The Impact of Edge Computing on the Industrial Internet of Things

Nkata Sekonya[1] and Siphesihle Sithungu[2]
University of Johannesburg, Johannesburg, South Africa

nkatasekonya61@gmail.com
siphesihles@uj.ac.za

Abstract: The emergence of the Industrial Internet of Things (IIoT) has improved the management of industrial operations and processes. IIoT involves collecting and processing data from a vast array of sensors deployed across industrial complexes. This enables the measurement of the efficiency of industrial processes, monitoring the health of machinery, optimisation of operations, and response to real-time events. In its application, IIoT underpins the operation of critical infrastructure in sectors including manufacturing and utilities. Maintaining the availability and resilience of critical infrastructure against internal and external threats is essential to minimise disruptions that could have a debilitating effect on a nation's economy. Although internal threats can lead to a critical infrastructure's downtime, external threats through cyberattacks also pose a significant threat. Historical events have demonstrated that the successful disruption of critical infrastructure can lead to the loss of human life, the interruption of necessary economic activities and national security concerns. Therefore, the availability of resilient critical infrastructures is vital to the well-being of a country. In this context, the paper compares the deployment of traditional IIoT to that of edge computing for the storage and processing of data. Traditional IIoT relies on a centralised server for data storage and processing, which is insufficient as IIoT environments cannot tolerate delays in responding to real-time events. Conversely, edge computing allows for data processing at the edge, closer to the data source, which plays a crucial role in enabling IIoT devices to respond to real-time events by reducing decision-making latency. Moreover, the decentralised nature of edge computing reduces the reliance on a centralised server by only sending required data to the cloud for further processing. Although edge computing enhances IIoT deployments, a notable concern is a resultant increase in the attack surface of IIoT environments, which consequently restricts its implementation. Exploratory research is conducted to explore the integration of edge computing into IIoT environments with a focus on improving the management and operation of critical infrastructures. A review of the current literature is performed to identify and discuss security concerns prevalent in edge computing-enabled IIoT environments and proposed mitigation strategies.

Keywords: Industrial Internet Of Things, Edge Computing, Critical Infrastructure, Cybersecurity

1. Introduction

The "Internet of Things" (IoT) refers to a network of devices with sensors and actuators that use the internet as a communication medium to gather, process, and transfer data (Koohang et al., 2022). IoT has gained popularity in human-centric applications since its inception, including connected homes, smart watches, and productivity software. As IoT expanded from human-centric applications to control industrial processes, the "Industrial Internet of Things" (IIoT) came into existence. A subset of IoT called IIoT is focused on the security and efficiency of industrial processes (Bhaiyat and Sithungu, 2022). The development of the IIoT has the potential to enhance critical infrastructure sectors, including manufacturing and utilities' management and operation. The IIoT establishes data gathering and analysis from a variety of sensor-equipped industrial equipment, enabling better industrial process efficiency, data-driven decision-making, monitoring the health of industrial machinery and optimising operations (Qiu et al., 2020). Since critical infrastructure sectors cannot tolerate delays in responding to real-time events, traditional IIoT setups that rely on a central server for storage and processing are insufficient (Qiu et al., 2022). By processing the data closer to the source, edge computing lowers the latency associated with data transfer to a centralised server (Mirani et al., 2022). However, edge computing is not without its critical flaws. The expanded attack surface that edge computing introduces to IIoT systems is a significant issue that limits its incorporation into IIoT environments. The objective of this paper is to conduct a literature review on the current state of edge computing in IIoT environments, with an emphasis on enhancing the management and operation of critical infrastructures. Security concerns common in edge computing-enabled IIoT environments are identified and discussed, together with proposed mitigation strategies.

To accomplish this objective, the paper is structured as follows: Section 2 discusses cloud, fog, and edge computing in the context of IIoT. Section 3 delves into the integration of edge computing into IIoT environments. Section 4 discusses the role of edge computing in improving critical infrastructure management and operation. Section 5 discusses the security concerns prevalent in edge-computing-enabled IIoT environments, as well as approaches to securing these environments. Section 6 concludes the paper.

