance, ITS-G5 (IEEE 802.11p) and C-V2X (3GPP Release 14) are promising technologies in terms of sampling/transmission frequencies and power/energy efficiencies [103] with minimized congestion and latency values. Nice progress is saved with 5G hybrid-mechanisms [85], which are supported by hybrid clouds with maximized bandwidth limits to exceed theoretical thresholds like Edholm's law of bandwidth [81]. Distributed computing paradigms are still under investigation to maximize the total system throughput values of the system [5] with novel AI/ML supported designs [6], [32]. These feature sets will be summarized in Section. IV C. The rest of the section briefs on mid/long-range challenges and potential future research directions.

- **Mid-Range (MAN < 100km)**: High Speed Wireless Internet, cable TV systems

As the amount of data traffic increases to the peta/exa-scale, controller mechanisms become more complicated and require advanced intelligent controllers inside edge/mobile devices with distributed mechanisms to be able to cover

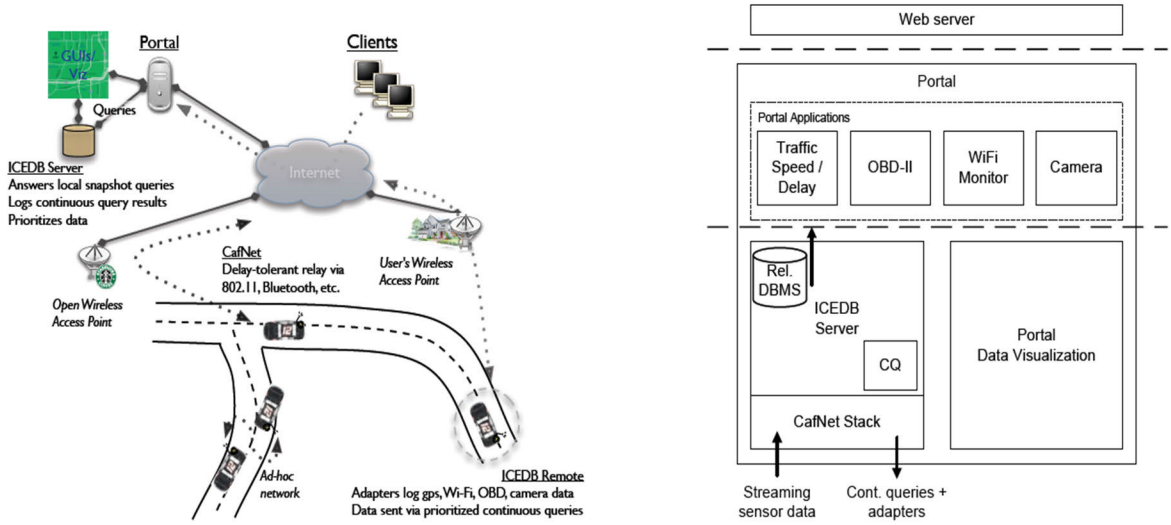

FIGURE 8. A distributed mobile sensor computing system [12].

wider ranges. The diversity of the components and interaction require advanced package processing features and real-time decision mechanisms. Fortunately, the state-of-the art methodologies can enable distributed sensor computing systems, as illustrated in Figure 8. [12]. The detailed feature sets of these mechanisms are explained in the next chapter with a focus on the end-to-end trust features of computing principles and paradigms. As a brief introduction, these features can cover on-board computing units with mobile/edge query processing mechanisms. Therefore, dynamic measurement metrics can be collected to help to ensure the connectivity and interactivity of mobile units with maximized trust values, as explained in the next chapter, as advanced feature sets of the trust mechanism to be able to extend networking and communication features to mid-range.

- **Long-Range (WAN > 1000 km)**: Space Networks, Sat Com, Space Internet, Futuristic (Drones, Low-Orbit Satellite etc.)

The growth in communication technologies and signal transmission features can enable us to reach higher signal frequency transmission features up to PHz scales. Futuristic components of the emerging smart systems, which have higher bandwidths, can ensure the connectivity and interactivity of the components at massive scale within continental scope and low-mid-high orbit space systems. These innovative space missions can cover space internet, space aircrafts, and other advanced high-throughput connectivity mechanisms like 6G and InfiniBand optical systems. These advanced radio signals and mm-to-ultraviolet frequencies are illustrated in Figure 9 [72].

Swarming and end-to-end trust mechanisms can help to maximize the throughput of each node and the total system within the critical system constraints [15] with novel AI-supported distributed computing system designs as the core mechanisms. Main characteristics of these features are summarized in Section. V.B within the detailed comparative features matrix. Figure 5 illustrates the categorization of these emerging networking and communication technologies with a range-based classification approach. Advanced communication and future networking systems will be considered in future related works. In this survey, the focus is on distributed computing paradigms and principles of emerging intelligent systems.

3) TRUST: END-TO-END TRUST MECHANISM JUSTIFICATION FEATURES AND INDICATORS

Trust paradigms are widely explored in technical and human science disciplines. Since our focus is on technical concerns with distributed computing scientific paradigms and communities, the categorization and futures are selected from the computing perspectives of a system with a set of nodes $N_i : \{N_o, N_1, N_2, \ldots, N_n,$. In this way, the continuous growth acceleration of an intelligent system can be maximized with dynamic feedback structures [5]. These justification features can be categorized into four main groups: (1) Performance, (2) Run-time monitoring, (3) Security, and (4) Test-based features and indicators. This chapter will explain these justification features by using a selection of the main related studies in the literature.

a: PERFORMANCE

Performance elements are the key metrics for the justification features and defined trust indicators. These can be measured, quantified, and monitored from many perspectives. In order to focus the indicators on distributed computing domains and improve the feedback control structure of the generic mechanism, we can address and focus mainly on the scalability, elasticity, connectivity, and energy efficiency features of the nodes and total system.

Thereby, the rationality and performance features of AI/ML methodologies can adapt to the dynamic context [13] and (near) real-time threshold constraints, and ensure the interactivity of mobile agents. This chapter explains the

identified performance elements of these trust justification features.

a. **Scalability, Elasticity, and Connectivity Limits:** Total number of nodes and users in the system

The scalability, elasticity, and connectivity features of a node can be identified as basic features of the performance-measuring approaches in system sciences. These are measured with number of nodes, users, data volume, and other system/algorithm level computational scalability limit metrics [5]. The approach has been widely applied with AI methodologies, such as distributed AI and multi-agents in many industries. For example, telecommunication systems became data intensive and improved with scalable system design paradigms [16]. Thanks to the advances in data-processing technologies, these features can be queried in real time and correlated with knowledge bases of the systems with dynamic holistic views [15]. The challenges will be discussed with a comparative feature analysis matrix in the next chapter.

b. **Energy Efficiency:** Average energy consumption of nodes and critical transactions

Dynamic management of system resources and physical capacity features requires both hardware and the physical layer monitoring of the units in real time. Energy efficiency average consumption value is the key capacity metric for the interactivity features of the mobile agents for the required power constraints. A novel system abstraction approach can enable the physical layer parameter/metric monitoring to be extended to ensure interactivity and adaptivity in near or near real-time [5].

c. **Energy Efficiency:** Average EMF (v/m), SAR(w/kg), Power(W) environment friendliness

Emerging networking/communication systems like 5/6G can enable the implementation of novel features of the AI methodologies, such as real-time massive scale analytics. However, this triggers risks pertaining to human health, include cancer, COVID-19, etc. [73], [74]. These challenges can be mainly identified and are rooted in EMF, SAR, and the power features of the nodes. In order to be able to justify trust in a dynamic context, these features have to be monitored in real time with the local/global regulative constraints. Thanks to the holistic view [5] of innovations in emerging computational ecosystems, this can also be achieved within the regulative constraints and it is discussed in the next chapter.

b: RUN-TIME MONITORING

In order to be able to maintain overall performance; dynamically justified trust features, the growth progress of the systems, and other trust indicators have to be monitored continuously. Active and passive systems have different constraints and limits, which trigger diverse challenges in distributed computing paradigms. AI methodology approaches can be improved to satisfy the need of the active system constraints at run-time with dynamic approaches. Trust features and indicators can be guaranteed for machine-learning systems [18] and distributed AI techniques [8]. Programming approaches like probabilistic/concurrent [20], dynamic/differential [1], [18] can enable knowledge bases and data states to be updated at run-time coherently. Therefore, the justification features can be trained and updated dynamically for a continuously growing mechanism. We focus these challenges on distributed computing and caching policies in the next chapter discussions. This chapter is a brief on data-state tracking/transitions for an efficient end-to-end feature embedding/manipulation mechanism of a running system.

a. **Data-flow monitoring:** Data state monitoring between applications

Data is the fuel and most valuable asset for the emerging intelligent systems [42]. It is the critical element of the justification features to ensure the integrity of the mechanisms and systems. Each state-change has to be tracked and manipulated during the whole lifecycle of the data. Emerging AI technologies can improve data challenges [30] with novel end-to-end paradigms and scientific improvements in the field. Improved ML systems can also help to improve knowledge bases and are dynamically generated up to data-state dependencies [2]. However, the training process is not only required for data states, it also has to be mapped to the pipelining [3] and feedback mechanisms of system nodes with trust indicators [4]. The features that can help to justify trust are discussed in the comparative matrix table in Chapter 4. B.

b. **Transaction-Flow Monitoring**: Transaction lifecycle monitoring

The diversity and heterogeneity of the emerging systems require decentralized and distributed designs to be able to ensure the growth of the mechanism [30]. Distributed computing paradigms are core features for managing the resources and mapping the data and computation where necessary. Swarm intelligence techniques at the algorithm and system levels can help to resolve the challenges and complexities that trigger swarm behavior in emerging intelligent systems [2]. Novel designs for control structures and abstraction hierarchies [5] can help to embed trust justification features and ensure continuous growth with the necessary updates at runtime with real-time threshold values. Thereby, transaction life-cycle can be monitored dynamically and failures can be recovered with minimum latency via the feedback controllers and holistic views. These features will be discussed in the next chapter.

c. **Trust Monitoring**: Periodical trust verification

Technical and human science concerns around trust modeling are critical paradigms and features for the justification mechanisms. Our focus will be on technical concerns of trust with distributed computing principles and paradigm challenges. In order to improve the quality attributes with user-level measurement metrics, we can consider the regulative aspects of the trust issues. Emerging trends like explainability features [32] can provide growth acceleration metrics, and these can be improved with lineage-tracking features [15]. Furthermore, these features are strongly dependent on the

secure execution of the monitored transactions. In [118], authors explored and improved hardware-based SEE (Secure Execution) with a Trusted Execution Environment (TEE) concept. Storage and user interfaces are identified as critical features and compared with some of the available technologies like ARM TrustZone-based TEEs.

However, these features have (near)real time interactivity constraints with diverse system components. For this reason, hardware isolation and separated kernels are far from achieving these latency, interactivity and scalability thresholds. Fortunately, dynamic holistic views can help to maximize the trusted scalability of the emerging AI Systems [28,29]. Additionally, holistic abstraction paradigms [5] can also help to measure and quantify trust with a trust factor coefficient-based throughput maximization approach as an extension to Amdahl's notation. Thereby, trust can also be verified periodically with the identified trust justification features. From a system-level perspective, the trustworthiness features of AI/ML principles [6], [7], [8], [33], [34], [36] can be interpreted as basic structures of feedback and other mechanical/digital control loops for the growing mechanisms [5]. Furthermore, the uncertainty of the harsh conditions [75] can also be measured and quantified at run-time as calibration metrics [15].

In order to obtain measurable and quantifiable metrics for trust concerns, we will keep the focus on regulative features, such as EMF/SAR/power values for health-care limits, privacy of data etc. with local/global perspectives [10], [76], [77]. These are the critical metrics of the massive-AI system justification features for real-time alerting and risk prediction algorithms [6].

