Examining Privacy and Trust Issues at the Edge of Isomorphic IoT Architectures: Case Liquid AI

Mamia.O. Agbese*
mamia.o.agbese@jyu.fi
University of Jyväskylä
Jyväskylä, Finland

Niko Mäkitalo
niko.k.makitalo@jyu.fi
University of Jyväskylä
Jyväskylä, Finland

Muhammad Waseem
muhammad.m.waseem@jyu.fi
University of Jyväskylä
Jyväskylä, Finland

Rahul Mohanani
rahul.p.mohanani@jyu.fi
University of Jyväskylä
Jyväskylä, Finland

Pekka Abrahamsson
pekka.abrahamsson@tuni.fi
Tampere University
Tampere, Finland

Tommi Mikkonen
tommi.j.mikkonen@jyu.fi
University of Jyväskylä
Jyväskylä, Finland

ABSTRACT

The growing domain of liquidity in computing extends its boundaries to include advancements like liquid artificial intelligence (AI). Liquid AI leverages liquid software using isomorphic Internet of Things (IoT) architecture to enhance computation at the edge. This innovation unveils vast opportunities yet also introduces significant challenges, particularly around privacy and trust. We explore the vulnerabilities that might hinder the progression of this technological fusion toward achieving trustworthy AI. Through an intensive examination of the literature, this research highlights the heightened threats to data integrity and stakeholder trust in these evolving ecosystems. Four main challenges: Data collection, Data storage and Access, Data utilization and sharing, and Surveillance and profiling were identified and examined under privacy, and two, Algorithms and decision-making and Security of IoT infrastructure under trust. The concerns are further categorized to highlight their impact on the development of trustworthy AI. The study acknowledges the early state of the field. Consequently, this research navigates through the limited available literature, initiating a pioneering discourse emphasizing fostering a foundation for developing secure and trustworthy Liquid AI environments.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Artificial Intelligence, Liquid Software, Isomorphic IoT architecture, Liquid AI, Edge computing, Trustworthy AI

ACM Reference Format:
Mamia.O. Agbese, Niko Mäkitalo, Muhammad Waseem, Rahul Mohanani, Pekka Abrahamsson, and Tommi Mikkonen. 2023. Examining Privacy and Trust Issues at the Edge of Isomorphic IoT Architectures: Case Liquid AI. In *The International Conference on the Internet of Things (IoT 2023), November 07–10, 2023, Nagoya, Japan.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3627050.3631574

IoT 2023, November 07–10, 2023, Nagoya, Japan

ACM ISBN 979-8-4007-0854-1/23/11.
https://doi.org/10.1145/3627050.3631574

1 INTRODUCTION

The digital technology world is rapidly evolving, requiring systems that are flexible and adaptable. Liquid software, which started as a web-based solution allowing easy transitions between different platforms and devices, has paved the way for this adaptability [8, 24]. This concept has grown, especially with the rise of the Internet of Things (IoT) - a system where everyday objects are interconnected. With the advancements in computing on the edge of the network (edge computing) and artificial intelligence (AI), we now see the emergence of 'Liquid AI' [33]. This new development aims to create AI systems that are both robust and can quickly adapt to their surroundings [33]. It promises faster responses by adjusting to changes in real-time, aligning with the main goals of edge IoT computing to reduce delays and use resources efficiently [11, 19, 30, 34, 35].

Adaptability is key in modern technology, with systems like Unmanned Autonomous Systems (UAS) and Intelligent Unmanned Autonomous Systems (IUAS) gaining importance, especially in healthcare [38]. For example, wearable IoT devices for elderly care could work in tandem with robots for more efficient care. UAS, which follow pre-set algorithms and sensor input, include drones and basic robots and can significantly benefit from IoT integration, like in wearable health monitors. IUAS, enhanced with AI, autonomously learns and makes real-time decisions, a critical capability for edge computing applications [38].

Isomorphism is key to the ´liquidity' or adaptability in the liquid AI paradigm [23, 33]. Isomorphic Software systems are central to this evolution, enabling a unified IoT infrastructure that can nurture a fluid AI ecosystem at the edge. This seamless integration can allow machine learning (ML) models to transition effortlessly between centralized cloud systems and local edge environments without structural overhauls. As a result, these AI models evolve into a 'liquid' form, deployable universally across diverse edge IoT devices without device-specific customizations. Such adaptable models are poised to make rapid, context-sensitive decisions in real-time, heralding a transformative phase in edge computing [23].

The emergence of Liquid Edge Intelligence, an intersection of Liquid AI and isomorphic IoT architectures, promises unparalleled

efficiency and adaptability [40]. However, it also ushers in challenges. Among these, ensuring the trustworthiness of AI model creation and deployment stands out, giving rise to concerns about data handling, system reliability, and potential misuse—all of which are deeply intertwined with privacy and trust issues [26, 28, 40]. It's crucial, therefore, to advocate AI systems that are transparent, fair, and rigorously safeguard user privacy. This paper explores these intricacies, pinpointing vulnerabilities while also spotlighting opportunities to steer the future toward more trustworthy AI systems [34, 37, 40]. Our investigation is guided by the following research question:

RQ: *What potential privacy and trust vulnerabilities are inherent in Liquid AI environments built on isomorphic architecture, and how do they impact the development of trustworthy AI?*

Through this review, we seek not only to bridge a current gap in understanding but also to pioneer discourse and exploration in a domain that stands as a frontier in technological evolution. The paper is structured as follows: Section 2 delineates this study's primary concepts, providing the necessary background. The methodology adopted for this research is explained in Section 3. Subsequently, Section 4 offers a comprehensive discussion of our findings and limitations. Finally, Section 5 concludes the study, summarizing the key insights and implications.

2 BACKGROUND

We examine the basic concepts of the study.

