IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Fortifying Critical Infrastructures: Secure Data Management with Edge Computing

Sahil Arora[1] and Apoorva Tewari[2]
Independent researcher
Staff Product Manager, Twilio Inc[1]
Senior Product Manager, Intuit Inc[2]
sahil9009@gmail.com and apoorvatewari91@gmail.com

Abstract: *Critical infrastructures (CIs), including energy, healthcare, and transportation, are vital to societal functions, making their security paramount. The emergence of edge computing as a means of safe data management is a direct result of the growing dependence of these infrastructures on real-time data and networked devices. Computing at the edge, or near the source of data, improves efficiency, simplifies data processing, and enables better real-time judgements by decentralising data processing. However, this distributed architecture introduces new security challenges, such as managing a broader attack surface and ensuring data integrity. This paper reviews the role of edge computing in securing critical infrastructures and discusses advanced security measures like encryption, access control, AI-driven anomaly detection, and blockchain. It also outlines future research directions, emphasizing the need for scalable, interoperable edge systems, AI-enhanced security models, quantum-safe encryption, and privacy-preserving techniques. Global standardization is highlighted as essential for consistent, reliable integration. Ultimately, edge computing offers a promising pathway to fortify critical infrastructures against evolving cyber threats, ensuring their continued, resilient operation in an increasingly connected and digital world.*

Keywords: Critical infrastructures, Edge computing, secure data management, real-time decision-making, data integrity, AI-driven security, privacy-preserving techniques, cyber threats

I. INTRODUCTION

The so-called critical infrastructures (CIs), which include networks for energy distribution and transportation, are becoming more broad and advanced in the most industrialized nations [1]. An organization's critical infrastructure consists of its most important resources, services, networks, information technology systems, and assets. Its degradation or loss would have a significant impact on important societal functions like SCM, public health, safety, and the economic and social welfare of the nation and its citizens[2].

Elemental to the regular functioning of human civilisation are the components that make up critical infrastructure (CI) [3]. A "critical asset" is any resource—physical or otherwise—that is essential to the smooth running of society as a whole, including but not limited to people's physical and mental health, financial stability, and social and economic opportunities[4]. It is challenging for countries to achieve and maintain their national objectives of social and economic growth and advancement when their CI is not functioning correctly or is weak. One way to look at it is as a nation's economic "central nervous system" [5].

Analytics of IoT data may be performed at the system's peripheral using edge computing prior to data transmission to a data center or the cloud. Problems arise as the number of devices transmitting data over a system grows, even when a single device may communicate data over a system properly[6][7]. An further way that companies might save money is by reducing the amount of data that has to be managed centrally or in the cloud. An interconnected system of physical objects that can exchange data with one another and with cloud services is known as the IoT. The advent of edge computing is a direct result of this. Furthermore, while operation, many IoT devices generate a great deal of data [8][9].Data security refers to the steps taken to prevent data loss, misuse, or tampering[10]. To do this, one may use a wide variety of virtual (software-based) and physical (hardware-based) approaches. Data masking is one option for protecting data in a virtual environment.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

The purpose of data masking is to prevent unwanted or unauthorised access to data by changing or hiding the original data and replacing it with additional content. The term "access control" describes the practice of ensuring that only authorised entities have access to certain data. When entities inside a system are subject to different levels of access control depending on the functions they perform, this method is known as role-based access control. Transforming data from a readable format into an unreadable one is the essence of data encryption. Nowadays, most businesses utilise encryption to safeguard the data of both themselves and their customers [11]. The following paper contribution as:

- By leveraging edge computing, the system enables faster data processing at a network's edge, decreasing latency and allowing for real-time decision-making. Important infrastructures must have this in place to provide increased resilience and operating efficiency in the face of possible dangers or system malfunctions that need rapid reactions.
- Edge computing processes and analyses data locally, reducing a quantity of datasets to central cloud systems. This decentralized approach significantly enhances data security by reducing exposure to cyber threats during transmission and decreasing the potential for data breaches.
- Edge computing frees up storage and processing capacity on central cloud servers, enabling effective resource allocation for vital infrastructure systems. This contributes to cost-effective management of large-scale infrastructures, enhancing scalability without sacrificing performance.
- Critical infrastructures are often interconnected, making them vulnerable to cascading failures. The edge computing framework proposed in this work allows for localized data processing, isolating issues before they propagate across systems. This containment of faults helps prevent widespread disruptions.