Risk predictions can also improve the scalability limits of large-scale optimization algorithms [10] at run time [5]. Therefore, trust performance and node regulative constraint thresholds can be justified and can help to improve the growth of the mechanism by ensuring the behavioral integrity of the total system. Next chapter summarizes and discusses the scope of the technical concerns with trust measurement and quantification perspectives in distributed computing paradigms with AI/ML pipelining features of growing intelligent systems.

d. AI/ML Pipelining: Dynamic knowledge base monitoring and update

Dynamic contexts, in which mobile agents and system components interact, require real-time updates in different system layers, data models, and most critically, knowledge bases for critical decision-support mechanisms. In order to be able to justify the trust features and indicators, interactivity of mobile agents has to be ensured with distributed computing paradigms and challenges. System acceleration units and algorithm level improvements can be designed for these purposes [11]. In order to be able to manage the system resources dynamically for the changing context parameters, AI/ML pipelining mechanisms can be designed [78] with novel digital control structures [79]. Swarming approaches are also useful for mission-critical constraints of the growing smart systems. Resiliency, robustness, durability, locality, and anti-fragility features [5], [80] are critical features of the trust justification mechanisms for the trusted computing units [37], which are explained in the next chapter.

e. Run-time feature embedding and interaction: Data fetching at run-time to knowledge bases

Previous sections introduced background information on the intelligent-system growth mechanisms. Some additional advanced system features can be explored in terms of trust justification features with technical concerns with a focus on distributed computing paradigms. Sensor-based approaches with wireless/visual detection/actuation interactors are promising for dynamic and fully-automated/autonomous designs. Detected features can be integrated within the limits of current networking/communication technologies [81]. Dynamic heuristics [82] and knowledge bases can be trained dynamically with critical-system constraints of massive AI systems [15]. Multi-layer neural networks and tree structures with different data structures can improve the interactivity and performance of training [119], [120].

Other critical feature sets like data poisoning, backdoor attack can also be monitored to improve the data collection process of training transactions [121]. The features can be extracted dynamically within the critical data sets like fingerprint images and can be embedded into other knowledge bases and used for critical missions like spoof detection [122]. Furthermore, privacy-preserving deep learning models with homomorphic encryption and chain structures can be designed. However, these feature definitions and interactions are limited due to computational scalability and critical system design constraints [5]. Emerging hybrid-cloud and distributed computing design paradigms can help to maximize total system throughputs in order to handle the limitations in a trusted scalable manner [29], [117]. The challenges and future directions will be summarized in a comparative analysis matrix in Section. IV B.

c: SECURITY

Security is also a critical system constraint for the justifiable trust features. Security concerns for distributed computing paradigms cover a wide scope from physical protection to digital security mechanisms. The trust features can be justified with digital security design principles for any system with the set of nodes $N_i : \{N_o, N_1, N_2, \ldots, N_n,$. Therefore, we can limit the scope to digital security concerns. Justifiable trust features can be ensured by improving system thinking paradigms [83] and artificially intelligent cyber-security mechanisms [84]. Adaptive protocols for dynamic contexts with checksum verification-based approaches can justify the trust features and indicators [5] dynamically. Next chapter will discuss the details of these features and future challenges. In this section, we will introduce the basic principles of context awareness and trusted computing paradigms.

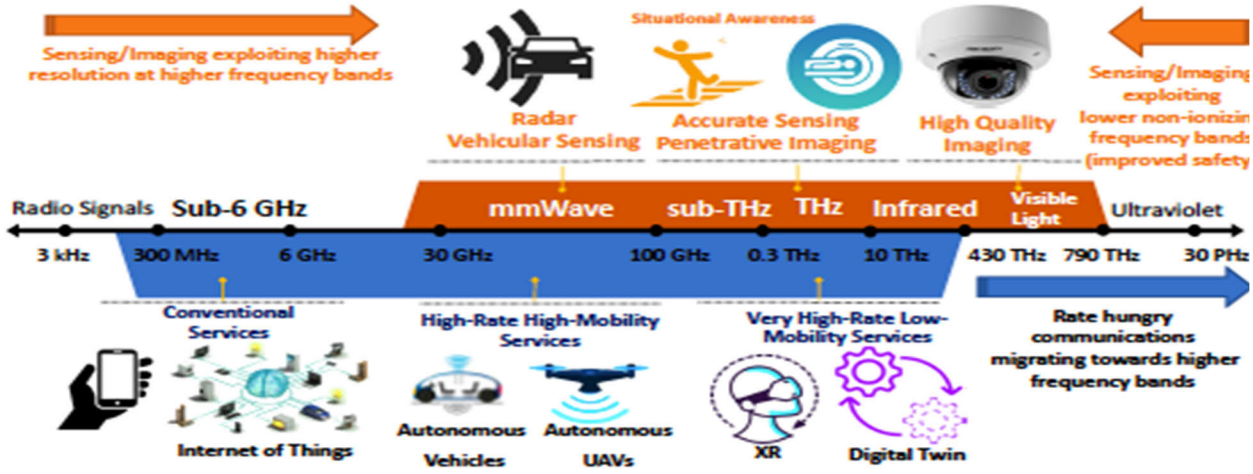

FIGURE 9. Frequency spectrum paradigm shift by communication and sensing features (3 kHz–30 PHz) [72].

a. Context aware dynamic adaptiveness: Event-based secure connection policies and protocols

Context change detection/actuation and correlation extraction between the system resource allocation abilities are increased with the capacity improvements of computing technologies. Event-based abstraction approaches can adapt to change and reconfigure the required trust justification features with the available policies and protocols [5]. Context-aware computing paradigms can distribute computing and process/extract the required features at the edge or on mobile units [27] with trusted computing mechanisms [37]. Furthermore, the bandwidth limitations of communication systems can also be made trusted with secure channels/interfaces [81], [85] and the interactivity of agents and nodes can be ensured for continuous growth [15]. Next chapter introduces checkpoint and verification approaches based feature for dynamic context change.

b. Context aware dynamic adaptiveness: Dynamic package check-sum verification

Thanks to the growth of distributed computing mechanisms, transaction flows can be verified at available checkpoints with dynamic package monitoring approaches to extract the required metric with sets of justification features. Package checksum verification approaches can verify the integrity check mechanism [5], and this can be applied to generic IT core mechanisms with end-to-end paradigms [15]. By that means, targeted justification features of the related context can be extracted dynamically within the edge units and merged the transaction flows at (near)-real-time. Therefore, we can rely on and limit the scope to package check-sum verification approaches to justify the defined trust features, which are summarized and discussed in the comparative matrix in Chapter 4. B.

d: TEST

Testing is also a de facto component for the system design lifecycle. Continuous testing mechanisms (black box, white box, grey box etc.) can detect anomalies and future risks with digital twins of the system units for continuous growth-assurance paradigms. Performance metrics are the key elements of trust justification features for both technical and human-level trust justification features. Behavioral anomaly detection/reaction-based monitoring approaches can detect/recover potential risks within the critical system design constraints [80]. Therefore, we can limit the testing scope to verification and confidence-building approaches.

a. Verification (survey, benchmarking, expert): Formal verification with regulative and technical standards

Verification mechanisms are part of the holistic system lifecycle for distributed computing paradigms. These challenges can be defined and categorized as software engineering [46] paradigms with system design perspectives. Therefore, the necessary quality attributes can be defined/tracked/monitored as performance indicators. In order to make the approaches dynamic and adaptive to changing contexts, we can limit the scope to check-point controller and feedback mechanism principles for continuous growth assurance concerns. Detailed features are summarized in the next chapters with the comparative matrix tables. Rest of the chapter briefs about the selected trust justification features of the testing and verification mechanisms of the growing intelligent systems.

i. Dynamic check-point locating with feedback controllers and optimization: End-to-end holistic checkpoint structures

Improvements in the distributed computing can enable packages to be processed at the edge or using mobile units as discussed in previous sections. Feedback controllers can be correlated with the total system performance and each system unit's throughput values can be correlated dynamically with the behavioral anomalies for feature extraction/detection/reaction mechanisms [5]. Novel structures and holistic abstraction approaches can be implemented on the edge devices and used to build end-to-end TEE. Dynamic

optimizers can be merged as critical supplementary components with respect to the context dependencies.

Therefore, the system can ensure growth acceleration and improve the performances of the mobile units and agents with the trust justification mechanism via the holistic views, which provides dynamic feedback for the continuous growth of an intelligent system. Critical feature sets are summarized within the comparative matrix in Table. 3. B.

ii. **Resiliency and robustness monitoring with holistic views and feedback controllers:** Data-driven dynamic control structures for monitoring mechanisms

User-level concerns are also critical metrics for the trust justification features at the technical and human/socio-dynamics levels. Resiliency and robustness features can be tracked with semantic or graph-modeling approaches, which are used to represent and visualize [43], [44] the correlations between the entities. These features can be named and generalized as conceptual modeling [42] and monitored with a holistic end-to-end trust mechanism [15] as part of the generic IT core structure. Thereby, it can used to monitor regulative constraints in related contexts to observe the identified thresholds and improve train sets of alerting mechanisms.

These features can be improved with scenario-based strategy planning paradigms [45]. Therefore, trust justification features can ensure the acceleration of the growth of the system with the monitored performance indicators and quality attributes of resiliency and robustness features with dynamic controllers and testing operations/processes. Table. 3 gives a summary of the identified features and emerging challenges to ensure the continuous growth of the intelligent systems.

b. **Confidence-Building:** Trust and confidence measurement/quantification in intelligent systems

Trust can be defined as the behavioral integrity of a system, that is, the system behaves as expected at all times, in computing paradigms and sciences [37]. Human/socio-dynamics level concerns can be limited to regulative legal metrics with IT audit paradigms. Socio-dynamical visions can help us to understand changing requirements and contexts dynamically and provide continuous feedback on the defined/monitored trust justification features to accelerate the growth progress of the intelligent systems.

Building confidence in these systems also requires critical constraint feature predictions and forecasts for potential anomalies. This level of confidence can be maximized with strategy planning and a vision of the future cases and predictions about the states of the contexts [45]. Therefore, the trusted mechanisms can keep learning and accelerate growth continuously with an increasing confidence in the total system. Regulative legal constraints are dependent on the digital dynamic operation context and socio-dynamic regulation within the client context. This field is a future possible direction and challenge in our research. Next chapter will elaborate on the user-level monitoring metrics, which can be identified as critical system threshold values of the alerting mechanisms. So that, user-oriented critical alerts can be minimized and confidence can be built with maximum level. Next chapter briefs about these metrics/parameters.

c. **User-level continuous trust measurement**: Facial expressions/body language, behavioral anomalies

In order to retain the validity of the metrics for trust measurement mechanisms in distributed computing paradigms, these justification features can be improved with novel indicators, such as facial expressions, body language or any other human-level behavioral anomalies that can be correlated as sensor units of opinion-mining algorithms [29]. Therefore, the impacts of socio-dynamical changes can provide dynamic feedback to the control loops of growth mechanisms via trusted channels [29], and the interactivity of the mobile units can be maximized with minimum latencies and fault penalties with a dynamic holistic view [5]. These features are observed dynamically with respect to the identified regulative legal constraints of the targeted context.

Regulation mechanisms are also disrupted by growth acceleration and the diverse structure of emerging intelligent systems. Real-time alerting mechanisms are required in daily life also be able to observe socio-dynamic changes and make dynamic alerts for the critical risks in the observed context. Mathematically well-defined structures can enable us to implement swarming approaches within the agent functions $f_{opt}()$ and maximize the cooperation between the exponentially increasing number of components and exa-scale data resources [15]. Thereby, measurable metrics of the regulative legal constraints of observed subject matter can be visualized within the high-level monitoring dashboards of the intelligent systems within the intelligence-flow mechanisms. Figure 4 visualizes the correlation between the end-to-end trust mechanism and growth-flow structure, which can enable to build dynamic intelligence flow within regulative legal constraints of the observed context. Thereby, trust can be quantified with respect to dynamic legal metrics of the socio-dynamic metrics and parameters. This field is also a research domain will be investigated in related future works, in this survey we will keep focus on behavioral anomaly observations of the observed context.