2.1 Liquid Software

Liquid software is a computing paradigm where applications provide a seamless user experience across various devices [8]. Liquid software is characterized by its adaptability and continuous updates, offering seamless experiences for users across multiple platforms, initially primarily on web-based applications. This fluidity has evolved to include the IoT (liquid IoT) [40], where the constant adaptability extends to devices operating at the edge of networks, facilitating a more harmonized interaction between various devices and systems [35, 40].

2.2 Edge Computing

Edge computing has its roots in distributed computing and network architecture concepts, with the term 'edge computing' gaining prominence in the late 2010s [9]. This rise was driven by the growing demand for low-latency, high-bandwidth processing, which conventional centralized cloud computing couldn't meet [9]. Facilitated by the exponential rise of IoT devices necessitating real-time data processing, edge computing situates computational resources close to data origins, such as IoT devices, consequently minimizing latency and bandwidth usage. This structural shift accentuates real-time analytics and optimizes the implementation of AI functionalities at the edge, cultivating a more agile and potent system. This computing paradigm is experiencing further refinement and sophistication, integrating seamlessly with modern technologies like Liquid software and IoT, thereby fostering a dynamic, adaptive computational ecosystem within IoT networks [42]. Liquid IoT, an emerging concept in the digital technology landscape, epitomizes the seamless adaptability and fluid functionality of the IoT [40]. Leveraging the capabilities of edge computing, it facilitates an environment where IoT devices can effortlessly adapt to changing conditions and technologies, enhancing efficiency and responsiveness. This progression is paving the way for the emergence of Liquid AI [23, 24, 34].

UAS encompasses a broad spectrum of autonomous systems, from aerial drones to ground vehicles and robots, operating without human pilots. These can be remotely controlled or function autonomously through predefined algorithms. Edge computing amplifies their capabilities by facilitating swift data processing near the source, ensuring prompt decision-making and efficient bandwidth utilization. The evolution towards Intelligent Unmanned Autonomous Systems (IUAS) integrates advanced AI, equipping these systems to learn, adapt, and make informed decisions based on environmental inputs. When combined with edge computing, IUAS can optimize real-time reactions in various scenarios, highlighting the significance of adaptability in local processing to enhance their capabilities [38].

2.3 Liquid AI

AI has a history dating back to the 1950s, marked by milestones such as Alan Turing's pioneering Turing Test [20]. The central aim of AI is to equip machines with cognitive abilities resembling human faculties, including learning, reasoning, and problem-solving. In the cloud-edge computing landscape context, AI plays a pivotal role in handling data from IoT devices, such as sensors and cameras [20]. By locally processing and filtering this data, AI enhances system efficiency, conserves bandwidth, and minimizes latency before cloud-based analysis.

In contrast, Liquid AI represents a recent innovation designed to overcome limitations associated with traditional AI systems [18, 33]. Liquid AI represents a significant paradigm shift that denotes AI's convergence with the concepts of liquid software, fostering an ecosystem where AI models can adapt swiftly, making real-time decisions based on changing contexts and environments [18, 33]. Additionally, a specialized subset of Liquid AI employs advanced neural network configurations inspired by the neural architecture of C. Elegans nematodes [11]. These microscopic worms manifest complex behaviors with a neuronal setup far less intricate than the ones employed in human-centric deep learning frameworks [11]. While this focus offers an intriguing direction for Liquid AI, it's worth mentioning that our research steers clear of this specialization. Instead, our work aims to build a versatile foundation that can adapt to a wide array of requirements, whether that involves interfacing with multiple types of technology or adapting to a diverse set of use cases.

The development of the Liquid AI framework is a direct response to the rise in data influx from IoT devices and advancements in ML data processing, further complemented by growing research in liquid software and liquid IoT [24, 35, 41]. This structure facilitates efficient ML model orchestration within interconnected networks, addressing the need for low latency, instantaneous analytics, and stringent security mechanisms [33]. Moving away from traditional monolithic models, it adopts a flexible, modular approach that dissects algorithms into smaller, manageable units and strategically positions ML models within the IoT edge network. Consequently,

data is processed incrementally as it transitions from the edge to the cloud [33], allowing for fluid modifications of algorithmic components within the system to accommodate evolving demands and constraints. It can also facilitate the creation and deployment of adaptable AI models across various edge devices without needing device-specific adjustments [34], paving the way for potential revolutions in IoT frameworks within sectors like smart energy systems. This strategy negates the need for massive data transmissions to centralized clouds, enhancing response times and bolstering decision-making effectiveness through edge-based data analysis [33]. It also encourages dynamic ML model allocation, optimizing resource utilization. Such adaptability becomes a cornerstone in the dynamic IoT landscape, especially at the edge, where swift adaptations to fluctuating conditions are critical. Implementing isomorphic IoT architecture is argued as a vital component in achieving this level of adaptability [23].

2.4 Isomorphic IoT Architecture

Isomorphic concepts in software engineering encompass structures, functions, or components capable of seamless operation across diverse systems, spanning hardware and software domains. This concept has evolved into what we now recognize as Isomorphic System Architecture, a pivotal component within the broader 'liquid software' paradigm [34]. Isomorphic elements range from simple functions to comprehensive libraries, all designed with modularity [35, 40]. Each component operates as a self-contained entity with a distinct purpose, making integration into various systems effortless. This modularity promotes reusability, simplifies the challenges associated with integration, and is pivotal to the 'liquid' approach, as shown in Figure 1. WebAssembly (Wasm) and JavaScript present key isomorphic software elements, and augment edge computing—JavaScript ensures cross-platform uniformity using consistent programming, while Wasm dynamically scales services, optimizing IoT device performance by providing a common runtime [35, 40].