The research demonstrates how edge computing designs, like Cloudlet, Multi-Access Edge Computing, and Fog Computing, may facilitate an integration of IoT devices into vital infrastructures. In addition to preserving safe and dependable operations, this promotes innovation by allowing cutting-edge applications like autonomous system control, AI-driven monitoring, and predictive maintenance.

A. Organization of the Paper

The paper is structured as follows: Section II covers the II. Overview of critical infrastructure vulnerabilities. Section III Details III.Role of edge computing in data integrity. Section IV Examines the IV. Secure data management with critical infrastructure. Section V presents a Literature review, identifies research gaps, and VI offers Recommendations for conclusions and future work.

II. OVERVIEW OF CRITICAL INFRASTRUCTURE VULNERABILITIES

Large-scale, man-made systems known as "critical infrastructures" rely on one another to generate and transmit necessities like electricity, water, and data as well as services like banking, healthcare, and transportation. If the loss of an infrastructure significantly affects the economy, social welfare, safety, or health of the public, it is considered essential infrastructure [12][13].Political decision-making is facilitated by infrastructure on many dimensions and in various settings, including goods and services, safety, health, and transportation [14]. Figure 1 shows that infrastructures are more than just closed supply chains or life-support systems. Contrarily, they are essential to the social fabric and our very survival as a group [15].

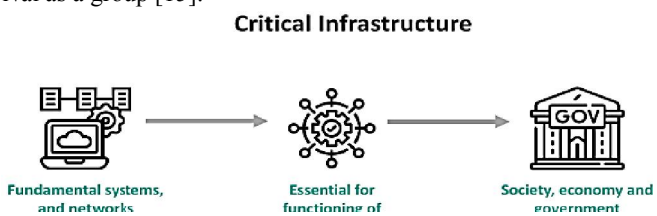

Figure 1: Critical Infrastructure

A. Vulnerability of Interdependent Critical Infrastructures

Infrastructures, as previously said, are large-scale systems that are integral to society's operation. All infrastructures, however, are systems that might be susceptible to attack. A number of disciplines use the term vulnerability" in their

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

work, including anthropology, economics, catastrophe studies, development studies, and climate change study [16]. Assessing a system's susceptibility to harm entails contrasting its current defences with its intended levels of protection and any future threats [17].

Assessing the risk and susceptibility of CIs is necessary for making design, operation, and management preparations to deal with them. With its formalisation over thirty years ago, risk analysis has found many uses in illuminating and detecting possible failure modes and dangers in our systems, allowing us to fix them before they ever happen[12].

The goals of vulnerability and risk analysis are:

- Consider a system and its intended goals (the positive side), then figure out what may go wrong (the negative side) in terms of the planned aims[18].
- Determine the relevant sequence of "initiating events" and assess the domino effect they have on a component or the whole system [18].
- Determine the sequence of events or sets of events that would lead to this consequence given a system and its intended goals. A huge number of event sequences are feasible in every given real-world scenario[18].
- Identify and describe (inter-)dependencies (both inside and across systems), as well as coupling of various orders, given the collection of starting events, event sequences, and observable outcomes [18].

B. Challenges of Critical Infrastructures

Critical infrastructure faces numerous challenges, especially in securing and managing essential systems and services. Key challenges include:

- **Cybersecurity Threats**: Critical infrastructure is a prime target for cyberattacks, including ransomware, nation-state threats, and advanced persistent threats (APTs), which can disrupt essential services like power grids, water supply, and transportation.
- **Aging Infrastructure**: Many critical infrastructures were not designed with modern digital threats in mind, leading to vulnerabilities in outdated systems and legacy technologies that are difficult to upgrade.
- **Interconnected Systems**: The increasing interdependence of infrastructure sectors (e.g., energy, transportation, and communications) amplifies the risk of cascading failures across systems if one sector is compromised.
- **Regulatory and Compliance Issues**: Balancing the need for security while maintaining regulatory compliance and operational efficiency can be complex, especially with evolving standards and international variations in policy.
- **Physical Security**: Protecting physical assets from sabotage, natural disasters, and physical attacks is critical, as disruptions can have far-reaching effects.
- **Data Management and Privacy**: Securing and managing the massive data volumes created by critical infrastructures without compromising data privacy has become more difficult due to the development of IoT devices and real-time monitoring systems.
- **Skills Gap**: There is often a shortage of skilled cybersecurity professionals capable of addressing the unique security needs of critical infrastructure systems.
- **Adoption of Emerging Technologies**: While technologies like AI, IoT, and edge computing can enhance operations, they introduce new vulnerabilities if not properly secured or integrated into the existing infrastructure[19].