On the other hand, data processing capabilities are still limited by edge device processing limitations and the latency values of these units. Fortunately, the current state regulatory standards define the critical constraints, which are emissions, power limits, and other critical factors. These have an impact on our health and can be monitored and extracted as trust justification features in real time or near real time via the alerting mechanisms. Nevertheless, massive scale deployment is still limited with scalability concerns at the algorithm and system levels [5]. These include critical risks for human health and environmental concerns. These features are also part of the future research directions. Table. 3 summarizes major concerns and identifies critical feature sets of trust justification features to be able to maximize trust in emerging intelligent systems and minimize socio-dynamic risks within the identified regulatory legal constraints.

B. COMPARATIVE MATRIX

TABLE 3. A. Related works. B. Trust justification features.

(a)

#	Type, Year, Authors	Impacts	Shortcomings
1	**Survey, 2018, Baydin et al., Oxford et al.**	Automatic differentiation is proposed for machine-learning applications to build end-to-end pipelines.	Limited evaluation of dynamic computational graphs and differentiable programming. Computational scalability considerations are missing.
2	**Method, 2013, Kraska et al., Brown Uni. et al.**	Support for machine learning and statistical techniques with a distributed system design view and novel data management features.	Limited evaluation of data management, networking, and distributed system design basics.
3	**Method, 2017, Milutinovic et al., Berkeley et al.**	End-to-end differentiable pipelining frameworks are proposed for ML frameworks.	Results are not presented with a proof-of-concept trial.
4	**Method, 2019, Cohen et al., University of Waterloo**	Trust modeling in multi-agent systems is proposed for trust assurance in AI systems.	Limited definition of trust and trust modeling metrics at system level.
5	**Method, 2019, Agca, TOBB ETU**	Holistic system abstraction is proposed for the end-to-end transaction flow monitoring of trusted AI systems.	Proof-of-concept test systems to be tested on larger scales and in different contexts.
6	**Method, 2020, Nassar et al., American University of Beirut et al.**	Blockchain structures and smart contracts are proposed for explainable and trustworthy AI.	Limited file system and caching policy evaluation. Theoretical system design and computational scalability indicators are missing.
7	**Method, 2020, Kumar et al., University of Helsinki, Finland et al.**	Trust issues for AI systems and smart-city use cases explored.	Limited system architecture and networking feature evaluations.
8	**Method, 2019, Hummer et al., IBM Research**	A framework is proposed for end-to-end AI Lifecycle management with a DevOps focus.	Limited system abstraction definition. Trust measurement and quantification is missing. Application layer perspectives are used for system design concepts like feedback mechanisms.
9	**Survey, 2020, Fernández et al., UPC-BarcelonaTech et al.**	Research directions identified for AI Models on Trustworthy Autonomous Systems.	Limited SOTA review and description of identified keywords. System verticals are not explored; limited application layer level DevOps design issues are identified.
10	**Survey, 2018, Bottou et al., Facebook AI Research et al.**	A comprehensive review for large-scale optimization methods for machine learning is provided.	Limited benchmarking and computational scalability evaluations.
11	**Method, 2017, Lee et al., University of California, Berkeley et al.**	An acceleration framework for increasing the performance of distributed machine learning algorithms is proposed. Noises, such as straggler nodes, system failures, or communication bottlenecks are identified and elaborated with coding theory techniques to provide resiliency in different engineering contexts.	Limited benchmarking and computational scalability/performance evaluations.
12	**Method, 2006, Hull et al., MIT**	A distributed mobile sensor computing system is proposed for the cars to dynamically process data at massive scale.	Scalability and trust mechanisms are not investigated.
13	**Survey, 2010, Russel & Norvig, Berkeley**	Full-breadth definition of AI as a scientific field.	Limited evaluation for networking and trust aspects.
14	**Survey, 2014,Steen& Tanenbaum, University of Twente et al.**	Full-breadth definition of Distributed Systems and Distributed Computing Principles and Paradigms.	Limited evaluation for networking, trust measurement/quantification and end-to-end paradigms.
15	**Method, 2020, Agca et al., LIST**	Key challenges for swarm intelligence mechanisms are identified as computing, communication, and control. In order to ensure resilience against manipulation threats, the other parts of the contribution concern end-to-end trust mechanism (integrated view of the three pillars: networking, processing/optimization, and security) and swarm controller methods guaranteeing safety, which aims to enable the trusted scalability of the swarm systems. It introduces CCAM Connected Cooperative, Autonomous Mobility) business-use cases.	Limited discussion of the results of the proposed methodology and proof-of-concept - POC implementations.
16	**Method, 1993 Velthuijsen, PTT Research**	Distributed AI usage in telecommunication is implemented.	Limited results and evaluation.
17	**Survey, 1997, Stone & Veloso, CMU**	ML potential applications to DAI and Multi-Agent systems are proposed.	Limited use cases and evaluations.
18	**Survey, 2019, Toreini et al., Newcastle Uni.**	Trust review for AI and ML studies.	Limited evaluation of ML and AI Systems.
19	**Method, 1992, Marsh, University of Stirling**	Formal definition and evaluation of trust for distributed AI.	Limited evaluation of AI methodologies and system perspectives.
20	**Method, 1999, Agha $ Jamali, MIT**	Concurrent programming paradigm based on multi-agent system actor model abstraction is proposed for DAI.	Limited context definition for distributed agent interactions.
	Other Related and Selected Studies		
30	**Survey, 2019, Gadepally et al., MIT**	Comprehensive view of AI systems and available and future technologies.	Limited system abstraction definitions and literature review of AI methodologies.
31	**Book, 2001, Russell, Computelligence LLC**	Emphasizes swarm-based coherence as collective adaptation for swarm intelligence with artificial neural networks.	Limited system design and scheduling metrics evaluation.

TABLE 3. *(Continued.)* **A. Related works. B. Trust justification features.**

32	**Survey, 2019, Xu et al., Lenovo Research et al.**	Explainability features of AI systems are explored with a neural network focus.	Limited evaluation of system abstraction hierarchies.
33	**Method, 2020, Wing, Columbia University**	Formal definitions of trust and relations between trusted computing and trustworthy AI are explored.	Limited evaluation of SOTA for the proposed concept.
34	**Survey, 2018, Sileno et al. University of Amsterdam, Netherlands et al.**	Emphasizes norm ware with computational artefacts to deal with trust and explainability problems.	Limited norm definition and trust modeling.
75	**Method, 2020, Tomsett et al., IBM Research et al.**	Interpretability and uncertainty of AI systems are identified for a trust calibration framework.	Limited AI methodology categorization and trust modeling to measure and quantify it in AI systems.
76	**Method, 2019, Smuha, KU Leuven, Belgium**	High-level governance framework is proposed for trustworthy AI systems.	System-level standard definitions and feasibility evaluations are missing. Trust measurement and quantification approaches are not evaluated.
104	**Method, 2016, Scherer, Harvard**	Regulative framework is proposed for AI systems.	Technical standard definitions and literature review is missing.
78	**Survey, 2019, Alsamhi et al., School of Aerospace Engineering, Tsinghua University, Beijing, China et al.**	AI methods are reviewed for robot teaming and human cooperation methodologies.	Limited categorization of AI methodologies and data management for swarm systems.
38	**Book, 2010 Golnaraghi et al., Simon Fraser University, Canada et al.**	Basics of automatic control systems are explained in detail. Feedback mechanisms for distributed systems are defined.	Limited evaluation of intelligent systems' actuator and sensor architectures. Data-intensive design and decentralization of computational resource evaluations are missing.
105	**Survey, 2004, Truskowski et al., NASA**	AI techniques are proposed for challenges of mission-critical autonomous software. Novel abstraction paradigms are identified as a requirement for reducing the complexity of swarm systems. The heterogenous structure of emerging intelligent swarms is identified as a challenge for system behavior monitoring and verification.	Trust measurement/quantification, computational scalability evaluations are missing; which are basic and fundamental requirements for critical systems.
80	**Survey, 2004, Rouff et al., NASA**	Formal methods and techniques are explored for the verification, validation, and assurance of future swarm-based missions, such as the ANTS (Autonomous Nano Technology Swarm) mission. It has 1,000 autonomous robotic agents designed to cooperate in asteroid exploration.	Context-aware computational paradigms and real-time data management/fetching features are not evaluated.
82	**Method, 2020, Machovec et al., Colorado State University, USA et al.**	Dynamic heuristics for surveillance mission scheduling with UAVs in heterogeneous environments are proposed. Real-time thresholds are targeted for critical-missions.	Computational load and feasibility evaluations for on-board UAV tasks are missing.
85	**Survey Report, 2021, Stuckman et al., EU Commission**	The main contributions of 5G projects are summarized as of 2021.	Limited evaluation for AI systems use-cases. System abstraction standard definition and benchmarking results are missing.
83	**Method, 2020, Crowder et al., Colorado Engineering Inc. et al.**	A system-level thinking process is proposed for AI systems.	Data-flow mapping with a computational transaction is missing. The categorization of AI agents has no mathematically well-defined context. Proof of concept experimentation is not provided.
84	**Method, 2020, Carbone et al., Forcepoint Global Governments and Critical Infrastructure LLC et al.**	A comprehensive transdisciplinary approach is proposed, which includes Axiomatic Design (AD), AI/ML techniques and Information Theoretic Methods (ITM), in order to reduce risks and complexity by improving cyber system adaptiveness, enhancing cyber system learning, and increasing cyber system predictions and insight potential.	System design theoretical design limitations are not included. Trust measurement and quantification is not identified, which is a fundamental concern for the proposed concept.
85	**Method, 2020, Crowder et al., Colorado Engineering Inc. et al.**	Concepts and notional architectures are presented for the Big Data Analytical Process (BDAP), in order to facilitate real-time cognition-based information discovery, decomposition, reduction, normalization, encoding, memory recall (knowledge construction), and decision-making for big data systems.	Limited evaluation of AI methodologies, feedback structures, and data-flow process and definition.
42	**Survey and Method, 2020, Proper, Luxembourg Institute of Science and Technology (LIST)**	Business analytics, statistics-based AI, digital twins, etc., are defined as "data hungry" application components of complex systems, which can be thought of as data ecosystems.	Data is not fully separated from computation, it has to be mapped to computation. Trust has to be measured and quantified. Novel holistic system abstractions are required to track transaction flows at the system level and to assign trust values to each one.
46	**Survey, 2020, Aksit, TOBB ETU, Ankara, TURKEY**	Software engineering challenges for smart-city systems are categorized. 1- Developing models for smart cities; 2- Designing a framework for managing and optimizing the configuration of clusters; 3- Designing models, methods, and tools for critical infrastructures; 4- Optimizing the necessary quality attributes through system adaptation at run-time; 5- Integrating software systems;	Software and hardware co-design principles are emerging. System level hardware/software integrated views are required, which interact with all verticals at run-time. Trust is not only about dependability. It also has to be measured and quantified for smart systems in order to inspire confidence.