This approach stands in sharp contrast to conventional IoT infrastructures, like sensors, actuators, gateways, cloud services, and user apps (Figure 1). Their monolithic and interdependent structures, coupled with varied programming tools, often hinder smooth functionality migration. These older infrastructures necessitate device-specific adaptations, restricting scalability and adding complexity. Primarily utilizing centralized computing, they exhibit higher latency and bandwidth due to centralized data processing and limited software and data update adaptability, making them less dynamic and more cumbersome to adjust to diverse contexts and conditions [23]. This adaptability is crucial in complex, interconnected IoT networks, facilitating optimizations in energy efficiency, response speed, and security-critical attributes [28]. Research is advancing in dynamic isomorphism using Wasm, promising heightened adaptability for the future [16].

2.5 Privacy and Trust Issues

The growing body of literature addressing privacy and trust challenges in developing trustworthy AI—particularly as it merges with nascent technologies like edge IoT intelligence underscores the pressing need for further study in the context of liquid edge intelligence leveraging isomorphic IoT infrastructures. Prominent areas of concern pinpointed in existing studies encompass aspects such as Consent and Transparency, Data Security and Integrity, Individual Autonomy and Control, and Data Minimization, among others [4, 17, 29, 31]. Yet, the literature shows a gap in addressing privacy and trust within isomorphic IoT frameworks, especially from a trustworthy AI perspective that can impact liquid AI development. Hence as Liquid AI and isomorphic infrastructures evolve, they present unique challenges for data privacy and trust, making their examination critical to the advancement of trustworthy AI.

3 METHODOLOGY

The literature on Liquid AI, encompassing concepts such as 'liquid software,' 'liquid IoT,' and 'isomorphic IoT architecture,' is still in its early stages. Also, the discourse surrounding these topics remains scarce and relatively underdeveloped compared to established domains like traditional AI or IoT infrastructure [33–35]. As such, We used an exploratory approach to address our research question to help bridge the gap in this fledgling field by scrutinizing existing literature to identify and categorize prevailing privacy and trust issues, thus laying a foundation for future empirical studies. Exploratory methods provide valuable flexibility, especially when delving into less-explored research areas [32].

3.1 Data Collection

We adopted a secondary research approach, focusing primarily on the literature on Google Scholar and unpublished studies or non-commercial sources such as reports and policy statements due to scarce resources from other academic databases. The literature review leveraged keywords including 'edge computing,' 'edge intelligence,' 'liquid IoT,' 'liquid software,' 'isomorphic software,' and 'isomorphic IoT architecture,' intertwined with privacy and trust issues. Our criteria for source selection concentrated on works that specifically address privacy and trust concerns in the areas mentioned, published from 2010 onwards. We also used backward citations from selected resources to broaden our search spectrum. 20 papers were identified that aligned with the study.

3.2 Data Analysis

We utilized content analysis, a methodical technique for examining qualitative data, facilitating the extraction of dominant themes and patterns to gain substantial insights [39]. We scrutinized the papers to ascertain the explored privacy and trust issues, using them as the central themes. We then coded and interpreted identified issues under the respective themes [39]. Adopting an interpretive approach allowed us to emphasize narrative interpretations in the literature, helping us to discern both the overt messages (manifest content) and the underlying or subtle meanings (latent content) encapsulated within the communication [39].

4 EXAMINING PRIVACY AND TRUST ISSUES IN LIQUID AI

The analysis outcomes are illustrated in Table 1. This table categorizes the notable privacy and trust issues. We discuss them further in this section towards steering the development of more trustworthy AI.

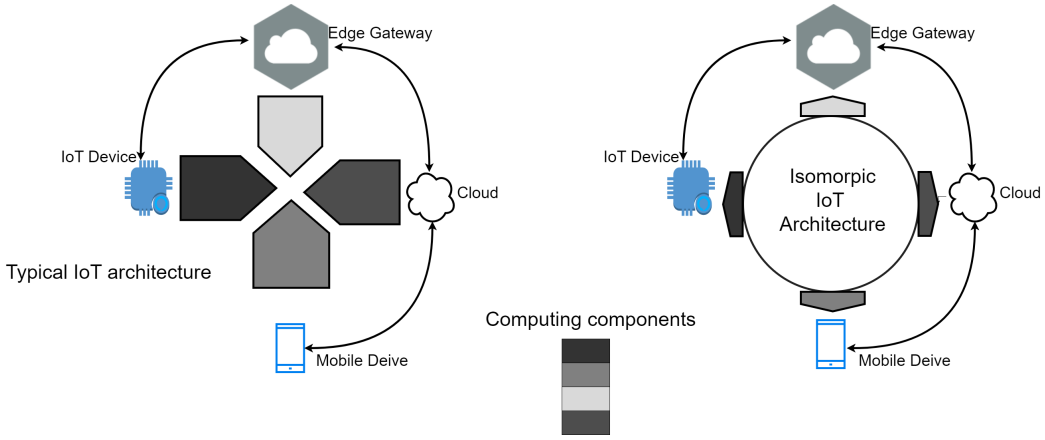

Figure 1: Isomorphic IoT architecture [23]

Table 1: Privacy and Trust Concerns in a Liquid AI Environment using Isomorphic IoT Architecture

Category	Subcategory	Concern
Privacy	Data Collection	Informed Consent [1, 3, 13] Autonomy Violation [1, 3, 13] Data Aggregation [1, 3, 13] Data De-identification [27, 41] Data Re-identification [27, 41]
	Data Storage and Access	Data Security and Encryption [13, 27] Data Ownership and Control [13]
	Data Utilization and Sharing	Data Monetization [7] Third-party Data Sharing [7]
	Surveillance and Profiling	Invasive Surveillance [25, 26] Mass Surveillance [13, 26]
Trust	Algorithms and Decision-making Processes	Propagation of Existing Biases [3, 25] Amplification through Integration [26] Limited Flexibility to Adapt [44] Interoperability Issues [26]
	Security of IoT Infrastructures	Security Breaches [1, 26] Transparency and Accountability [13, 26]