2. Cloud, Fog, and Edge Computing

The "Industrial Internet of Things" (IIoT) establishes the collection, communication, and processing of data from a vast array of sensors deployed across industrial complexes (Goswami, Jadav and Soni, 2022). IIoT is an extension of the "Internet of Things", focusing on the industrial applications of IoT. IIoT acts as a catalyst to enhance the management of industrial processes and operations, allowing for monitoring of the health of machinery, optimisation of operations, and response to real-time events. The Industrial Internet Reference Architecture (IIRA) is an open architecture for the industrial internet (Pivoto et al., 2021). The IIRA presents a functional view of an IIoT deployment typical across industries. The functional domains and crosscutting functions are concerned with the functionality of a system, while the system requirements are concerned with efficiency, i.e., how well the system works (Industrial Internet Consortium, 2019). Figure 1 depicts the functional domains, crosscutting functions, and system requirements of IIoT environments.

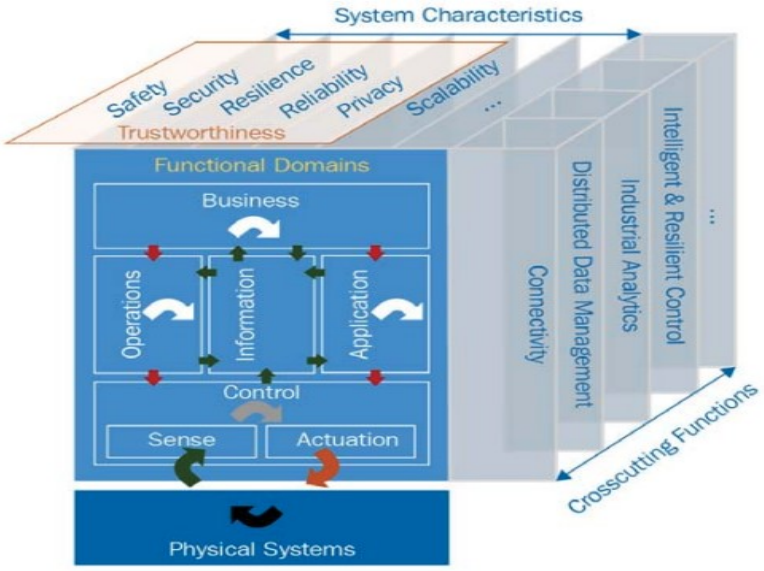

Figure 1: IIRA functional domains, crosscutting functions, and system requirements (Industrial Internet Consortium, 2019)

The requirements of IIoT systems include scalability, efficient storage management, fault tolerance, security, computational proximity, data transfer, latency minimisation, and safety assurances (Industrial Internet Consortium, 2019; Chalapathi et al., 2021; Zhang, Li and Chen, 2021; Sittón-Candanedo et al., 2019). Computing infrastructure is necessary for IIoT environments to store and process data that has been acquired. There are also several computing paradigms to be explored in relation to IIoT, such as cloud, fog, and edge computing. For IIoT contexts, some computer paradigms are more efficient than others. As such, the remainder of this section reviews cloud, fog, and edge computing.

2.1 Cloud Computing

Cloud computing refers to the practice of leasing computer resources from a centralised pool of shared capacity, with consumption taking place over the Internet (Zhang, Li and Chen, 2021). Cloud computing is an enabler of IoT because it provides scalable computing resources and data storage for IoT sensors. Traditional cloud computing, on the other hand, is insufficient for IIoT environments, where delays in responding to real-time events are unacceptable. The requirements of IIoT environments include low latency, reliable communication, and security, which existing cloud infrastructure can hardly meet (Angel et al., 2021), especially as IIoT devices continue to generate large amounts of data.

Other cloud computing limitations include the location of the centralised servers, as some countries may have laws prohibiting the storage of critical data in other countries (Basir et al., 2019). Computing and storage resources in a cloud computing setup may be exhausted as all data collected by IIoT sensors is transferred to a centralised server for storage and processing (Mirani et al., 2022). To offload the burden on the servers, processes must be in place to determine the criticality of the data before processing. By bringing resources closer to the IIoT environment, fog computing aims to address challenges encountered in IIoT environments that rely on centralised servers.