TABLE 3. *(Continued.)* **A. Related works. B. Trust justification features.**

		6- Designing a smart infrastructure with a high degree of interoperability, configurability, adaptability, and evolvability.	
27	**Survey, 2013, Perera et al., Information and Communication Centre, Australia**	Context awareness is surveyed from an IoT perspective, which includes techniques, methods, models, functionalities, systems, applications, and middleware solutions. Growth progress of context-aware computing from desktop applications, web applications, mobile computing, and pervasive/ubiquitous computing concerning the Internet of Things (IoT) is explained.	Limited evaluation for distributed caching and memory management. The computational scalability of the emerging complex systems is not evaluated with system throughput limitations.
37	**Method, 2009, Martin et al., University of Oxford**	Trusted computing, trusted platforms, and trusted systems are defined as the system components, which behave as expected.	Limited definition for data caching, trust measurement, and computational scalability issues.
81	**Survey, 2004, Cherry, Northwestern University, USA**	The throughput data rates of communication technologies correlated with Moore's law and Edholm's law of bandwidth.	Limited evaluation for computational scalability and system throughput limitations.
116	**Survey, 2020, Reuther et al., MIT, USA**	AI/ML accelerators with end-to-end approaches are summarized. Vector engines, dataflow engines, neuromorphic designs, flash-based analog memory processing, and photonic based processing approaches are discussed.	Limited evaluation for middleware categories and trusted scalability concerns.
117	**Method, 2021, Samsi et al., MIT, USA**	Modern AI/ML workloads are categorized, and limitations of HPC systems are explained. SuperCloud hybrid mechanisms are introduced with recent data sets.	End-to-end trust mechanisms and holistic abstraction paradigms are not considered. Limited evaluation for middleware components.

(b)

#	AI				Architecture			Networking				Trust																				
	Behavior/ (Acting Humanly/Turing Test Approach): NLP, Knowledge Representation, Automated Reasoning, Machine Learning Learning	**Thought Processes and Reasoning / (Thinking Humanly/ Cognitive Modeling Approach):** Cognitive Science, Neuroscience, General Problem Solver	**Rational Thinking/ (Success Measurement Respect to Human Performance):** Syllogism/Right Thinking, Computational Reasoning and Logic Design	**Acting Rationally / (Rational Agent Approaches):** Rationality/ Mathematically Well-Defined General Design	**Centralized/ (Fully connected):** Processing and memory resources are fully centralized	**Decentral/ (Autonomous/ Embedded/Local):** Processing and memory resources are fully decentralized	**Distributed/ (Edge/Hybrid/Hierarchical/Multi-layer):** Processing and memory resources are distributed	**Close-Range (PAN < 100m):** Bluetooth, Wi-Fi, 802.11p/ITS G5 for V2X, low latency networks, etc.	**Short-Range (LAN < 10km):** Cellular networks, 4G/LTE, 5G NR, etc.	**Mid-Range (MAN < 100km):** Global networks, High Speed Wireless Internet, cable TV systems, etc.	**Long-Range (WAN > 1000 km):** Space Networks, Sat Com, Space Internet, Futuristic (Drones, Low-Orbit) Satellite etc.)	**Performance**	**Scalability, Elasticity and Connectivity Limits** Total number of nodes and users in the system	**Energy Efficiency** - Average energy consumption of nodes and transactions - EMF (v/m), SAR(w/kg), Power(W) environmental friendliness	**Run-Time Monitoring**	**Data- flow monitoring:** Data-state monitoring between applications	**Transaction-Flow Monitoring:** Transaction lifecycle monitoring	**Trust Monitoring:** Periodical trust verification	**AI/ML Pipelining:** Dynamic knowledge-based monitoring and update	**Run-time feature embedding and interaction:** Data fetching at run-time to knowledgebases at run-time	**Security**	**Context-aware dynamic adaptiveness:** - Event-based secure connection policies and protocols	**Context-aware dynamic adaptiveness:** - Dynamic Package checksum verification	**Test**	**Verification (survey, benchmarking, expert):** - Dynamic check-point locating with feedback controllers and optimization - Resiliency, reliability, dependability, and robustness monitoring with holistic views and feedback controllers	**Confidence Building:** - Trust and confidence measurement/quantification in smart systems	**User-level continuous trust measurement:** Face mimics/body language, behavioral anomalies
	Denominators: Distributed computing/caching, differential/probabilistic/dynamic programming																															
	✓: YES **X: NO** **? : NOT INDICATED**																															
1	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	✓	X	✓	X		X	X		X	X	X
2	✓	X	X	X	X	X	✓	?	?	?	?		✓	X		✓	X	X	X	✓		X	X		X	X	✓
3	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	X	X	✓	X		X	X		X	X	X
4	✓	X	X	✓	?	?	?	?	?	?	?		X	X		X	X	✓	X	X		X	X		X	✓	✓
5	✓	X	X	✓	X	X	✓	✓	✓	X	X		✓	✓		✓	✓	✓	✓	X		✓	✓		✓	✓	X
6	✓	X	X	✓	✓	X	✓	?	?	?	?		X	X		X	✓	X	✓	X		X	X		X	X	✓
7	✓	X	X	X	?	?	?	?	?	?	?		X	X		✓	✓	X	X	X		X	X		X	X	✓
8	✓	X	X	X	?	?	?	?	?	?	?		✓	X		✓	✓	X	✓	✓		✓	✓		X	✓	✓
9	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	✓	✓	X	X		✓	✓		✓	X	✓
10	✓	X	X	X	✓	X	✓	?	?	?	?		✓	X		X	X	X	✓	X		X	X		X	X	X
11	✓	X	X	X	✓	X	✓	✓	✓	X	X		✓	✓		✓	✓	✓	✓	✓		✓	✓		X	X	X
12	✓	X	X	X	X	X	✓	X	✓	X	X		X	X		✓	X	X	X	X		X	✓		X	X	X
13	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	✓	X	✓	X		X	X		X	X	X
14	X	X	✓	✓	✓	✓	✓	✓	✓	✓	✓		X	X		✓	X	X	X	X		✓	✓		✓	X	X
15	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	X		✓	✓	✓	✓	✓		✓	✓		✓	✓	X
16	X	X	X	✓	X	✓	✓	?	✓	✓	?		X	X		X	X	X	X	✓		X	X		X	X	X
17	✓	X	X	✓	X	X	✓	✓	X	X	X		?	?		?	?	?	?	?		X	X		X	X	X
18	✓	X	X	?	?	?	?	?	?	?	?		X	X		X	X	✓	✓	X		X	X		X	X	✓
19	X	X	X	✓	X	X	✓	?	?	?	?		X	X		X	X	✓	X	X		X	X		X	X	X
20	X	X	X	✓	X	X	✓	?	?	?	?		X	X		X	✓	X	X	✓		X	X		X	X	✓
	Other Related and Selected Studies																															
30	✓	X	X	X	?	?	?	?	?	?	?		✓	✓		✓	X	✓	✓	X		✓	X		X	✓	✓
13	✓	X	X	X	?	?	?	?	?	?	?		✓	X		X	X	X	X	X		X	X		✓	X	X
32	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	X	X	✓	X		X	X		X	X	X
33	✓	X	X	X	?	?	?	?	?	?	?		✓	X		X	X	✓	✓	X		X	X		✓	X	X
34	✓	X	X	✓	?	?	?	?	?	?	?		X	X		✓	X	✓	X	X		X	X		X	X	✓

TABLE 3. *(Continued.)* **A. Related works. B. Trust justification features.**

75	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	X	?	X	X		X	X		X	✓	✓
76	✓	X	X	X	?	?	?	?	?	?	?		X	X		X	X	X	X	X		X	X		X	X	X
104	✓	X	X	✓	?	?	?	?	?	?	?		X	X		X	X	X	X	X		X	X		X	X	✓
78	✓	X	X	✓	✓	✓	✓	✓	✓	X	X		X	✓		X	✓	X	X	X		✓	✓		X	X	X
38	X	X	✓	✓	✓	✓	✓	✓	✓	✓	✓		X	✓		X	X	X	X	✓		X	X		✓	X	X
105	✓	X	X	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		X	X	X	X	✓		X	X		✓	X	✓
80	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓		X	X		X	X	X	X	X		X	X		✓	X	✓
82	✓	X	X	✓	✓	✓	✓	✓	✓	X	X		X	✓		X	X	X	X	X		X	X		X	X	X
85	✓	X	✓	X	✓	✓	✓	✓	✓	✓	✓		✓	✓		X	✓	✓	X	X		✓	✓		✓	X	✓
83	✓	✓	X	✓	✓	✓	✓	?	?	?	?		X	X		✓	✓	X	X	X		X	X		X	X	✓
84	✓	X	X	X	✓	✓	✓	?	?	?	?		✓	X		✓	✓	X	X	X		✓	✓		X	X	✓
85	✓	✓	X	X	✓	✓	✓	?	?	?	?		✓	X		✓	X	X	X	X		✓	✓		✓	X	X
42	✓	X	X	X	✓	✓	✓	X	X	X	X		X	X		✓	✓	✓	✓	X		X	X		X	✓	✓
46	✓	X	X	X	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	X	X	X	✓		✓	✓		✓	X	✓
27	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		X	X	X	X	✓		✓	✓		X	X	✓
37	X	X	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	X		✓	✓	✓	X	X		✓	✓		✓	X	✓
81	✓	X	X	X	✓	✓	✓	✓	✓	✓	✓		X	X		✓	✓	X	X	X		X	X		X	X	X
116	✓	X	✓	✓	✓	✓	X	✓	✓	X	X		X	✓		✓	X	X	✓	✓		X	X		✓	X	X
117	✓	X	✓	X	✓	X	✓	✓	✓	X	X		✓	✓		✓	X	X	✓	✓		X	X		X	X	X

C. RESULT ANALYSIS

As a brief summary to the explored research challenges identified in the previous section, we emphasize major concerns and express a strong interest in the trusted distributed AI mechanism with the identified justification features. The features and indicators of the end-to-end trust mechanism can be listed as below.

- **Performance**
  - **Scalability, Elasticity, and Connectivity Limits:** Total number of nodes and users in the system
  - **Energy Efficiency:** Average energy consumption of nodes and transactions
  - **Energy Efficiency:** Average EMF (v/m), SAR (w/kg), Power(W) environmental friendliness
- **Run-time Monitoring**
  - **Data-flow monitoring:** Data-state monitoring between applications
  - **Transaction-Flow Monitoring**: Transaction lifecycle monitoring
  - **Trust Monitoring**: Periodical trust verification
  - **AI/ML Pipelining**: Dynamic knowledge-base monitoring and update
- **Security**
  - **Context-aware dynamic adaptiveness:** Event-based secure connection policies and protocols
  - **Context-aware dynamic adaptiveness:** Dynamic package checksum verification
- **Test**
  - **Verification (survey, benchmarking, expert):**
    - **Dynamic check-point locating with feedback controllers and optimization**
    - **Resiliency and robustness monitoring with holistic views and feedback controllers**
  - **Confidence-Building:** Trust and confidence measurement/quantification in smart systems
  - **User-level continuous trust measurement**: Face mimics/body language, behavioral anomalies.

The main categories of these features and indicators identified are: (1) Performance (2) Run-Time Monitoring (3) Security (4) Test-based dynamic metrics. These can build the end-to-end trust mechanism with technical computing paradigms and user-level concerns. The rest of the section will provide information on the main related works identified that introduce the emerging challenges.

The reviewed literature shows that distributed AI has been investigated in many domains, such as telecommunication technologies [16]. It has been merged with multi-agent systems as a joint approach for complex system [17] design. Trust features are also explored for the AI/ML paradigms, which are [18] Fair, Explainable, Auditable and Safe (FEAS), to be explored in different stages of a system lifecycle, with each stage forming part of a Chain of Trust. Formal definitions of trust are also elaborated widely in literature [4], [19]. The mechanisms are improved with ML and statistical perspectives to cover data management challenges [2] with end-to-end pipelining mechanisms [3]. Programming paradigms, such as concurrent [20], probabilistic/dynamic/differential [1] are also explored to adapt the mechanisms to change in a dynamic context.