4.1 Trustworthy AI

Trustworthy AI aims to advance individual well-being and community prosperity by harnessing AI's wealth generation, value creation, and resource optimization capabilities. It aspires to promote a more equitable society by uplifting public health and facilitating equal economic, social, and political access [12]. This overarching framework rests on three fundamental pillars pivotal for our research: adherence to legal standards, commitment to ethical values, and the robustness of safety and security measures [12]. While the legal dimension ensures strict compliance with all applicable laws and regulations, our primary focus centers on the ethical facet of Trustworthy AI rooted in AI ethics and how it impacts the robustness of safety and security measures, this multifaceted domain extends beyond mere legal compliance and explores a spectrum of ethical principles, including transparency, fairness, non-maleficence, accountability, privacy, beneficence, individual freedom, trustworthiness, sustainability, human dignity, and societal solidarity [2, 12].

4.2 Privacy

Privacy involves safeguarding personal information from unauthorized access and closely examines how data is collected, transferred, and processed [14, 25]. We examine the potential privacy vulnerabilities.

4.2.1 Data Collection. Data collection is a pivotal starting point in the Liquid AI framework using isomorphic IoT architecture. The dynamic nature of Liquid AI necessitates constant data movement, potentially increasing vulnerability to unauthorized access and privacy breaches. Additionally, managing and securing the vast and diverse data generated within this framework poses inherent complexities [3]. We explore data collection further.

Informed Consent. Using isomorphic IoT infrastructure for liquid edge intelligence creates a complex landscape where data navigates through various layers and modules for aggregation, analysis, and utilization. This complexity necessitates a profound understanding of technical nuances, which may be beyond the grasp of average users, thereby posing significant challenges in attaining

genuine informed consent. The system's multifaceted processing of data further complicates users' ability to fully comprehend the scope and consequences of the activities they are consenting to.

Autonomy Violation. Obtaining informed consent from users in a system employing liquid edge intelligence can be challenging due to the intricate and dynamic data processing. This system may engage in excessive surveillance, invading personal privacy, and eroding individuals' autonomy. Users might be subtly coerced into disclosing more data than they intended, undermining their autonomous decision-making rights. Moreover, diverging from initial consensual purposes, the evolving data landscape introduces unpredictability and jeopardizes user autonomy in foreseeing and consenting to future data applications. Additionally, opaque algorithmic decisions in this setting can bypass individual preferences, limiting users' control over their data's fate, leading to legal and regulatory dilemmas [13, 35, 36, 40].

Data Aggregation: Data aggregation involves collecting and merging information from various sources, including IoT devices and online platforms, to create a comprehensive dataset for pattern analysis. While valuable for data analysis, this practice raises substantial privacy concerns. It can enable the inference of sensitive information about individuals that may not be evident in isolated datasets. Additionally, aggregated data might be repurposed for objectives beyond the initial intent, potentially without individuals' consent or awareness, heightening privacy risks [5, 13].

Data De-identification. De-identification involves stripping or masking personally identifiable information (PII) from datasets to safeguard individual privacy, including removing or altering explicit identifiers such as names and addresses. Despite its protective intent, it harbors the inherent risk of re-identification, where individuals can be identified through data linkage or statistical analysis that amalgamate diverse data sources or exploit data patterns, respectively. Consequently, this re-identification risk could nullify the privacy shields erected through de-identification efforts [14, 27, 36].

Data Re-identification. The risk of re-identifying de-identified data poses concerns of exposing sensitive information, potentially leading to misuse, privacy violations, or identity theft. Ethical questions arise regarding the scope of informed consent when data is used for undisclosed or unforeseen purposes. Such misuse can erode trust in technology and service providers, potentially resulting in adverse consequences for individuals, including discrimination or stigmatization, based on inferred characteristics [36, 41].

4.2.2 Data storage and Access. Data storage and access broadly refers to how data is stored, managed, and accessed within a system or network. Within the context of our study, data storage and access revolve around adaptive, decentralized storage methods paired with harmonized, real-time data retrieval. This approach, supported by secure protocols and end-to-end encryption, allows for swift, seamless, and fast data handling. We discuss some of the potential concerns in this environment [31].

Data Security and Encryption. In a liquid-edge intelligence environment, ensuring data security is paramount but intricate. At its core, security means protecting data from unauthorized access, alterations, and safeguarding the physical infrastructure and data transmissions across networks [31]. Edge IoT's prevalent personal data collection amplifies this need. Here, encryption serves as a pivotal defense, ensuring only authorized entities access encoded data, preserving its confidentiality and integrity [31]. However, isomorphic IoT infrastructures propose multifaceted challenges. With ever-evolving technology comes potential vulnerabilities, demanding adaptive encryption and rigorous security protocols. The dynamism of this environment intensifies the threat of data breaches, emphasizing the necessity for cohesive protective strategies and strict adherence to cross-border data transfer regulations. Ethically, this evolving paradigm complicates informed consent, potentially amplifying privacy breaches and unsolicited profiling. Issues of data ownership can arise, leading to potential conflicts and misuse. Algorithmic decisions also risk introducing biases, perpetuating inequalities, and driving constant tech upgrades, with environmental implications [3, 13, 21, 25, 36].