2.2 Fog Computing

Fog computing is a cloud computing extension that provides a bridge from the data centre to the edge to reduce network latency (Caiza et al., 2020). A fog computing network comprises nodes closer to the IIoT environment, with each node acting as a lightweight version of a cloud computing server (Caiza et al., 2020). This is done to offload the processing burden and shorten the time it takes to process and analyse the collected data (Mirani et al., 2022). In the management of IIoT environments, fog computing outperforms traditional cloud computing. Fog computing is less centralised than cloud computing and does not have a single point of failure (Zhang, Li and Chen, 2021).

2.3 Edge Computing

Edge computing provides an advantage over cloud and fog computing by allowing data processing at the edge, reducing the resources required for cloud computing by sending only the required data to the cloud for further processing (Mirani et al., 2022). Edge computing reduces data transfer latency, allowing for quick responses to real-time events. Edge computing also reduces the computing and storage requirements of cloud servers, lowering the cost of running the cloud infrastructure significantly (Basir et al., 2019). Figure 2 depicts the various computing paradigms.

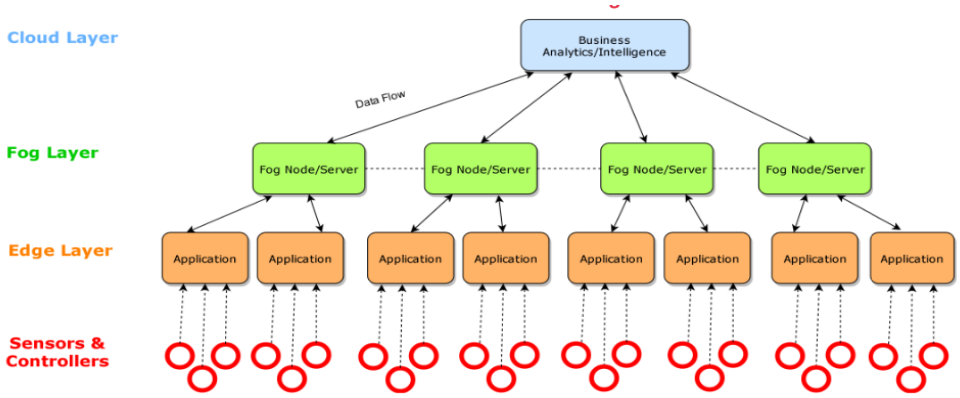

Figure 2: Industrial IoT data processing layer stack (Chalapathi et al., 2021)

The purposes of cloud, fog, and edge computing are similar in that they all aim to provide scalable computing and storage resources. The difference is in how the targets are met; cloud computing offers these resources through servers located in remote locations. By deploying lightweight servers closer to the IIoT environment, fog computing creates a bridge between the IIoT environment and the cloud. These resources are provided at the *edge*. Table 1 presents a comparison of cloud, fog, and edge computing. The following section goes over the role of edge computing in IIoT.

Table 1: Comparison between cloud, fog, and edge computing

Criteria	Cloud Computing	Fog Computing	Edge Computing
Deployment Nature	Relies on centralised servers in remote data centres for storage and computation	Acts as a bridge between remote data centres and the data source, with fog computing nodes acting as a lightweight version of a cloud computing server	Deployed at the network edge, closer to the data source
Computing and Storage Capacity	Scalable	Fairly Scalable	Limited
Advantages	Provides scalable computing resources and data storage	Offers improved data transfer compared to cloud computing	Reduced data transfer latency, enabling prompt response to real-time events
Disadvantages	Increased data transfer latency because of the distance between the data source and remote servers	Exhibits centralisation as it relies on relatively few fog nodes	Limited computing and storage capacity

3. The Integration of Edge Computing into Industrial IoT

Traditional IIoT devices have limited resources and cannot efficiently store and process data collected in IIoT environments (Khan et al., 2020). Conventionally, this issue was addressed by having the IIoT device send data to centralised servers for storage and processing. However, delays in data transfer to centralised servers made it difficult for IIoT devices to respond to real-time events promptly (Basir et al., 2019). Edge computing was proposed as a solution for reducing data transfer latency by performing computations on the network's edge, which is close to the data source (Mirani et al., 2022). Only the necessary data is transferred to the centralised server for further processing in an edge computing environment, reducing the latency associated with data transfer (Qiu et al., 2020).