III. ROLE OF EDGE COMPUTING IN DATA INTEGRITY

Edge computing has a leg up on fog and cloud computing because it allows data processing to happen at the edge and saves resources by just sending the most important data to the cloud for processing. Quick responses to real-time events are possible because to edge computing's reduction in data transfer latency[20]. Additionally, edge computing lessens the burden on cloud servers in terms of computation and storage, which in turn decreases the cost of maintaining the cloud infrastructure [21].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Edge computing allows for more efficient management of critical infrastructures by reducing the amount of data delivered to the central server. This prevents operators from being overwhelmed. Additionally, the data transmission method reduces data transfer latency, letting operators get critical data quickly and make data-driven decisions. Due to their dispersed nature and complexity, critical infrastructure systems and equipment are notoriously difficult to maintain and fix.

A. Architecture of Edge Computing

Several edge computing designs, including cloudlet, fog, and MAEC, will be discussed in this section.

Multi-Access Edge Computing (MAEC)

The ETSI defines MAEC, formerly known as MEC, as the application of cloud computing concepts to IT servers situated at the network's edge. To put it simply, MEC is a cloud server that can operate at the periphery of a mobile network and manage operations that go beyond what is normally possible with conventional network architecture. Figure 2 shows the network context, which may greatly decrease latency, and how local edge servers in a wireless network can use lower-level signaling information to determine the position of linked end devices [22].

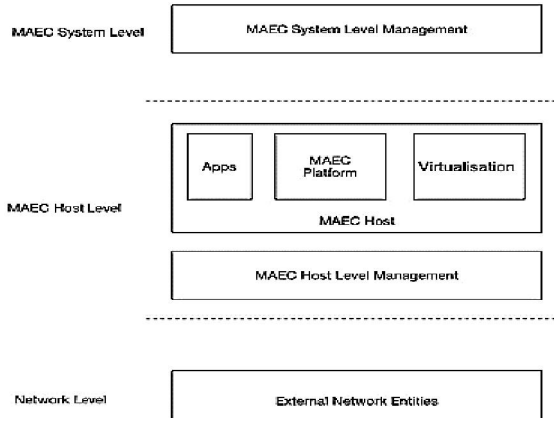

Figure 2: Multi-access edge computing framework.

Cloudlet Computing

A dependable computer or network of robust computers is what Cloudlet is all about[23]. These servers or groups of servers have good Internet connections and are accessible from mobile devices in the area. We can get answers in real time this way. Most of the time, cloudlets are situated within a hop's distance from mobile devices. Low latency and high bandwidth are typical characteristics of Cloudlet access. On top of that, the Cloudlet may run independently thanks to virtual machine technology[24]. The overall design of Cloudlet computing is seen in Figure 3.

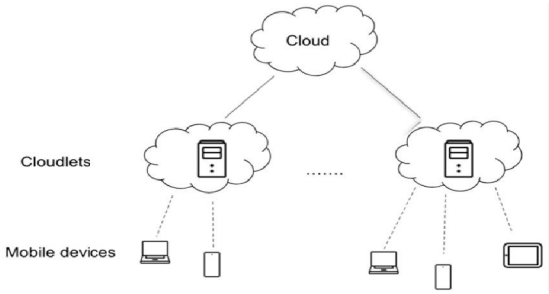

Figure 3: The overall hierarchical architecture of Cloudlet computing.

Fog Computing

The term "fog computing" refers to a "along a continuum from the cloud to the objects, this horizontal, system-level architecture brings computing, storage, control, and networking closer to the consumers." When compared to MAEC

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

and Cloudlet computing, two other edge computing designs, fog computing places a greater emphasis on the collaboration and communication amongst decentralised devices, including IoT devices. The proximity and efficiency of fog computing services to terminal devices are therefore enhanced. This main characteristic may aid in delivering effective and high-quality services [25].Data transmission, storage, and computing are handled by the many fog nodes, which include routers and switches, that make up the fog layer [26].Fog computing's overall hierarchical design is seen in Figure 4.

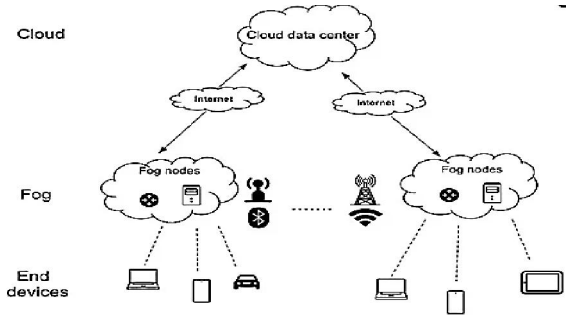

Figure 4: The overall hierarchical architecture of fog computing.