Data Ownership and Control. In liquid-edge intelligence, safeguarding data ownership and control is complex [40]. The interconnected ecosystem risks exposing personal information and heightens the potential for data tampering at various network points. Navigating the associated legal and regulatory challenges becomes intricate as data crosses international borders. Simultaneously, the blurred lines concerning data ownership can give rise to disputes over the intellectual property rights of data and analytical products. The dynamic nature of this system can foster data monopolies, complicating the creation of sustainable governance models. Ethically, the system might spur intrusive surveillance and unauthorized data usage, potentially encouraging discriminatory practices and widening existing social biases. The obscured nature of algorithm-driven decisions complicates accountability, possibly undermining individual autonomy and fostering environmental concerns due to increased device proliferation [13, 36].

4.2.3 Data Utilization and Sharing. Data utilization and sharing embody the streamlined management and dissemination of extensive information generated by edge IoT devices. The process aims to facilitate seamless data exchanges across the network while emphasizing robust security measures and upholding privacy standards [29]. We explore potential emergent concerns.

Data Monetization. Data monetization in this emerging landscape brings forth critical issues. The complex data flows heighten the risk of personal data exploitation and complicate obtaining informed consent from individuals, making the environment a prime target for cybercriminal activities. These complexities could foster monopolies, causing market imbalances and hurdles in fair compensation for data generators. Further, the intricate infrastructure might compromise data integrity, potentially catalyzing malicious monetization and misinformation spread. Legal complexities can arise with cross-border data transfers, burdening compliance with regional data protection laws. Ethically, this setup could violate privacy rights and control over personal data, potentially fostering exploitation and inequality. It might also accentuate existing biases and discrimination, mainly through exploitative advertising strategies, exacerbating social disparities. [7, 36].

Third-party Data Sharing The continuous movement of data across numerous nodes and external systems escalates the risk of breaches and unauthorized access, undermining data integrity and quality. Tracing data origins and pathways, critical for ensuring

authenticity, become significantly complex, especially when complying with diverse data protection regulations and contractual obligations in cross-border transfers [40]. Within this environment, third-party data sharing presents substantial ethical challenges. The complexity of securing genuine informed consent can infringe on privacy standards, escalating the risk of sensitive data mishandling by third parties and igniting severe ethical dilemmas. This setup could inadvertently intensify societal biases and foster unfair targeting of vulnerable groups. Moreover, failing to address fair compensation for data creators can exacerbate economic disparities and induce exploitation [7].

4.2.4 Surveillance and Profiling. Surveillance entails relentlessly monitoring data streams and user engagements across interconnected platforms and devices. Leveraging the intrinsic properties of IoT, many devices persistently gather, transmit, and analyze data, frequently in real-time. On the other hand, profiling involves employing data analytics to craft intricate profiles of individuals or groups, utilizing the data amassed from various IoT devices [31, 40].

Invasive surveillance. Invasive surveillance is the unrestrained monitoring of individuals, often without their consent or knowledge, facilitated by constant data collection and analysis through interconnected devices [40]. Such activity violates personal privacy by harvesting data without explicit permission and exposes sensitive information (like health, financial, or locational details) to potential misuse by unauthorized entities. This can provide a fertile ground for malicious entities to exploit the information for stalking, harassment, or manipulation through targeted content. Moreover, it can transgress legal norms, causing individuals to lose lawful control over their data, induce psychological distress, and curtail personal freedom [10]. The atmosphere created by such surveillance can cultivate a “chilling effect" in society, discouraging individuals from expressing themselves freely or engaging in open activities due to fear of continuous monitoring. This scenario also amplifies security concerns, paving the way for criminal exploitation of data for illicit activities, including identity theft and coordinated cyber-attacks, escalating the risk of cybercrime [13, 25, 26].

Mass Surveillance. Liquid edge intelligence, facilitated by isomorphic IoT infrastructure, intensifies the risk of pervasive surveillance. Interconnected IoT devices, which continuously collect detailed personal data, create a breeding ground for expansive monitoring initiatives, often bypassing individuals' consent. This network potentially violates privacy rights, with the complex nature of data flows making acquiring genuine consent challenging. Moreover, this surveillance landscape can facilitate manipulative advertising or even more malicious intentions by profiling individuals in detail. The societal implications are significant, potentially leading to a climate of self-censorship and mistrust, where individuals hesitate to express their views openly, fostering a fearful and paranoid society. Furthermore, it borders on legal gray areas, potentially conflicting with existing data protection regulations, and raises complex ethical issues, including ensuring data integrity and preventing unauthorized access in intricate data networks. Hence, liquid edge intelligence may be on the verge of ushering in an era of invasive surveillance, threatening personal privacy and societal harmony [13].

4.3 Trust

Trust is cultivated through steady, secure, and expected performances that safeguard user interests without manipulative intents. Trust helps foster a reliable relationship between users and systems, facilitating smoother interaction and collaboration [36]. It is built upon consistent, predictable, and secure performance [36].

4.3.1 Algorithms and decision-making. AI algorithms and decision-making processes are central to fostering user trust in liquid edge intelligence systems. Establishing user trust in liquid edge intelligence systems fundamentally hinges on the impartiality and reliability of AI algorithms during decision-making processes. However, algorithmic bias, stemming from flawed training data or design, can foster unjustly biased decisions, posing a severe trust concern. Algorithmic bias refers to the tendency of an AI system to make decisions that are unfairly skewed or prejudiced due to underlying issues in the data it was trained on or the algorithms' design. It can manifest in various forms and potentially lead to significant trust issues [26]. This bias can appear in multiple forms and significantly undermine user trust.