IIoT deployments must meet requirements such as data transfer latency minimisation, computational proximity, scalability, efficient storage management, fault tolerance, security, cost-effectiveness, interoperability between heterogeneous IIoT systems, and safety assurances to be a viable option for industrial applications (Industrial Internet Consortium, 2019; Chalapathi et al., 2021; Zhang, Li and Chen, 2021; Sittón-Candanedo et al., 2019). Additionally, IIoT should allow for consistent management and operation of industrial processes. IIoT environments with edge computing capabilities are scalable because increased data transfer can be addressed by adding more edge nodes. These additional edge nodes should be able to raise data transfer capacity while reducing network latency (Chalapathi et al., 2021). Edge computing also enables efficient offloading strategies for determining which processes should be computed at the network core and which at the edge (Zhang, Li and Chen, 2021). Edge computing nodes enable effective storage management by distributing data around the network's edge, increasing network resilience, and sparing storage resources by only transferring the necessary data to the centralised servers (Sittón-Candanedo et al., 2019).

Because IIoT environments are distributed, edge computing ensures fault tolerance. The failure of one edge device should not bring the entire network to a halt. In a centralised cloud computing environment, this type of fault tolerance is difficult to achieve because the disruption of a centralised server will halt network operation, rendering IIoT devices useless (Chalapathi et al., 2021). Cloud computing environments present a single point of failure compared to edge computing environments. Due to their distributed nature, edge computing devices help to ensure the security of the data collected to some extent. To gain access to any useful information, a threat actor would need to compromise many edge devices (Sittón-Candanedo et al., 2021). A compromise of one edge device may be ineffective. Data privacy is also ensured by the isolation of each network node (Qiu et al., 2020).

IIoT devices produce vast volumes of data that must be transferred (Qiu et al., 2020). Edge computing nodes communicate only the required information, minimising the quantity of data that must be stored and processed in cloud computing environments (Angel et al., 2021). The development of reference architectures to standardise the integration of edge computing into IIoT systems is receiving more attention from industry and academia (Qiu et al., 2020). Since it guarantees consistent outcomes across different edge computing implementations, this will accelerate the adoption of edge computing. By standardising the collected data into a format understood by systems in the upper tiers of the IIoT stack, edge computing nodes can promote interoperability across systems in IIoT environments (Antao et al., 2018). Edge computing nodes also enable quick problem detection in IIoT contexts, safeguarding industrial and worker safety (Angel et al., 2021).

Industries requiring reliable data collection and processing for time-sensitive projects have adopted this computing paradigm due to the performance gains brought about by the integration of edge computing into IIoT systems (Sittón-Candanedo et al., 2019). Manufacturing, mining, transportation, and healthcare are a few of these. To better deliver medical services like the monitoring of ECG data and the processing of MRI data, the healthcare industry has begun implementing IIoT technologies (Chalapathi et al., 2021). However, the majority of these solutions rely on cloud-based processing and storage, which is inconvenient for time-sensitive operations such as responding to heart attacks. Due to the benefits of reduced latency and improved reliability, there has been a gradual shift towards edge-enabled IIoT. Table 2 depicts the benefits of incorporating edge computing into IIoT environments.

Table 2: The Integration of edge computing into IIoT

IIoT Requirement	Edge Computing Enhancement
Minimisation of the latency associated with data transfer; Computational Proximity	Computations are performed on the edge of the network, closer to data sources
Scalability	Increased data transfer can be addressed by the introduction of additional edge nodes
Storage and Computational Offloading	Computations are performed at the edge; only necessary data is sent for further processing at the network core
Efficient Storage Management	Storage is distributed across the edge of the network ensuring increased resilience
Fault Tolerance	The distributed nature of edge computing ensures fault tolerance
Security	The distributed nature of edge computing environments makes it difficult to compromise
Cost Effectiveness	Only necessary data is transferred to the cloud, reducing the cost associated with storage and processing
Consistent management and operation of industrial processes	Reference architectures ensure consistent results from the deployment of edge computing
Interoperability between heterogeneous IIoT systems	Nodes can format the collected data in a manner understandable to systems in the upper layers on the IIoT stack
Safety	Allows for the timely detection of faults in IIoT environments