Performance modeling paradigms are widely discussed in the literature. For instance, an acceleration framework is proposed for the performance increase of distributed machine-learning algorithms. Noises, such as straggler nodes, system failures, or communication bottlenecks are identified and elaborated with a coding theory technique to provide resiliency in different engineering contexts [11]. The authors state a bandwidth reduction gain of O(1/n) from the fundamental limit of communication rate for coded shuffling. Another current problem identified is to find an information-theoretic lower boundary for the rate of coded shuffling. AI methods have been reviewed for robot teaming and human cooperation methodologies. Mobile robotic communication and swarm UAVs will be explored with CNN and RNN methods for the data processing of the obtained image/video data [78].

AI techniques are proposed for challenges of mission-critical autonomous software. Novel abstraction paradigms are identified as a requirement in order to reduce the complexity of swarm systems. The heterogenous structure of emerging intelligent swarms is identified as a challenge

for system behavior monitoring and verification. Requirements in engineering, nontrivial learning and planning, agent technology, self-modifying systems, and verification technologies are emphasized as future challenges for critical swarm mission autonomous software [79]. Formal methods and techniques are explored for the verification, validation, and assurance of future swarm-based missions, such as the ANTS (Autonomous Nano Technology Swarm) mission. It has 1,000 autonomous robotic agents designed to cooperate in asteroid exploration [80]. Its non-deterministic nature, high degree of parallelism, intelligent behavior, and emergent behavior, and new kinds of verification methods remain to be explored. Formal specification language to predict and verify the emergent behavior of future NASA swarm-based systems is currently being designed and developed.

In order to have a comprehensive overview of the challenges, it is proposed to limit the scope to the system-level thinking process for AI systems [83]. Comprehensive transdisciplinary approaches are proposed, which include Axiomatic Design (AD), AI/ML techniques, and Information Theoretic Methods (ITM) to reduce risks and complexities by improving cyber-system adaptiveness, enhancing cyber-system learning, and increasing the cyber-system prediction and insight potential [84]. The growth perspectives of the mechanisms are another research direction [27] in context awareness surveyed from an IoT perspective, and include techniques, methods, models, functionalities, systems, applications, and middleware solutions. The growth progress of context-aware computing, from desktop applications, web applications, mobile computing, pervasive/ubiquitous computing to the Internet of Things (IoT) is explained. Therefore, trusted computing paradigms can help to ensure the behavioral integrity of the mechanisms, in which trusted computing, trusted platforms, and trusted systems are defined as the system components which behave as expected for all transactions [37].

These challenges for the mechanisms can be identified in a nutshell as major points. Key challenges for emerging smart-system mechanisms are identified as computing, communication, and control. In order to ensure resilience against manipulation threats, the other research directions concern end-to-end trust mechanisms (integrated view of the three pillars: networking, processing/optimization, as well as security) and swarm controller methods guaranteeing safety, which aim to enable the trusted scalability of the swarm systems. These features are called CCAM Connected, Cooperative, Autonomous Mobility) as generalized use/business cases [15]. Chapter. V briefs on these emerging features and discusses the challenges with a focus on the last ten years between 2011-21.

V. DISCUSSION AND CHALLENGES

Previous sections presented a comprehensive scientific background on emerging intelligent systems with a focus on TDAI concept and trust justification features. Potential research directions and challenges are also discussed in detail from a historical perspective. In this section, these features will focus on the challenges between 2011-21, and potential directions will be summarized in Table. 3.

Intelligent systems require more elaboration on distributed computing principles and paradigms to improve the identified challenges. Based on the explored literature, we can say that the system resource management principles and AI system perspectives introduced in previous sections can enable continues growth for smart-system mechanisms with the set of nodes $N_i : \{N_o, N_1, N_2, \ldots, N_n,$. Thus, critical features like robustness, resilience, reliability, and trust of the nodes can be ensured. We can identify the research challenges and AI systems research studies with the four main questions below:

- **How can trust in distributed systems be measured/quantified/justified?**
- **How can the trusted scalability of autonomous systems be enabled?**
- **How can trust for swarm intelligence mechanisms be ensured?**
- **How can swarm system units with a search and mining focus be manipulated to implement trusted distributed AI methodology in real time?**

These questions can help us to understand how to build a growth-flow mechanism for emerging intelligent systems, which have dynamic and untrusted contexts. For this reason, the trusted distributed AI methodologies need to be implemented to maximize confidence and accelerate the growth of intelligent systems. Table. 3. summarizes the recent challenges and require main feature sets and is followed by the conclusion with a focus on the distributed computing principles and paradigms of the identified trust justification features.

An intelligent system with of nodes $N_i : \{N_o, N_1, N_2, \ldots, N_n$, which have critical selected features can be categorized into five main groups as in Table. 3:

- Trusted scalability and elasticity for throughput maximization
- Resilience to adversarial/adversarial threads
- Simulation-based validation and verification with digital twins or limited context simulations
- Monitoring with holistic views of the system
- Thread detection and reaction with dynamic feedback controllers for continuous growth flow.

As summarized in Table. 3, state-of-the-art approaches investigate the challenges with disruptive system-level innovations. For instance, a data-centric operating system is proposed with limited features [106]. Higher-throughput lower-latency features are also studied with protected data planes [107]. The approach has triggered paradigm switches on transaction definitions and implementations, such as a device [108] is proposed for a secure transaction with advanced feature sets like dynamic feedback controllers. Although trusted scalability remains an open issue but novel

TABLE 4. Artificial intelligence system state-of-the-art and main research challenges between 2011–2021.

RELATED WORKS AND MAIN FEATRUES	Trusted scalability and elasticity for throughput maximization	Adversarial/ un-adversarial threads	Simulation-based validation and verification	Monitoring	Detection and reaction with dynamic feedback-controllers for continuous growth-flow
[106] Data-Centric Operating System	❌	❌	❌	✅	❌
[107] A protected data-plane operating system for high throughput and low latency	✅	✅	✅	❌	❌
[108] A device for secure transaction approval	❌	✅	✅	✅	✅ Limited with end-to-end latencies
[5] A holistic abstraction to ensure trusted scaling and memory-speed trusted analytics	✅	✅	✅	✅	✅
[109] White Paper – Artificial Intelligence	❌	✅	❌	✅ Limited evaluation for abstraction levels	❌
[110,111,112,113] Adversarial/un-adversarial thread monitoring for transaction approvals.	❌	✅	✅	✅	❌
[114] Quantum cryptography features	❌	✅	❌	✅	❌
[115] BioDynaMo_ a general platform for scalable agent-based simulation	❌	❌	✅	✅	❌
[116] Survey on AI/ML accelerators.	❌	❌	✅	✅	❌
[117] SuperCloud Data sets and categorization of AI/ML workloads.	✅	❌	✅	✅	❌

TABLE 5. Summary of future directions.

#	Future Directions
1	Faster convergence and exploration to be investigated. Neural network objective functions to be defined for some types of transformations.
2	Entire distributed ML system design progress is ongoing.
3	Framework design and experimentation are ongoing.
4	Different trust metrics and performance indicators to be explored.
5	Different use cases are under evaluation for future experiments.
6	Minimization of humans in loop and real-time decision-support limitations to be explored.
7	Smart city use cases to be implemented.
8	Framework to be improved and tested with large scale use-cases.
9	Holistic DevOpS lifecycle is expected to bring together the development and operation of AI with increasing trust.
10	Next-generation stochastic directions and batch-based second-order derivative approximation methods to be investigated.
11	Bandwidth reduction gain of O(1/n) is stated as being from the fundamental limit of the communication rate for coded shuffling. Finding an information-theoretic lower bound on the rate of coded shuffling is identified as another open problem.
12	Larger-scale data amounts and number of users to be investigated. Driver behaviors also to be observed in future versions.
13	Potential use cases of AI systems proposed, and consciousness of machines is retained as a future research direction.
14	Coordination-based systems, caching policies, and middleware mechanisms to be investigated. Security/Privacy/Trust support are also limited aspects of proposed solutions.
15	Proposed end-to-end trust mechanism and methodologies to be tested in related use cases, mainly for swarm intelligence mechanisms.
16	Other approaches are proposed for feature interaction problems.
17	DAI and multi-agent systems are proposed for complex system design.
18	Fair, Explainable, Auditable, and Safe (FEAS) futures to be explored in different stages of a system lifecycle, with each stage forming part of a Chain of Trust.
19	Further trust formalizations and understandings to be identified.
20	Agent features to be broadened and distributed design paradigms to be investigated.
	Other Related and Selected Studies
30	AI-enabled future technology paradigms are investigated in detail, adversarial and un-adversarial cyber-threads are introduced.
13	Particle swarm optimizers - PSO controllers to be improved for better performances.
32	Need for trusted AI systems expressed by indicating limitations if there is an explainable AI definition. Trust features to be improved.
33	Identified research challenges for Trustworthy AI to be explored within a community.
34	Normware artefacts to be identified for interfaces between the agents.
9	Holistic DevOps lifecycle to be explored in identified use-cases.
75	Framework provided by Laswell's communication model to be used to structure future research efforts.
76	Proposed guidelines to be discussed though a final truth.
104	Proposed regulations to be discussed though an improved version.
78	Mobile robotic commination and swarm UAVs to be explored with CNN and RNN methods for the data processing of obtained images/video data.
38	Defined automatic control systems to be tested and improved in real-life use cases, such as machine tools, flexible robotics, photolithography, biomechanical and biomedical, process control.
105	Requirements engineering, nontrivial learning and planning, agent technology, self-modifying systems, and verification technologies are emphasized as future challenges for autonomous critical swarm mission software.
80	Non-deterministic nature, high degree of parallelism, intelligent behavior and emergent behavior, new kinds of verification methods are to be explored. Formal specification language to predict and verify emergent behavior of future NASA swarm-based systems is being designed and developed.
82	More complex scenarios and techniques to be evaluated for critical UAV missions.
85	Limitations of 5G and future directions to be identified.
83	A system-level thinking autonomous and functional AI entity, that is not just a collection of algorithms and processing boards, is to be studied.
84	Proposed method to be improved within experimentations in potential solutions.
85	Proposed architecture to be completed and requirements of prototype systems to be identified.
42	Data ecosystems to be studied more closely, where a future role for the VMBO community is envisioned.
46	Key research challenges and obstacles are identified in six categories and possible research approaches are proposed for emerging smart city systems as whole.
27	Importance of context awareness in the IoT paradigm is emphasized to build a foundation for future directions identified for the upcoming IoT technologies.
37	Trusted computing paradigm to be tested in real-life use-cases and to be improved for large-scale systems.
81	High throughput wireless and mobile technologies to be replaced with tethered ones.
116	Diversity of architecture and technologies, such as neuromorphic, flash-based analog memory processing, dataflow engines, and photonic-based processing is expected to improve performance in future systems.
117	HPC limitations to be improved with modern AI/ML frameworks with hybrid cloud design paradigms.

holistic abstraction approaches [5] can help maximize the throughput of nodes and total systems.

AI-driven system modeling is also a hot topic, especially for decentralized and distributed systems [109]. Adversarial/un-adversarial thread monitoring and transaction approval approaches [110]–[113] also promising to minimize system-level anomalies and failures in (near)-real time. Quantum computing and quantum cryptography features [114] are becoming a critical challenge and feature for the growing intelligent systems. Simulation-based digital twins are [115] widely implemented to minimize potential future failures and improve knowledge bases and training sets.

In a nutshell, we can say that decentralized and distributed designs enable us to implement massive-scale AI/ML algorithms within the growing intelligent systems as hybrid clouds [116], [117] with novel accelerator components, as indicated in Table. 3. The next chapter summarizes these challenges and main findings and introduces potential TDAI research fields.