Propagation of Existing Biases Pre-trained models can perpetuate existing biases in an isomorphic IoT infrastructure, particularly when adjusting to real-world circumstances. Often originating from the initial training data, these biases can hinder the models' adaptation to diverse or changing contexts, manifesting as predictive bias. Federated learning emerges as a promising strategy in such setups, offering opportunities and challenges to enhance trust and reduce biases. Also, processing data on individual devices promises a richer and more representative dataset to curb certain biases, fostering a more reliable and responsive AI system attuned to real-world nuances. However, this approach also brings potential new biases and vulnerabilities, including data skewness and varied data quality, possibly introducing inaccurate data into the system which may prove challenging to identify and correct. Also, issues like aggregation difficulties and increased vulnerability to adversarial attacks underscore the necessity for solid frameworks to supervise ongoing monitoring and bias reduction, highlighting federated learning's role as a pathway, albeit requiring careful governance to nurture an ethically sound and trustworthy AI environment [26].

Amplification through Integration. The concept of amplification through integration highlights the potential escalation of existing biases during the merger of various data sources or systems. This process can exacerbate biases found in individual datasets, possibly fostering more significant biases or unveiling new ones in the combined system. Techniques like federated learning, which can bolster Liquid AI, seek to build a diversified learning base. However, it can inadvertently cultivate heightened biases sourced from localized datasets, especially in isomorphic IoT infrastructures. This amplification can occur through numerous channels, such as intricate data integration and potentially flawed aggregation strategies that may overemphasize certain data types or devices, further accentuating existing biases. Moreover, the integrated learning environment might foster feedback loops, where biases from one area can influence learning in another, creating a network effect that globally escalates biases [14, 36, 44].

Limited Flexibility to Adapt: Limited Flexibility to Adapt refers to the potential restriction in the agility of AI systems to

adjust swiftly to new data trends, demands, or challenges. Despite being designed for adaptability, the intricacies and complexity of an isomorphic IoT architecture might occasionally hinder progress. For instance, in liquid edge intelligence, employing tools like Wasm modules in deploying pre-trained AI models [16, 22] presents a double-edged sword. While it fosters stability and efficiency, it could constrain the system's capacity to readily adjust to new or complex scenarios markedly differing from its initial training conditions, partly due to fixed learning parameters [6]. Moreover, the symbiotic relationship of various components in a dynamic IoT infrastructure makes rapid adaptations or adjustments a complex task, potentially risking system stability. Given the interdependent nature of liquid edge intelligence, modifications to one part may necessitate parallel changes in several other components, ensuring system coherence and functionality. Thus, despite offering seamless data interaction and real-time processing, dynamic liquid edge intelligence systems might face challenges in swiftly and efficiently adapting to evolving scenarios or needs [15, 26, 43]. This limited flexibility can hamper the timely incorporation of necessary safeguards or updates meant to enhance user privacy or data security, thus potentially putting users at risk of data breaches or other forms of exploitation.

Interoperability Issues: Interoperability challenges in dynamic liquid edge intelligence environments can stem primarily from different devices and modules' varied characteristics and operational standards. These differences can cause data format inconsistencies and communication protocol conflicts, hampering smooth data flow and complicating real-time analytics. Addressing this requires careful strategizing to enhance compatibility and streamline system functions. Using tools like orchestrators [16] can potentially mitigate some complexities, facilitating better synchronization between components. However, the efficacy of an orchestrator hinges on its design and capabilities. It may struggle to integrate newer technologies or adapt to unexpected shifts in network dynamics, potentially introducing new vulnerabilities and becoming a target for cyber-attacks that aim to disrupt network harmony. Ethically, these issues essentially erode trust in AI algorithms and decision-making processes. The potential for data breaches and unauthorized access may cultivate mistrust among users, heightening concerns about privacy violations and data misuse and thereby increasing user skepticism and reluctance.

4.3.2 Security of IoT Infrastructures. Trust in IoT infrastructure security signifies users' and stakeholders' confidence in the protective measures instituted within IoT ecosystems to safeguard data and facilitate stable device interconnectivity. Trust also encapsulates the physical safety of individuals, given the frequent management of critical infrastructure components by these networks [29, 31].

Security breaches: Security breaches, typically unauthorized intrusions, result in potential data misuse, alteration, or destruction. Often arising from system vulnerabilities, poor encryption, or advanced cyber-attacks, these breaches primarily lead to data theft and tampering [29, 31]. In the developing isomorphic IoT infrastructures for liquid edge intelligence, where data flows are decentralized, the risk magnifies. Malware might exploit real-time data gaps, undermining AI's capabilities. Advanced AI-powered phishing schemes can easily deceive users, while open tools like Wasm could inadvertently permit data interception. The decentralized nature of this infrastructure also makes it a ripe target for zero-day attacks and internal threats, complicating data ownership and accountability. Ethically, such breaches stir debates on privacy and unauthorized data use, introducing manipulative methods and significant societal concerns [1, 26].

Transparency and Accountability. Transparency and accountability denote the clarity and openness surrounding the decision-making processes of AI systems and the responsibility taken for the outcomes and actions produced by these systems [14]. Transparency and accountability are pivotal concerns in an isomorphic IoT infrastructure's intricate and decentralized nature. The inherent complexity of the algorithms and the continuous evolution and adaptation of these AI systems pose a significant challenge in maintaining a transparent operational modality. As these systems dynamically adapt based on a constant stream of new data, pinpointing the exact influences and pathways leading to specific decisions becomes increasingly difficult. This dynamic nature might foster unpredictability, potentially impeding the clear documentation of processes, thereby raising substantial hurdles in preserving transparency. Furthermore, the decentralized structure of these systems diffuses responsibility, complicating the task of attributing errors or decisions to specific entities. This dispersion of accountability can muddle the identification of mistakes' origins and the delineation of responsibility for rectifications. These issues can potentially undermine trust and raise legal and ethical concerns, including violations of privacy rights and the propagation of inequality and discrimination [13].

4.4 Limitation

This research acknowledges the limitations arising from the limited number of references available. The inherent limitations due to scarce resources are acknowledged. Yet, it stimulates innovative approaches, scholarly discourse, and critical thinking in this emerging domain.