Although edge computing has improved the efficiency of IIoT environments, significant issues exist that impede its growth, the most important of which is security (Zeyu et al., 2020). Edge computing devices are typically placed in easily accessible areas, posing a security risk to the devices. Because these devices have limited resources and are relatively complex, traditional security mechanisms are difficult to implement. The following section discusses the security concerns prevalent in edge computing devices.

4. Security Concerns of Edge Computing in IIoT

IIoT underpins the operation and management of critical infrastructures, meaning cyberattacks targeted at IIoT environments can cause disruptions in crucial economic activities. They can lead to devastating effects on the health and safety of industrial workers (Angel et al., 2021). The integration of edge computing further increases the attack surface in IIoT environments, especially if it involves the addition of dedicated edge devices, which present difficulties in assuring security. The following subsections discuss security concerns resulting from the integration of edge computing into IIoT environments, with table 3 summarising the reviewed literature.

4.1 Internal Threats

Many contexts, including edge computing, frequently experience internal threats. Internal threats include malicious attacks such as sabotage and unintentional attacks brought on by human error or ineptitude (Gaidarski and Minchev, 2021). Employees who are not adequately trained to carry out their responsibilities securely pose a security risk to the company. In addition, disgruntled employees constitute a severe threat to the company's security. The deployment of malicious software in edge computing environments and the unintentional disclosure or deletion of sensitive data are two examples of threats in this category. Training personnel to carry out their responsibilities appropriately and securely is one measure to prevent internal hazards (Bhaiyat and Sithungu, 2022). Another measure is behaviour analysis and risk profiling (Gaidarski and Minchev, 2021).

4.2 Identification and Authentication

Mechanisms for identification and authentication focus on allowing only authorised users to access the system (Alwakeel, 2021). This involves the identification and authentication of IIoT devices in the context of edge computing and IIoT. Edge computing environments in IIoT contain many devices, making it challenging to identify rogue devices (Zhang, Li and Chen, 2021). An IIoT network can be breached using rouge devices as the first attack vector (Husain and Askar, 2021). Hardware-based authentication methods and access control monitoring are examples of mitigations that can prevent authentication-based intrusions (Chalapathi et al., 2021).

4.3 Authorization

Authorisation is concerned with access rights, which in the context of edge computing refers to the actions an edge node is permitted to perform (Zhao et al., 2021). Edge computing node access rights can pose security issues. A compromise of an edge node in an IIoT environment with overreaching access rights can result in

privilege escalation, which could grant an attacker further control of the IIoT network (Qiu et al., 2020). To protect against this type of attack, edge computing nodes should be granted only the access rights required to carry out their duties (Zhao et al., 2021).

4.4 Data Security

Vast volumes of data are produced in edge and IIoT contexts. Although this data enables data-driven decision-making, security issues with the data's storage and transmission exist. Compromises to the data's availability, confidentiality, and integrity are among the security threats (Chalapathi et al., 2021). Such compromises may result in the modification of critical data, resulting in system failures (Zhang, Li and Chen, 2021). Mitigations include employing mechanisms to perform integrity checks, using lightweight encryption mechanisms to avoid sensitive data disclosure, and implementing Denial of Service (DoS) protections (Parikh et al., 2019).

4.5 Network Attacks

Edge computing employs a variety of communication networks, including wired and wireless networks, as well as the internet (Roman, Lopez and Mambo, 2018). These communication networks introduce security risks that could potentially disrupt critical infrastructure operations. Denial of Service (DoS) attacks, which prevent legitimate users from accessing network resources, and Man in the Middle attacks, which can result in information disclosure, modification, and destruction, are examples of attacks in this category (Roman, Lopez and Mambo, 2018). Mitigation strategies include using Intrusion Detection and Prevention Systems (IDPS) to detect and prevent network attacks (Parikh et al., 2019). Furthermore, systems in the edge computing environment should be isolated to avoid lateral movement by threat actors (Bhaiyat and Sithungu, 2022).