VI. CONCLUSION

A. SUMMARY OF THE MAIN FINDINGS

As a brief conclusion of the research challenges explored, we ascertain that TDAI is seen as a missing, and as yet, largely unexplored area. Critical feature sets can be summarized as illustrated in Table.2, that is: (1) trust measurement and quantification (2) trusted scalability (3) trust assurance (4) swarm manipulation (5) system and user behavior monitoring. The feature sets identified can help to ensure the continuous growth of the intelligent systems, which are core mechanisms of emerging smart ecosystems, with software-driven dynamic systems to ensure adaptiveness and flexibility in a dynamic context, rather than hardware-dependent designs. Thereby, the trust factor of the system, $P(x^*) \propto t$ with the set of nodes $N_{E:}\{N_1, N_2, N_3, \ldots, N_n\}$ can be increased to maximize the throughput in the well-defined dynamic context with the adaptive agent function $f_{opt}()$. The critical feature sets selected in Table.3.B can be considered as the key elements of the end-to-end trust mechanism for the continuous growth of intelligent systems. The better the features justified, the faster the growth for the dynamic objectives of the mechanisms is ensured.

The challenges summarized in Tables.2 and 3 briefly introduced potential research directions. Architectural design principles are critical concerns for the novel innovations in the growing context. Decentralized approaches can build autonomous/embedded/local components with basic functionalities like swarm manipulation. In order to improve the components with trusted scalability and monitoring features, end-to-end fully connected channels are required. Centralized designs can guarantee these features with respect to end-to-end latency limits. Identified advanced justified functionalities are required for the novel futuristic designs, which are possible with the distributed design paradigms, which include edge/hybrid/hierarchical/multi-layer features with emerging holistic abstraction principles [14], [15], [31]. These features and research challenges are also included in the growth-flow of the emerging intelligent systems with advanced trusted AI capabilities. Next chapter introduces potential research challenges and future directions within a summary table.

B. POTENTIAL TDAI RESEARCH FIELDS

Disruptive innovations proposed for growing intelligent systems trigger acceleration to obtain an end-to-end fully trusted execution environment, which can be operated in the distributed context within the limits of critical systems constraints. However, the limitations of the decentralized components can only provide basic functionalities, like swarm manipulation features. These features can be improved with decentralized designs and hybrid mechanisms for the recent challenges. Table.5 introduces major points from the related works and reviewed literature between 1950 and 2021, with a focus on recent years. These challenges remain open issues to be explored in detail to obtain a fully trusted execution environment for growing intelligent systems with dynamically correlated and observed socio-dynamic features, which mainly focus on the regulative legal measurement metrics of alerting methodologies. These identified challenges will be investigated in detail in future related works.

In the TDAI research field, we identify the following emerging areas as being of increasing interest within the **distributed computing communities:**

- Trust measurement, quantification, and justification in distributed systems and its underlying diverse components.
- Trusted scalability of autonomous systems with algorithms and system levels with end-to-end holistic views.
- Trusted architecture mechanisms (e.g. Machine Learning) with novel abstraction approaches of end-to-end paradigms.
- Real-Time swarm manipulation to implement trusted distributed AI methodology.

The challenges and future directions identified in this survey can be defined as key features and milestones for massive scale trusted AI. Thereby, an intelligence flow can be assured for growing intelligent mechanisms via end-to-end trust mechanisms, which have TEE based trusted interaction with the environments within the smart-ecosystems and dynamic contexts. The more features justified within the critical systems constraints, the more trust can be obtained with TDAI for the growing intelligent systems.

On the other hand, in spite of the major progress made in computing systems with distributed design innovations, there are still challenges for the critical system constraints for the continuous growth of the intelligence systems. For instance, in [37] experiments have recently reported with trusted computing paradigms in real life use-cases. In [81] high throughout mobile and wireless communication technologies have recently been replaced with tethered ones. More critically, [117] HPC limitations are still set to be improved with modern AI/ML frameworks with hybrid cloud design paradigms.

Table.5 gives the summary of the major parts of the identified future directions. Fortunately, defined architectural perspectives (central, decentral/autonomous, distributed/hybrid) for emerging trusted distributed AI mechanisms can enable to ensure resiliency and robustness in a dynamic context with an end-to-end TEE for growing intelligent mechanisms and systems. Furthermore, the trust measurement, quantification, and justification methodologies can be applied in emerging distributed systems and their underlying diverse application domains with TDAI, which will be explored and experimented in our related future works.

REFERENCES

[1] A. G. Baydin, B. A. Pearlmutter, A. A. Radul, and J. M. Siskind, "Automatic differentiation in machine learning: A survey," *J. Mach. Learn. Res.*, vol. 18, no. 1, pp. 5595–5637, 2017.

[2] T. Kraska, A. Talwalkar, J. Duchi, R. Griffith, M. J. Franklin, and M. Jordan, "MLbase: A distributed machine-learning system," *CIDR*, vol. 1, pp. 1–2, Jan. 2013.

[3] M. Milutinovic, A. G. Baydin, R. Zinkov, W. Harvey, D. Song, F. Wood, and W. Shen, "End-to-end training of differentiable pipelines across machine learning frameworks," in *Proc. Neural Inf. Process. Syst. (NIPS), Autodiff Workshop: Future Gradient?Based Mach. Learn. Softw. Techn.*, Long Beach, CA, USA, Dec. 2017.

[4] R. Cohen, M. Schaekermann, S. Liu, and M. Cormier, "Trusted AI and the contribution of trust modeling in multiagent systems," in *Proc. 19th Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*. Montreal, QC, Canada: International Foundation for Autonomous Agents and Multiagent Systems, May 2019, pp. 1644–1648.

[5] M. A. Agca, "A holistic abstraction to ensure trusted scaling and memory speed trusted analytics," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2019, pp. 1428–1434.

[6] M. Nassar, K. Salah, M. H. U. Rehman, and D. Svetinovic, "Blockchain for explainable and trustworthy artificial intelligence," *WIREs Data Mining Knowl. Discovery*, vol. 10, no. 1, Jan. 2020, Art. no. e1340.

[7] A. Kumar, T. Braud, S. Tarkoma, and P. Hui, "Trustworthy AI in the age of pervasive computing and big data," 2020, *arXiv:2002.05657*.

[8] W. Hummer, V. Muthusamy, T. Rausch, P. Dube, K. E. Maghraoui, A. Murthi, and P. Oum, "ModelOps: Cloud-based lifecycle management for reliable and trusted AI," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Jun. 2019, pp. 113–120.

[9] S. Martínez-Fernández, X. Franch, A. Jedlitschka, M. Oriol, and A. Trendowicz, "Research directions for developing and operating artificial intelligence models in trustworthy autonomous systems," 2020, *arXiv:2003.05434*.

[10] L. Bottou, F. E. Curtis, and J. Nocedal, "Optimization methods for large-scale machine learning," *SIAM Rev.*, vol. 60, no. 2, pp. 223–311, 2018.

[11] K. Lee, M. Lam, R. Pedarsani, D. Papailiopoulos, and K. Ramchandran, "Speeding up distributed machine learning using codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1514–1529, Mar. 2018.

[12] B. Hull, V. Bychkovsky, Y. Zhang, K. Chen, M. Goraczko, A. Miu, E. Shih, H. Balakrishnan, and S. Madden, "CarTel: A distributed mobile sensor computing system," in *Proc. 4th Int. Conf. Embedded Netw. Sensor Syst.*, 2006, pp. 125–138.

[13] S. Russell and P. Norvig, "A modern, agent-oriented approach to introductory artificial intelligence," *ACM SIGART Bull.*, vol. 6, no. 2, pp. 24–26, Apr. 1995.

[14] M. van Steen and A. S. Tanenbaum, "A brief introduction to distributed systems," *Computing*, vol. 98, no. 10, pp. 967–1009, 2016.

[15] M. A. Ağca, P. A. Sarvari, S. Faye, and D. Khadraoui, "Challenges for swarm of UAV/drones based intelligence," in *Advances in Parallel Distributed Processing, and Applications*. Cham, Switzerland: Springer, 2021, pp. 633–645, doi: 10.1007/978-3-030-69984-0_45.

[16] H. Velthuijsen, "Distributed artificial intelligence for runtime feature-interaction resolution," *Computer*, vol. 26, no. 8, pp. 48–55, 1993.

[17] P. Stone and M. Veloso, "Multiagent systems: A survey from a machine learning perspective," *Auton. Robots*, vol. 8, no. 3, pp. 345–383, Jun. 2000.

[18] E. Toreini, M. Aitken, K. Coopamootoo, K. Elliott, C. G. Zelaya, and A. van Moorsel, "The relationship between trust in AI and trustworthy machine learning technologies," in *Proc. Conf. Fairness, Accountability, Transparency*, Jan. 2020, pp. 272–283.

[19] S. Marsh, "Trust in distributed artificial intelligence," in *Proc. Eur. Workshop Modelling Auton. Agents Multi-Agent World*. Berlin, Germany: Springer, Jul. 1992, pp. 94–112.

[20] G. Agha and n. Jamali, *Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence*. Cambridge, MA, USA: MIT Press, 1999, ch. 2, pp. 505–534. [Online]. Available: http://osl.cs.illinois.edu/media/papers/agha-1999-concurrent_programming_for_distributed_artificial_intelligence.pdf

[21] M. Alan, "Turing," *Comput. Mach. Intell.*, vol. 59, no. 236, pp. 433–460, Oct. 1950. [Online]. Available: https://www-jstor-org.proxy.bnl.lu/stable/2251299?seq=1

[22] J. Moor, "The dartmouth college artificial intelligence conference: The next fifty years," *AI Magazine*, vol. 27, no. 4, p. 87, 2006, doi: 10.1609/aimag.v27i4.1911.

[23] J. J. McCarthy, M. L. Minsky, and N. Rochester, *Artificial Intelligence*. Cambridge, MA, USA: Massachusetts Institute of Technology, 1959.

[24] J. McCarthy, "Artificial intelligence, logic and formalizing common sense," in *Philosophical Logic and Artificial Intelligence*. Dordrecht, The Netherlands: Springer, 1989, pp. 161–190.

[25] J. McCarthy, "What is artificial intelligence?" Tech. Rep., Jan. 1998. [Online]. Available: http://www-formal.stanford.edu/jmc/

[26] J. McCarthy, "Concepts of logical AI," in *Logic-Based Artificial Intelligence*. Boston, MA, USA: Springer, 2000, pp. 37–56.

[27] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 414–454, 1st Quart., 2013.

[28] C. Mitchell, Ed., *Trusted Computing*, vol. 6. Edison, NJ, USA: IET, 2005.

[29] M. A. Ağca, Ş. Ataç, M. M. Yücesan, Y. G. Küçükayan, A. M. Özbayoğlu, and E. Doğdu, "Opinion mining of microblog texts on Hadoop ecosystem," *Int. J. Cloud Comput.*, vol. 5, nos. 1–2, pp. 79–90, 2016.

[30] V. Gadepally, J. Goodwin, J. Kepner, A. Reuther, H. Reynolds, S. Samsi, J. Su, and D. Martinez, "AI enabling technologies: A survey," 2019, *arXiv:1905.03592*.

[31] R. C. Eberhart, Y. Shi, and J. Kennedy, *Swarm Intelligence*. Amsterdam, The Netherlands: Elsevier, 2001.

[32] F. Xu, H. Uszkoreit, Y. Du, W. Fan, D. Zhao, and J. Zhu, "Explainable AI: A brief survey on history, research areas, approaches and challenges," in *Proc. CCF Int. Conf. Natural Lang. Process. Chin. Comput.* Cham, Switzerland: Springer, Oct. 2019, pp. 563–574.

[33] J. M. Wing, "Trustworthy AI," 2020, *arXiv:2002.06276*.

[34] G. Sileno, A. Boer, and T. van Engers, "The role of normware in trustworthy and explainable AI," 2018, *arXiv:1812.02471*.