5 CONCLUSIONS

Innovations like Liquid AI, driven by the rapid advancement of isomorphic architectures, bring latent privacy and trust vulnerabilities to the forefront. This study explores the privacy and trust challenges these technologies face, emphasizing their impact on building trustworthy AI. We highlight the heightened risk of security breaches that can lead to unauthorized data manipulation. Additionally, maintaining transparency and accountability in these complex, evolving systems becomes critical, especially given the decentralized nature of AI algorithms in isomorphic IoT frameworks.

This research serves as a precursor to more in-depth investigations, illustrating the inherent privacy and trust issues. Future research will foster empirical studies to scrutinize further and validate the identified vulnerabilities, creating a robust foundation for developing trustworthy systems. Equally crucial is the initiation of a profound discourse and research on the ethical dimensions of these technologies, facilitating the formulation of ethical guidelines and frameworks adept at safeguarding user rights and privacy.

REFERENCES

[1] Mohamed Abomhara and Geir M Køien. 2014. Security and privacy in the Internet of Things: Current status and open issues. In *2014 international conference on privacy and security in mobile systems (PRISMS)*. IEEE, 1–8.

[2] AS Albahri, Ali M Duhaim, Mohammed A Fadhel, Alhamzah Alnoor, Noor S Baqer, Laith Alzubaidi, OS Albahri, AH Alamoodi, Jinshuai Bai, Asma Salhi, et al. 2023. A systematic review of trustworthy and explainable artificial intelligence in healthcare: Assessment of quality, bias risk, and data fusion. *Information Fusion* (2023).

[3] Yehia I Alzoubi, Valmira H Osmanaj, Ashraf Jaradat, and Ahmad Al-Ahmad. 2021. Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy* 4, 2 (2021), e145.

[4] Sadiq Ur Rehman Aqeel-ur Rehman, Iqbal Uddin Khan, Muzaffar Moiz, and Sarmad Hasan. 2016. Security and privacy issues in IoT. *International Journal of Communication Networks and Information Security (IJCNIS)* 8, 3 (2016), 147–157.

[5] Luiz Bittencourt, Roger Immich, Rizos Sakellariou, Nelson Fonseca, Edmundo Madeira, Marilia Curado, Leandro Villas, Luiz DaSilva, Craig Lee, and Omer Rana. 2018. The internet of things, fog and cloud continuum: Integration and challenges. *Internet of Things* 3 (2018), 134–155.

[6] Misha Denil, Babak Shakibi, Laurent Dinh, Marc'Aurelio Ranzato, and Nando De Freitas. 2013. Predicting parameters in deep learning. *Advances in neural information processing systems* 26 (2013).

[7] Farshad Firouzi, Bahar Farahani, Mojtaba Barzegari, and Mahmoud Daneshmand. 2020. AI-driven data monetization: The other face of data in IoT-based smart and connected health. *IEEE Internet of Things Journal* 9, 8 (2020), 5581–5599.

[8] Andrea Gallidabino, Cesare Pautasso, Tommi Mikkonen, Kari Systa, Jari-Pekka Voutilainen, and Antero Taivalsaari. 2017. Architecting liquid software. *Journal of Web Engineering* (2017), 433–470.

[9] Julien Gedeon, Florian Brandherm, Rolf Egert, Tim Grube, and Max Mühlhäuser. 2019. What the fog? edge computing revisited: Promises, applications and future challenges. *IEEE Access* 7 (2019), 152847–152878.

[10] Giammaria Giordano, Fabio Palomba, and Filomena Ferrucci. 2022. On the use of artificial intelligence to deal with privacy in IoT systems: A systematic literature review. *Journal of Systems and Software* 193 (2022), 111475.

[11] Ramin Hasani, Mathias Lechner, Alexander Amini, Lucas Liebenwein, Aaron Ray, Max Tschaikowski, Gerald Teschl, and Daniela Rus. 2022. Closed-form continuous-time neural networks. *Nature Machine Intelligence* (2022), 1–12.

[12] High-Level Expert Group on Artificial Intelligence (AI HLEG). 2019. *Ethics Guidelines for Trustworthy AI*. Technical Report. European Commission.

[13] Haochen Hua, Yutong Li, Tonghe Wang, Nanqing Dong, Wei Li, and Junwei Cao. 2023. Edge computing with artificial intelligence: A machine learning perspective. *Comput. Surveys* 55, 9 (2023), 1–35.

[14] Anna Jobin, Marcello Ienca, and Effy Vayena. 2019. The global landscape of AI ethics guidelines. *Nature machine intelligence* 1, 9 (2019), 389–399.

[15] C Kaspar, BJ Ravoo, Wilfred G van der Wiel, SV Wegner, and WHP Pernice. 2021. The rise of intelligent matter. *Nature* 594, 7863 (2021), 345–355.

[16] Pyry Kotilainen, Ville Heikkilä, Kari Systä, and Tommi Mikkonen. 2023. Towards Liquid AI in IoT with WebAssembly: A Prototype Implementation. In *International Conference on Mobile Web and Intelligent Information Systems*. Springer, 129–141.

[17] Pranjal Kumar, Siddhartha Chauhan, and Lalit Kumar Awasthi. 2023. Artificial intelligence in healthcare: review, ethics, trust challenges & future research directions. *Engineering Applications of Artificial Intelligence* 120 (2023), 105894.

[18] Mathias Lechner, Ramin Hasani, Alexander Amini, Thomas A Henzinger, Daniela Rus, and Radu Grosu. 2020. Neural circuit policies enabling auditable autonomy. *Nature Machine Intelligence* 2, 10 (2020), 642–652.

[19] Zhihan Lv and Liang Qiao. 2020. Optimization of collaborative resource allocation for mobile edge computing. *Computer Communications* 161 (2020), 19–27.