4.6 Side Channel Attacks

Side Channel attacks attempt to exploit a system by gathering publicly available information to deduce sensitive private information (Patil et al., 2020). Communication protocols and embedded sensors are popular side channels in edge computing systems (Xiao et al., 2019). The systems may leak some operational data, which threat actors may use to deduce sensitive information. Side channel attacks can be mitigated by randomising publicly available data to avoid targeted attacks and restricting side channels altogether (Xiao et al., 2019).

Table 3: Security concerns and countermeasures

Security Issue	Examples	Countermeasures	References
Internal Threats	Accidental disclosure or deletion of critical data, deployment of malicious software	Employee training, Behaviour analysis and risk profiling	(Bhaiyat and Sithungu, 2022); (Gaidarski and Minchev, 2021);
Identification and Authentication	Rogue IIoT devices	The implementation of hardware-based authentication schemes, monitoring of access control attempts	(Zhang, Li and Chen, 2021); (Husain and Askar, 2021); (Chalapathi et al., 2021)
Authorisation	Privilege escalation	Limited access rights	(Qiu et al., 2020); (Zhao et al., 2021)
Data Security	Compromises to the confidentiality, integrity, and availability of data in storage or transmission	The implementation of integrity validation and encryption mechanisms, Denial of Service protection	(Parikh et al., 2019); (Chalapathi et al., 2021); (Cao et al., 2020)
Side Channel Attacks	Inference of sensitive information	Restrictions of side channels, randomisation of publicly available data to avoid targeted attacks	(Xiao et al., 2019); (Patil et al., 2020)
Network Attacks	Denial of Service (DoS) and man-in-the-middle attacks	Network segmentation and the deployment of Intrusion Detection and Prevention systems	(Roman, Lopez and Mambo, 2018); (Husain and Askar, 2021); (Parikh et al., 2019)
Legacy Systems	Known attacks on outdated systems	Change and vulnerability management	(Patil et al., 2020)
Physical Security	Physical damage and tampering with the device	Physical security measures such as guards, barriers, strict access controls and CCTV cameras	(Roman, Lopez and Mambo, 2018)
Digital Forensics Readiness	Poor effectiveness and efficiency of digital forensic investigations	Establish mechanisms to collect and perverse potential digital evidence	(Kebande, Karie and Venter, 2018); (Stoyanova et al., 2020); (Shalaginov, Iqbal and Olegård, 2020);

4.7 Legacy Systems

Edge computing is essential to operating critical infrastructures that cannot afford downtime. Furthermore, edge computing is used in environments that run legacy systems not built with security in mind (Bhaiyat and Sithungu, 2022). Edge nodes are thus vulnerable to cyber-attacks. Other issues that arise as a result of the use of legacy systems include the management and deployment of updates, which include security updates (Patil et al., 2020). Change and vulnerability management should be employed to better prepare for attacks and manage vulnerabilities of legacy systems.

4.8 Physical Security

By bringing edge nodes closer to IIoT devices, edge computing lowered the latency associated with data transfer to centralised cloud servers, raising questions about physical security. Threat actors can physically harm edge nodes and IIoT devices if there are no physical security measures in place (Khan et al., 2020). Critical infrastructure operations may be disrupted as a result of the physical damage, endangering human life. Security guards, physical barriers that restrict access to IIoT locations, and CCTV cameras are examples of mitigations against physical damage (Roman, Lopez and Mambo, 2018).

4.9 Digital Forensics Readiness

Edge computing integration into IIoT environments introduces new challenges to the field of digital forensics (Stoyanova et al., 2020). The vast amounts of data produced in IIoT environments can aid digital forensics investigations. However, the variety of devices, distributed nature, and non-standard formats present challenges (Stoyanova et al., 2020). Previously, (Kebande, Karie and Venter, 2018) proposed an IoT architecture incorporating Digital Forensics Readiness (DFR) as a security component in IoT environments. DFR ensures the efficiency and effectiveness of digital forensics investigations by establishing mechanisms for gathering and preserving evidence in the event of a security incident (Kebande, Karie and Venter, 2018). Digital forensics readiness in edge computing environments is still in its early stages. (Shalaginov, Iqbal and Olegård, 2020) present a methodology for digital forensics readiness in edge computing environments in their research.