[35] D. F. Oriesek, "The potential impact of artificial intelligence on preventive diplomacy from a balance-of-threat perspective," Doctoral dissertation, Harvard Univ., 2022. [Online]. Available: https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37370754

[36] S. Martínez-Fernández, X. Franch, A. Jedlitschka, M. Oriol, and A. Trendowicz, "Developing and operating artificial intelligence models in trustworthy autonomous systems," in *Research Challenges in Information Science (RCIS)* (Lecture Notes in Business Information Processing), vol. 415, S. Cherfi, A. Perini, and S. Nurcan, Eds. Cham, Switzerland: Springer, 2021, pp. 221–229, doi: 10.1007/978-3-030-75018-3_14.

[37] L. Chen, C. J. Mitchell, and A. Martin, Eds., "Trusted computing," in *Proc. 2nd Int. Conf. Trust*, vol. 5471. Oxford, U.K.: Springer, Apr. 2009.

[38] B. C. Kuo and F. Golnaraghi, *Automatic Control Systems*. Hoboken, NJ, USA: Wiley, 2010.

[39] D. Gambetta, "Can we trust trust?" in *Trust: Making and Breaking Cooperative Relations*, D. Gambetta, Ed. Oxford, U.K.: Blackwell, 1990, pp. 213–237.

[40] M. Dorodchi, M. Abedi, and B. Cukic, "Trust-based development framework for distributed systems and IoT," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 437–442.

[41] G. Schryen, M. Volkamer, S. Ries, and S. M. Habib, "A formal approach towards measuring trust in distributed systems," in *Proc. ACM Symp. Appl. Comput. (SAC)*, 2011, pp. 1739–1745.

[42] H. Proper, "Data ecosystems-fuelling the digital age," in *Proc. VMBO*, 2020, pp. 1–4.

[43] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Sci. Amer.*, vol. 284, no. 5, pp. 34–43, 2001.

[44] G. Antoniou and F. Van Harmelen, *A Semantic Web Primer*. Cambridge, MA, USA: MIT Press, 2004.
[45] T. Lehr, U. Lorenz, M. Willert, and R. Rohrbeck, "Scenario-based strategizing: Advancing the applicability in strategists' teams," *Technol. Forecasting Social Change*, vol. 124, pp. 214–224, Nov. 2017, doi: 10.1016/j.techfore.2017.06.026.
[46] M. Aksit, "Software engineering challenges in realizing smart-city systems," Tech. Rep., 2019.
[47] M. B. Taylor, J. Kim, J. Miller, D. Wentzlaff, F. Ghodrat, B. Greenwald, H. Hoffman, P. Johnson, J.-W. Lee, W. Lee, A. Ma, A. Saraf, M. Seneski, N. Shnidman, V. Strumpen, M. Frank, S. Amarasinghe, and A. Agarwal, "The raw microprocessor: A computational fabric for software circuits and general-purpose programs," *IEEE Micro*, vol. 22, no. 2, pp. 25–35, Apr./May 2002, doi: 10.1109/MM.2002.997877.
[48] A. Agarwal, A. Mitra, P. Joshi, and K. Rastogi, U.S. Patent 10 248 566, 2019.
[49] D. Wentzlaff, P. Griffin, H. Hoffmann, L. Bao, B. Edwards, C. Ramey, M. Mattina, C.-C. Miao, J. F. Brown, III, and A. Agarwal, "On-chip interconnection architecture of the tile processor," *IEEE Micro*, vol. 27, no. 5, pp. 15–31, Sep./Oct. 2007.
[50] O. Mutlu and T. Moscibroda, "Stall-time fair memory access scheduling for chip multiprocessors," in *Proc. 40th Annu. IEEE/ACM Int. Symp. Microarchitecture (MICRO)*, 2007, pp. 146–160.
[51] O. Mutlu, S. Ghose, J. Gómez-Luna, and R. Ausavarungnirun, "A modern primer on processing in memory," 2020, *arXiv:2012.03112*.
[52] A. Agarwal, "Limits on interconnection network performance," *IEEE Trans. Parallel Distrib. Syst.*, vol. 2, no. 4, pp. 398–412, Oct. 1991.
[53] O. Mutlu, "Intelligent architectures for intelligent computing systems," 2020, *arXiv:2012.12381*.
[54] A. Agarwal, J. Hennessy, and M. Horowitz, "Cache performance of operating system and multiprogramming workloads," *ACM Trans. Comput. Syst.*, vol. 6, no. 4, pp. 393–431, Nov. 1988.
[55] A. Agarwal. (2013). Online distributed interaction. edX, Cambridge, MA, USA. [Online]. Available: https://www.freepatentsonline.com/y2013/0204942.htmlaaa
[56] M. Alizadeh, A. Greenberg, D. A. Maltz, J. Padhye, P. Patel, B. Prabhakar, S. Sengupta, and M. Sridharan, "Data center TCP (DCTCP)," in *Proc. ACM SIGCOMM Conf.*, 2010, pp. 63–74.
[57] B. Tekinerdogan, K. Özcan, S. Yağız, and I. Yakin, "Systems engineering architecture framework for physical protection systems," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Oct. 2020, pp. 1–8.
[58] E. Ahoa, A. Kassahun, and B. Tekinerdogan, "Business processes and information systems in the Ghana cocoa supply chain: A survey study," *Wageningen J. Life Sci.*, vol. 92, no. 1, pp. 1–11, Dec. 2020.
[59] H. Mao, M. Alizadeh, I. Menache, and S. Kandula, "Resource management with deep reinforcement learning," in *Proc. 15th ACM Workshop Hot Topics Netw.*, Nov. 2016, pp. 50–56.
[60] A. Agarwal, R. Bianchini, D. Chaiken, K. L. Johnson, D. Kranz, J. Kubiatowicz, B.-H. Lim, K. Mackenzie, and D. Yeung, "The MIT Alewife machine: Architecture and per formance," *ACM SIGARCH Comput. Archit. News*, vol. 23, no. 2, pp. 2–13, 1995.
[61] S. Dustdar, O. Mutlu, and N. Vijaykumar, "Rethinking divide and conquer—Towards holistic interfaces of the computing stack," *IEEE Internet Comput.*, vol. 24, no. 6, pp. 45–57, Nov. 2020, doi: 10.1109/MIC.2020.3026245.
[62] M. A. Ağca, "Özelleştirilmiş analitik bulut mimarilerinde dağıtık dosya sistemleri ile performans iyileştirilmesi," M.S. thesis, TOBB ETÜ Fen Bilimleri Enstitüsü, 2015.
[63] P. Negi, R. Marcus, A. Kipf, H. Mao, N. Tatbul, T. Kraska, and M. Alizadeh, "Flow-loss: Learning cardinality estimates that matter," 2021, *arXiv:2101.04964*.
[64] R. Baghdadi, A. N. Debbagh, K. Abdous, F. Z. Benhamida, A. Renda, J. E. Frankle, M. Carbin, and S. Amarasinghe, "TIRAMISU: A polyhedral compiler for dense and sparse deep learning," 2020, *arXiv:2005.04091*.
[65] D. Han, M. Wooldridge, A. Rogers, O. Ohrimenko, and S. Tschiatschek, "Replication robust payoff allocation in submodular cooperative games," *J. IEEE Trans. Artif. Intell.*, 2022. [Online]. Available: https://arxiv.org/pdf/2006.14583.pdf
[66] J. Gutierrez, M. Najib, G. Perelli, and M. Wooldridge, "On computational tractability for rational verification," Tech. Rep., 2020.
[67] D. Han, P. Harrenstein, S. Nugent, J. Philpott, and M. Wooldridge, "Behavioural strategies in weighted Boolean games," *Inf. Comput.*, vol. 276, Feb. 2021, Art. no. 104556, doi: 10.1016/j.ic.2020.104556.
[68] M. Wooldridge, "Artificial intelligence requires more than deep learning," Tech. Rep., 2020.
[69] G. Marcus and E. David, *Review of Rebooting AI: Building Artificial Intelligence We Can Trust*. New York, NY, USA: Pantheon Books, 2019. [Online]. Available: https://ora.ox.ac.uk/objects/uuid:105102f7-9a2d-424f-8559-0a50ec1fdd29/download_file?safe_filename=Wooldridge_2020_artificial_intelligence_requires.pdf&type_of_work=Journal+article
[70] I. Chih-Lin, S. Kuklinski, T. Chen, and L. Ladid, "A perspective of O-RAN integration with MEC, SON, and network slicing in the 5G era," *IEEE Netw.*, vol. 34, no. 6, pp. 3–4, Nov. 2020, doi: 10.1109/MNET.2020.9277891.
[71] L. Ladid, G. Karagiannis, and R. M. Potts, "D3.4: Harmonisation of standards for 5G technologies," Tech. Rep., 2019.
[72] C. Chaccour, M. N. Soorki, W. Saad, M. Bennis, P. Popovski, and M. Debbah, "Seven defining features of terahertz (THz) wireless systems: A fellowship of communication and sensing," *IEEE Commun. Surveys Tuts.*, early access, 2021, doi: 10.1109/COMST.2022.3143454.
[73] M. A. Ağca, D. Khadraoui, and S. Faye, "Persisting trust in intrusted varying resilient citv context V," in *Proc. Int. Conf. Artif. Intell. (ICAI)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2019, pp. 312–318.
[74] C. Krienke, L. Kolb, E. Diken, M. Streuber, S. Kirchhoff, T. Bukur, Ö. Akilli-Öztürk, L. M. Kranz, H. Berger, J. Petschenka, M. Diken, S. Kreiter, N. Yogev, A. Waisman, K. Karikó, Ö. Türeci, and U. Sahin, "A noninflammatory mRNA vaccine for treatment of experimental autoimmune encephalomyelitis," *Science*, vol. 371, no. 6525, pp. 145–153, 2021.
[75] R. Tomsett, A. Preece, D. Braines, F. Cerutti, S. Chakraborty, M. Srivastava, G. Pearson, and L. Kaplan, "Rapid trust calibration through interpretable and uncertainty-aware AI," *Patterns*, vol. 1, no. 4, Jul. 2020, Art. no. 100049.
[76] N. A. Smuha, "The EU approach to ethics guidelines for trustworthy artificial intelligence," *Comput. Law Rev. Int.*, vol. 20, no. 4, pp. 97–106, Aug. 2019.
[77] M. Veale, "A critical take on the policy recommendations of the EU high-level expert group on artificial intelligence," *Eur. J. Risk Regulation*, vol. 11, no. 1, p. e1, 2020.
[78] S. H. Alsamhi, O. Ma, and M. S. Ansari, "Survey on artificial intelligence based techniques for emerging robotic communication," *Telecommun. Syst.*, vol. 72, pp. 483–503, Mar. 2019.
[79] E. Vassev, R. Sterritt, C. Rouff, and M. Hinchey, "Swarm technology at NASA: Building resilient systems," *IT Prof.*, vol. 14, no. 2, pp. 36–42, Mar. 2012.
[80] C. Rouff, A. Vanderbilt, W. Truskowski, J. Rash, and M. Hinchey, "Verification of NASA emergent systems," in *Proc. 9th IEEE Int. Conf. Eng. Complex Comput. Syst.*, Apr. 2004, pp. 231–238.
[81] S. Cherry, "Edholm's law of bandwidth," *IEEE Spectrum*, vol. 41, no. 7, pp. 58–60, Jul. 2004, doi: 10.1109/MSPEC.2004.1309810.
[82] D. Machovec, J. A. Crowder, H. J. Siegel, S. Pasricha, and A. A. Maciejewski, "Dynamic heuristics for surveillance mission scheduling with unmanned aerial vehicles in heterogeneous environments," in *Advances in Artificial Intelligence and Applied Cognitive Computing* (Transactions on Computational Science and Computational Intelligence), H. R. Arabnia, K. Ferens, D. de la Fuente, E. B. Kozerenko, J. A. Olivas Varela, F. G. Tinetti, Eds. Cham, Switzerland: Springer, 2021, pp. 583–605, doi: 10.1007/978-3-030-70296-0_43.
[83] D. Machovec *et al.*, "Dynamic heuristics for surveillance mission scheduling with unmanned aerial vehicles in heterogeneous environments," Colorado Eng., Colorado Springs, CO, USA, White Paper, 2020.
[84] J. N. Carbone and J. A. Crowder, "Artificially intelligent cyber security: Reducing risk & complexity," in *Advances in Artificial Intelligence and Applied Cognitive Computing* (Transactions on Computational Science and Computational Intelligence), H. R. Arabnia, K. Ferens, D. de la Fuente, E. B. Kozerenko, J. A. Olivas Varela, F. G. Tinetti, Eds. Cham, Switzerland: Springer, 2021, pp. 499–523, doi: 10.1007/978-3-030-70296-0_38.
[85] Stuckman *et al.*, "EU commission," *Eur. 5G Annu. J.*, 2021.
[86] H. Balakrishnan, V. N. Padmanabhan, S. Seshan, and R. H. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," *IEEE/ACM Trans. Netw.*, vol. 5, no. 6, pp. 756–769, Dec. 1997.