Capabilities of Edge Computing

Computing at a network's periphery, or "edge," makes employ of cloudcomputing. Cloud computing takes care of network administration, while edge computing ensures service continuity. Near the consumer, the edge device distributes data storage, management, and communication. Therefore, there are many ways in which the network benefits from using edge computing [27].

- **Efficiency:** In order to make the most of the resources that are accessible, an edge device may distribute storage, computation, and control operations to any location between the user and the cloud. This makes it possible for IoT devices to make good use of the shared computing resources at the edge[28].
- **Cognition:** A needs of a consumer are considered by an edge device [29]. IoT devices track patients' vitals in an e-health system, which is particularly useful in emergency circumstances, and users' health-risk grades inform how computing resources are allocated[30].
- **Agility:** Due to the increased proximity of data processing and storage with edge devices and clients, experimentation becomes more efficient and cost-effective.
- **Latency:** IoT apps can make better and quicker choices due to edge computing, which helps time-critical apps by allowing data processing and analysis close to the end-user [27].

IV. SECURE DATA MANAGEMENT WITH CRITICAL INFRASTRUCTURE

Data management refers to a set of procedures for arranging and storing data in a way that makes it readily accessible and useful. Data acquisition, validation, storage, protection, and processing are all part of these operations. If a company or organisation wants to increase productivity, save expenses, and lessen risk, it needs good data management techniques. Recent years have seen data-driven public and corporate organisations craft data policies and strategies that support their objectives. Various data-related abilities and knowledge are covered by these strategies: creation, storage, administration, retrieval, enhancement, publishing, security, analysis, sharing, usage, privacy, and archiving. Taking into account the interdependencies among these stages, the data life cycle spans all elements of data from planning and collecting to disposal and serves as the principal instrument for data management inside the government's big-data ecosystem.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

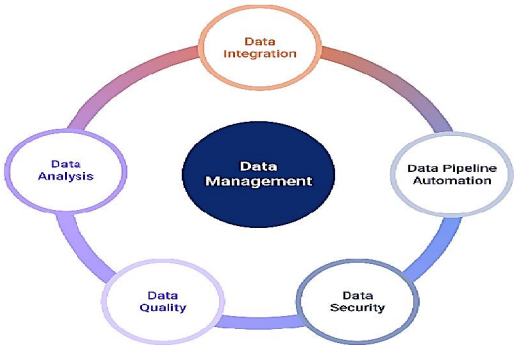

Figure 5. Data Management and Its Top Challenges

Displayed in Figure 5 The most pressing issues and threats facing data management are addressed here[31].

- **Data Integration:** Data that is incompatible with one another and with different formats from various sources causes processes to use a lot of resources.
- **Data Pipelines:** The value of data is greatly diminished because of late deliveries caused by a lack of automation, which results in outdated data.
- **Data Quality:** Losses in capital caused by erroneous conclusions drawn from data that is inconsistent, incomplete, or duplicated.
- **Data Security:** Data breaches and accidental employee access may lead to hefty penalties, harm to reputation, and a loss of confidence.
- **Data Analysis:** A decrease in consumer happiness, a loss of competitive advantage, and a bad return on investment as a result of inefficient or nonexistent data analysis.

A. Application State of Data Management

Distributed data management solutions mainly target applications that need hosting large amounts of data. This information is unique to the application and is called the application state. There is often a two to three order of magnitude difference between the system state and the application state. An applications have different needs for consistency, scalability, and availability[32].

Data Model and its Implications:

A three primary systems that are the focus of this research are distinguished by their straightforward data model. A key-value pair for each item in a table is the main abstraction. Dynamo uses uninterpreted strings for values, whereas PNUTS and Bigtable use structured values. There is no assurance that atomic read/write or atomic read-modify-write will work across objects; instead, atomicity is only supported at the item level. A primary key identifies a single entity, and it is often noted that many actions are entity-restricted.

Single Object Operations and Consistency:

Making sure scalability is manageable and that actions are restricted to a single key makes it possible to provide consistency for individual objects. In the absence of object-level replication, every request for an object will reach the same hosting node. In spite of data partitioning, queries can only reach a single node due to their single-key nature. Algorithms like atomic read, write, and read-modify-write are now available in the system.