5. How Edge Computing can transform critical infrastructure sectors

The management and operation of critical infrastructures may change as a result of edge computing-enabled IIoT. This is significant since a nation's economic health depends on its critical infrastructure (Lanz, 2022). Because they are distributed, edge computing systems are fault resistant; a disruption on one node should not affect others. For critical infrastructures that cannot afford downtimes, this is transformational. Critical infrastructure sectors can potentially become more resilient to attacks and disruptions when the advantages provided by edge computing are appropriately leveraged.

Edge computing limits the amount of data it delivers to the central server, which makes it possible to run critical infrastructures effectively because operators are not overloaded. The data transfer mechanism also lowers data transfer latency, enabling operators to get crucial data promptly and make data-driven choices. Critical infrastructure systems and equipment tend to be distributed and complicated, making maintenance and troubleshooting challenging. Operators may be able to remotely check on the condition of these components thanks to IIoT and edge computing devices. However, this creates security issues because threat actors may exploit the same tools for maintenance for malicious reasons.

Finally, the convergence of Information Technology (IT) and Operational Technology (OT) has increased in critical infrastructure sectors (Angel, 2021). Historically, IIoT environments in critical infrastructure sectors like utilities were disconnected from the internet (Murray, Johnstone and Valli, 2017). The increased efficiencies brought about by the growth of the internet necessitated the integration of traditional OT and IT environments. Because OT systems were never designed with security in mind, the convergence introduces security risks. Edge computing can help alleviate some security concerns by implementing security controls at the network's edge to ensure secure data storage and transmission.

6. Conclusion

The paper's objective was to address edge computing's incorporation into IIoT contexts, with a particular emphasis on the management of crucial infrastructures. In support of this, the paper pointed out that IIoT includes IoT's industrial applications. The paper also contrasted the application of edge and cloud computing in

IIoT contexts. Edge computing is more suited for IIoT contexts because it lowers the latency associated with data transfer to centralised servers.

The integration of edge computing into IIoT was then covered in this paper, with advances in safety, security, and the efficient use of storage and computing resources noted. Edge computing makes it possible to manage critical infrastructures consistently. There was a discussion of the widespread security issues in edge computing environments. Internal dangers brought on by uninformed or disgruntled personnel, attacks on authentication and authorisation mechanisms, data security, side-channel attacks, network attacks, legacy systems, and physical security were all discussed.

Finally, the paper briefly explored IoT Digital Forensics Readiness (DFR), a new research area focusing on securing edge computing environments against potential threats. DFR sets up procedures that enable a quick reaction to a security incident. This paper's objective was thus accomplished. Future work should investigate how edge computing has impacted the convergence of Information and Operational Technology in IIoT environments.

References

Angel, N.A., Ravindran, D., Vincent, P.D.R., Srinivasan, K. and Hu, Y.C. (2021) Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. *Sensors*, 22(1), p.196.

Antao, L., Pinto, R., Reis, J. and Gonçalves, G. (2018, April) Requirements for testing and validating the industrial internet of things. In *2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)* (pp. 110-115). IEEE.

Alwakeel, A.M. (2021) An overview of fog computing and edge computing security and privacy issues. *Sensors*, 21(24), p.8226.

Basir, R., Qaisar, S., Ali, M., Aldwairi, M., Ashraf, M.I., Mahmood, A. and Gidlund, M. (2019) Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors*, 19(21), p.4807.

Bhaiyat, H. and Sithungu, S. (2022, June) The Emergence of IIoT and its Cyber Security Issues in Critical Information Infrastructure. In *European Conference on Cyber Warfare and Security* (Vol. 21, No. 1, pp. 46-51).