[20] Liye Ma and Baohong Sun. 2020. Machine learning and AI in marketing–Connecting computing power to human insights. *International Journal of Research in Marketing* 37, 3 (2020), 481–504.

[21] Niko Mäkitalo et al. 2018. Architecting the Web of Things for the fog computing era. *IET Software* 12, 5 (2018), 381–389.

[22] Niko Mäkitalo, Tommi Mikkonen, Cesare Pautasso, Victor Bankowski, Paulius Daubaris, Risto Mikkola, and Oleg Beletski. 2021. WebAssembly modules as lightweight containers for liquid IoT applications. In *International Conference on Web Engineering*. Springer, 328–336.

[23] Tommi Mikkonen, Cesare Pautasso, and Antero Taivalsaari. 2021. Isomorphic internet of things architectures with web technologies. *Computer* 54, 7 (2021), 69–78.

[24] Tommi Mikkonen, Kari Systä, and Cesare Pautasso. 2015. Towards liquid web applications. In *Engineering the Web in the Big Data Era: 15th International Conference, ICWE 2015, Rotterdam, The Netherlands, June 23-26, 2015, Proceedings 15*. Springer, 134–143.

[25] Jessica Morley, Luciano Floridi, Libby Kinsey, and Anat Elhalal. 2020. From what to how: an initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and engineering ethics* 26, 4 (2020), 2141–2168.

[26] Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. 2021. Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials* 23, 4 (2021), 2384–2428.

[27] Aleksandr Ometov, Oliver Liombe Molua, Mikhail Komarov, and Jari Nurmi. 2022. A survey of security in cloud, edge, and fog computing. *Sensors* 22, 3 (2022), 927.

[28] Ella Peltonen, Mehdi Bennis, Michele Capobianco, Merouane Debbah, Aaron Ding, Felipe Gil-Castiñeira, Marko Jurmu, Teemu Karvonen, Markus Kelanti, Adrian Kliks, et al. 2020. 6G white paper on edge intelligence. *arXiv preprint arXiv:2004.14850* (2020).

[29] Rodrigo Roman, Jianying Zhou, and Javier Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer networks* 57, 10 (2013), 2266–2279.

[30] Weisong Shi, Jie Cao, Quan Zhang, Youhuizi Li, and Lanyu Xu. 2016. Edge computing: Vision and challenges. *IEEE internet of things journal* 3, 5 (2016), 637–646.

[31] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K Markakis. 2020. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 1191–1221.

[32] Richard Swedberg. 2020. Exploratory research. *The production of knowledge: Enhancing progress in social science* (2020), 17–41.

[33] Kari Systä, Cesare Pautasso, Antero Taivalsaari, and Tommi Mikkonen. 2023. LiquidAI: Towards an Isomorphic AI/ML System Architecture for the Cloud-Edge Continuum. In *International Conference on Web Engineering*. Springer, 67–74.

[34] Antero Taivalsaari, Tommi Mikkonen, and Cesare Pautasso. 2021. Towards Seamless IoT Device-Edge-Cloud Continuum: Software Architecture Options of IoT Devices Revisited. In *ICWE 2021 Workshops: ICWE 2021 International Workshops, BECS and Invited Papers, Biarritz, France, May 18–21, 2021, Revised Selected Papers*. Springer, 82–98.

[35] Antero Taivalsaari, Tommi Mikkonen, and Kari Systä. 2014. Liquid software manifesto: The era of multiple device ownership and its implications for software architecture. In *2014 IEEE 38th Annual Computer Software and Applications Conference*. IEEE, 338–343.

[36] Scott Thiebes, Sebastian Lins, and Ali Sunyaev. 2021. Trustworthy artificial intelligence. *Electronic Markets* 31 (2021), 447–464.

[37] Usman Wajid, Alexandros Nizamis, and Victor Anaya. 2022. Towards Industry 5.0–A Trustworthy AI Framework for Digital Manufacturing with Humans in Control. *Proceedings http://ceur-ws. org ISSN* 1613 (2022), 0073.

[38] Wenfei Wan, Ya Meng, Bin Shang, Xiaobing Li, Bing Mo, and Shuang Rong. 2022. Reliability Assessment Scheme for Intelligent Autonomous System. In *2022 13th International Conference on Reliability, Maintainability, and Safety (ICRMS)*. IEEE, 285–289.

[39] Robert Philip Weber. 1990. *Basic content analysis*. Vol. 49. Sage.

[40] Tingting Yang, Meng Qin, Nan Cheng, Wenchao Xu, and Lian Zhao. 2022. Liquid software-based edge intelligence for future 6G networks. *IEEE Network* 36, 1 (2022), 69–75.

[41] Yilong Yang, Quan Zu, Peng Liu, Defang Ouyang, and Xiaoshan Li. 2018. MicroShare: Privacy-preserved medical resource sharing through microservice architecture. *International journal of biological sciences* 14, 8 (2018), 907.

[42] Ashkan Yousefpour, Caleb Fung, Tam Nguyen, Krishna Kadiyala, Fatemeh Jalali, Amirreza Niakanlahiji, Jian Kong, and Jason P Jue. 2019. All one needs to know about fog computing and related edge computing paradigms: A complete survey. *Journal of Systems Architecture* 98 (2019), 289–330.

[43] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang. 2017. A survey on the edge computing for the Internet of Things. *IEEE access* 6 (2017), 6900–6919.

[44] Liang Zhao, Weiliang Zhao, Ammar Hawbani, Ahmed Y Al-Dubai, Geyong Min, Albert Y Zomaya, and Changqing Gong. 2020. Novel online sequential learning-based adaptive routing for edge software-defined vehicular networks. *IEEE Transactions on Wireless Communications* 20, 5 (2020), 2991–3004.