[87] P. Martinet, J. Gallice, and K. Djamel, "Vision based control law using 3D visual features," in *Proc. Robot. Manuf. Syst., World Automat. Congr. (WAC)*, vol. 3, May 1996, pp. 497–502.
[88] H. Shukur, S. R. M. Zeebaree, A. J. Ahmed, R. R. Zebari, O. Ahmed, B. S. A. Tahir, and M. A. M. Sadeeq, "A state of art survey for concurrent computation and clustering of parallel computing for distributed systems," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 4, pp. 148–154, Dec. 2020.
[89] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for Internet applications," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 149–160, 2001.
[90] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proc. 33rd Annu. Hawaii Int. Conf. Syst. Sci.*, Jan. 2000, p. 10.
[91] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.
[92] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.
[93] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw.*, 1999, pp. 174–185.
[94] B. Chen, K. Jamieson, and H. Balakrishnan, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Netw.*, vol. 8, no. 5, pp. 481–494, 2002.
[95] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris, "Resilient overlay networks," in *Proc. 18th ACM Symp. Operating Syst. Princ.*, Oct. 2001, pp. 131–145.
[96] H. Balakrishnan and V. Arun, *Surface for Controlled Radio Frequency Signal Propagation*. Cambridge, MA, USA: Massachusetts Institute of Technology, 2020. [Online]. Available: https://www.freepatentsonline.com/y2020/0350693.html
[97] J. Meklenburg, M. Specter, M. Wentz, H. Balakrishnan, A. Chandrakasan, J. Cohn, G. Hatke, L. Ivers, R. Rivest, G. Jay Sussman, and D. Weitzner, "SonicPACT: An ultrasonic ranging method for the private automated contact tracing (PACT) protocol," 2020, *arXiv:2012.04770*.
[98] P. Goyal, A. Agarwal, R. Netravali, M. Alizadeh, and H. Balakrishnan, "ABC: A simple explicit congestion controller for wireless networks," in *Proc. 17th USENIX Symp. Netw. Syst. Design Implement. (NSDI)*, 2020, pp. 353–372.
[99] V. Arun and H. Balakrishnan, "RFocus: Practical beamforming for small devices," 2019, *arXiv:1905.05130*.
[100] I. S. A. Cho, J. Fried, S. J. Park, M. Alizadeh, and A. Belay, "Overload control for μs-scale RPCs with breakwater," in *Proc. 14th USENIX Symp. Oper. Syst. Design Implement. (OSDI)*, 2020, pp. 299–314.
[101] F. Ye, S. Zhou, A. Venkat, R. Marcus, N. Tatbul, J. J. Tithi, N. Hasabnis, P. Petersen, T. Mattson, T. Kraska, P. Dubey, V. Sarkar, and J. Gottschlich, "MISIM: A neural code semantics similarity system using the context-aware semantics structure," 2020, *arXiv:2006.05265*.
[102] H. Balakrishnan, L. D. Girod, and I. Ossin, U.S. Patent 14 529 812, 2015.
[103] V. Mannoni, V. Berg, S. Sesia, and E. Perraud, "A comparison of the V2X communication systems: ITS-G5 and C-V2X," in *Proc. IEEE 89th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2019, pp. 1–5, doi: 10.1109/VTC-Spring.2019.8746562.
[104] M. U. Scherer, "Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies," Social Sci. Res. Netw., Rochester, NY, USA, Tech. Rep., 2016.
[105] W. Truszkowski, M. Hinchey, J. Rash, and C. Rouff, "NASA's swarm missions: The challenge of building autonomous software," *IT Prof.*, vol. 6, no. 5, pp. 47–52, Sep. 2004, doi: 10.1109/MITP.2004.66.
[106] M. Cafarella, D. DeWitt, V. Gadepally, J. Kepner, C. Kozyrakis, T. Kraska, M. Stonebraker, and M. Zaharia, "DBOS: A proposal for a data-centric operating system," 2020, *arXiv:2007.11112*.
[107] A. Belay, G. Prekas, A. Klimovic, S. Grossman, C. Kozyrakis, and E. Bugnion, "IX: A protected dataplane operating system for high throughput and low latency," in *Proc. 11th USENIX Symp. Operating Syst. Design Implement. (OSDI)*, 2014, pp. 49–65.
[108] A. Athalye, A. Belay, M. F. Kaashoek, R. Morris, and N. Zeldovich, "Notary: A device for secure transaction approval," in *Proc. 27th ACM Symp. Operating Syst. Princ.*, Oct. 2019, pp. 97–113.
[109] REIFF. (Feb. 2021). *Artificial Intelligence Technology, Use Cases and Applications, Trustworthiness and Technical Standardization*. [Online]. Available: https://portail-qualite.public.lu/dam-assets/publications/normalisation/2021/ilnas-white-paper-artificial-intelligence.pdf
[110] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards deep learning models resistant to adversarial attacks," 2017, *arXiv:1706.06083*.
[111] M. Goldblum, D. Tsipras, C. Xie, X. Chen, A. Schwarzschild, D. Song, A. Madry, B. Li, and T. Goldstein, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," 2020, *arXiv:2012.10544*.
[112] N. Carlini, A. Athalye, N. Papernot, W. Brendel, J. Rauber, D. Tsipras, I. Goodfellow, A. Madry, and A. Kurakin, "On evaluating adversarial robustness," 2019, *arXiv:1902.06705*.
[113] H. Salman, A. Ilyas, L. Engstrom, S. Vemprala, A. Madry, and A. Kapoor, "Unadversarial examples: Designing objects for robust vision," 2020, *arXiv:2012.12235*.
[114] W. Beullens *et al.*, "Post-quantum cryptography: Current state and quantum mitigation," in *Proc. ENISA*, Attiki, 2021, p. 39. [Online]. Available: https://research.tue.nl/en/publications/post-quantum-cryptography-current-state-and-quantum-mitigation, doi: 10.2824/92307.
[115] L. Breitwieser *et al.*, "BioDynaMo: A general platform for scalable agent-based simulation," *bioRxiv*, 2021.
[116] A. Reuther, P. Michaleas, M. Jones, V. Gadepally, S. Samsi, and J. Kepner, "Survey of machine learning accelerators," in *Proc. IEEE High Perform. Extreme Comput. Conf. (HPEC)*, Sep. 2020, pp. 1–12.
[117] S. Samsi *et al.*, "The MIT supercloud dataset," 2021, *arXiv:2108.02037*.
[118] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug. 2015, pp. 57–64.
[119] J. Chen, K. Li, K. Bilal, X. Zhou, K. Li, and P. S. Yu, "A bi-layered parallel training architecture for large-scale convolutional neural networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 5, pp. 965–976, May 2018.
[120] J. Chen, K. Li, Z. Tang, K. Bilal, and K. Li, "A parallel patient treatment time prediction algorithm and its applications in hospital queuing-recommendation in a big data environment," *IEEE Access*, vol. 4, pp. 1767–1783, 2016.
[121] M. Goldblum, D. Tsipras, C. Xie, X. Chen, A. Schwarzschild, D. Song, A. Madry, B. Li, and T. Goldstein, "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses," 2020, *arXiv:2012.10544*.
[122] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Gener. Comput. Syst.*, vol. 110, pp. 758–771, Sep. 2020.
[123] J. Chen, K. Li, and P. S. Yu, "Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain," *IEEE Trans. Intell. Transp. Syst.*, early access, Aug. 26, 2021, doi: 10.1109/TITS.2021.3105682.

MUHAMMED AKİF AĞCA (Member, IEEE) received the degree from Middle East Technical University (METU), in 2011, and the master's degree in computer engineering from Turkish Stock Market Union Economy and Technology University (TOBB ETU), Ankara, Turkey, in 2015. He joined HAVELSAN Aerospace and Defense Company, in 2014, as a Software Engineer and worked as a NATO Coordinator for two years. He is pursuing his research and development studies in various groups as a Full-Stack Systems Architect and a Researcher. Currently, he is working on his Ph.D. thesis with the Luxembourg Institute of Science and Technology (LIST).

SÉBASTIEN FAYE (Member, IEEE) received the Ph.D. degree from Télécom ParisTech, Paris, France, in 2011. He became interested in telecommunication networks as a graduate student with the University of Picardie Jules Verne, Amiens, France, in 2009. During his M.S. thesis, he carried out several studies on wireless sensor networks and the security mechanisms they offer. Between 2009 and 2014, he was a web entrepreneur and created several web services and two startups. During his Ph.D. degree, he focused on distributed systems applied to intelligent transportation systems. His studies focused on how sensors equipped with magnetometers and short-range wireless radio interfaces can be deployed along with the road networks to detect the passage of vehicles and exchange traffic count information, investigating their deployment and performance in the area of traffic light management. Between 2014 and 2017, he was a Research Associate with the SnT/University of Luxembourg and responsible for the VehicularLab Team. He is a Research and Technology Associate with the ITIS Department, Luxembourg Institute of Science and Technology (LIST); and works on projects related to connected mobility, the IoT, wireless sensor networks, and 5G. He is an expert in mobile computing and has already worked on several national and European initiatives related to implementing embedded intelligence to address mobility, traffic flow optimization, and human activity detection. In particular, he has implemented a series of demonstrators designed to assist end-users in their daily mobility choices. He has recently started working in the 5G domain, with active involvement in several national and European initiatives. He is also the author of two recently filed patents about location profiling based on networks traces. He has authored and coauthored about 50 journals and refereed conference papers.

DJAMEL KHADRAOUI (Member, IEEE) is the Head of the Reliable Distributed Systems Research Unit (READY), LIST, Luxembourg. His research interests include the concept of trusted distributed and optimized systems, these systems can be physical infrastructures (buildings, roads, vehicles, and drones) but they are also more and more increasingly IT infrastructures, such as data centers, networks, and clouds. It is important to collect and manage data about the functioning of these infrastructures in order to guarantee the quality of the delivered services. This is the role of service systems to transform these data into information and decisions guaranteeing the alignment of the infrastructures with the business services delivered. Examples of such systems include supply chains, mobility systems, ICT/telco systems and communication networks, remote manufacturing, and space systems. The Trusted Service Systems research activities are dealing with the design, the security, and the optimization of service systems enabled by data-intensive infrastructures engineering and aligned with the creation of business impact. The actual research activities will target the following topics: data intensive systems with a focus on the processes, the science, and the platforms of big data; security, privacy and resilient critical infrastructures with a focus on data privacy and security, cybersecurity, and information security management; operations and supply chain optimization with a focus on data optimization and requirements, operations optimization, and sustainable supply chains; and enterprise modeling, value creation, and reliable infrastructures.