Caiza, G., Saeteros, M., Oñate, W. and Garcia, M.V. (2020) Fog computing at industrial level, architecture, latency, energy, and security: A review. *Heliyon*, 6(4), p.e03706.

Cao, K., Liu, Y., Meng, G. and Sun, Q. (2020) An overview on edge computing research. *IEEE access*, 8, pp.85714-85728.

Chalapathi, G.S.S., Chamola, V., Vaish, A. and Buyya, R. (2021) Industrial internet of things (iiot) applications of edge and fog computing: A review and future directions. *Fog/edge computing for security, privacy, and applications*, pp.293-325.

Gaidarski, I. and Minchev, Z. (2021) Insider Threats to IT Security of Critical Infrastructures. In *Digital Transformation, Cyber Security and Resilience of Modern Societies* (pp. 381-394). Springer, Cham.

Goswami, V., Jadav, P. and Soni, S.K. (2022) Review on How IIoT Has Revolutionized Greenhouse, Manufacturing and Medical Industries. In *Recent Advances in Mechanical Infrastructure* (pp. 179-192). Springer, Singapore.

Husain, B.H. and Askar, S. (2021) Survey on Edge Computing Security. *International Journal of Science and Business*, 5(3), pp.52-60.

Industrial Internet Consortium. (2019) *The Industrial Internet of Things Volume G1: Reference Architecture*. Available at: https://www.iiconsortium.org/pdf/IIRA-v1.9.pdf [Accessed 19 November 2022]

Kebande, V.R., Karie, N.M. and Venter, H.S. (2018) Adding digital forensic readiness as a security component to the IoT domain.

Khan, W.Z., Rehman, M.H., Zangoti, H.M., Afzal, M.K., Armi, N. and Salah, K. (2020) Industrial internet of things: Recent advances, enabling technologies and open challenges. *Computers & Electrical Engineering*, 81, p.106522.

Koohang, A., Sargent, C.S., Nord, J.H. and Paliszkiewicz, J. (2022) Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, 62, p.102442.

Lanz, Z. (2022) Cybersecurity Risk in US Critical Infrastructure: An Analysis of Publicly Available US Government Alerts and Advisories. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(1), pp.43-70.

Mirani, A.A., Velasco-Hernandez, G., Awasthi, A. and Walsh, J. (2022) Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors*, 22(15), p.5836.

Murray, G., Johnstone, M.N. and Valli, C. (2017) The convergence of IT and OT in critical infrastructure.

Patil, K., Gupta, S., Nair, A. and Gutte, V. (2020) Cloud, Fog and Edge Computing: Security and Privacy Concerns.

Parikh, S., Dave, D., Patel, R. and Doshi, N. (2019) Security and privacy issues in cloud, fog and edge computing. *Procedia Computer Science*, 160, pp.734-739.

Pivoto, D.G., de Almeida, L.F., da Rosa Righi, R., Rodrigues, J.J., Lugli, A.B. and Alberti, A.M. (2021). Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. *Journal of Manufacturing Systems*, 58, pp.176-192.

Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D.O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. *IEEE Communications Surveys & Tutorials*, 22(4), pp.2462-2488.

Roman, R., Lopez, J. and Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78, pp.680-698.

Shalaginov, A., Iqbal, A. and Olegård, J. (2020), September. Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications. In *International Conference on Edge Computing* (pp. 1-17). Springer, Cham.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, E.K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. *IEEE Communications Surveys & Tutorials*, 22(2), pp.1191-1221.

Sittón-Candanedo, I., Alonso, R.S., Corchado, J.M., Rodríguez-González, S. and Casado-Vara, R. (2019). A review of edge computing reference architectures and a new global edge proposal. *Future Generation Computer Systems*, 99, pp.278-294.

Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J. and Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, 107(8), pp.1608-1631.

Zhao, Y., Yang, J., Bao, Y. and Song, H. (2021). Trustworthy authorization method for security in Industrial Internet of Things. *Ad Hoc Networks*, 121, p.102607.

Zhang, T., Li, Y. and Chen, C.P. (2021). Edge computing and its role in Industrial Internet: Methodologies, applications, and future directions. *Information Sciences*, 557, pp.34-65.