Replication and Consistency:

Per-object replication is sometimes necessary for high availability in modern systems, and it may also sometimes improve speed by spreading the burden across the copies. Since changes to an item also need to be reflected in the clones, this makes providing consistency guarantees more complicated. On the basis of the processes used to synchronise the copies, various systems provide varying degrees of consistency, including eventual consistency and timeline consistency [33].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Availability:

In the past, distributed databases treated all of the data as a single, cohesive whole. As a result, the inability to access any particular portion of the data was taken to indicate that the whole system was unavailable. However, data correlation has decreased thanks to the single-object semantics of contemporary systems. Because of this, contemporary systems can accept that some data may not be available while still offering the remaining data a respectable level of service [32].

V. LITERATURE REVIEW

In this section, provide some previous work on Edge computing and secure data management with critical infrastructure. Some authors have tried to in cloud computing by using both.

Begam and Mohamed (2012), suggests using surrogate objects as a means of safe data management in a mobile grid setting. Additionally, topics covered include authentication and encrypted communication. The authentication protocol addresses security concerns in a mobile grid context by being developed on top of surrogate objects. A communication service is the foundation of an authentication protocol, which in turn provides cryptographically secure methods for authenticating people and resources. A surrogate object model uses the mobile host's cache to decreasean amount of datasent wirelessly. The model handles the mobility of mobile hosts by solving the location management issue using a collection of surrogate objects as a place holding frame [34].

Fan et al. (2018), this paper offers an approach to secure data sharing between domains utilizing the edge computing model; in this model, each domain consists of an edge computing node and controlled edge equipment; the cloud connects all of these domains; and the challenge of authentication across domains is easily solved.At the same time, one-to-many data exchange and information secrecy are guaranteed by using the RSA algorithm and CP-ABE. Analysis confirms the security of our system[35].

Dolui and Datta (2017), the beginning of a new era called "Edge Computing," the aim of which is to move context-aware distributed computation and storage to the network's perimeter. In particular, this article examines and contrasts Mobile Edge Computing, Fog Computing, and Cloudlet, three separate implementations of Edge Computing. They lay out a set of criteria for selecting the optimal implementation and include a DT to aid in making that selection. When it comes to managing massive amounts of data, cloud computing has become the standard during the last decade [36].

Jin et al.(2020), implement a secure paradigm for edge computing that can handle people, data, devices, and more via the usage of decentralized microservices providers on an edge gateway equipped with a security gateway. An edge gateway, a nerve center of a neighborhood network, has a plethora of IoT sensors that can detect and respond to physical objects and environments. In a recent shift in computing, dubbed "edge computing," data is moved to the very edges of networks, closer to where sensors and actuators are located[37].

Liu et al (2019), evaluate potential threats to the security of edge computing and then lay forth standards for the secure analytics of its data. Based on our objectives, we also provide a detailed analysis of the current literature on data analytics in edge computing, including both its strengths and weaknesses. Our review of the literature allows us to identify unanswered questions and potential avenues for further study. Data processing and storage in the network's perimeter are ideal for edge computing due to their location awareness and efficiency in comparison to cloud computing[38].

Mor et al., (2019), suggest a data management architecture based on federated edge computing. In our ideal world, users would be able to engage into commercial agreements with infrastructure maintainers to store and communicate data, without having to trust the provider, all because of the "data-services" paradigm that we envision. In pursuit of this goal, we introduce Data Capsules, which are coherent sets of cryptographically protected data objects, and the Global Data Plane, a description of the federated architecture that supports them[39].

This Table 1 provides a summary of the key aspects of each research contribution, helping to highlight similarities and differences across studies for Critical Infrastructures: Secure Data Management with Edge Computing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Table 1: Comparative related work summary for Critical Infrastructures: Secure Data Management with Edge Computing

Reference	Research Area	Key Findings	Metrics	Demerits	Future Work
[34]	Secured Data Management in Mobile Grid Environments	Proposed surrogate object model to manage mobility and authentication, reducing wireless data transfer.	Data transfer efficiency, authentication	Limited to mobile grid; not scalable across platforms.	Enhance scalability and generalization to other environments.
[35]	Secure Data Sharing in Edge Computing	Used RSA and CP-ABE encryption to ensure confidentiality and one-to-many data sharing across domains.	Data confidentiality, RSA, CP-ABE	Computational overhead due to encryption complexity.	Improve computational efficiency and scalability across domains.
[36]	Edge Computing Paradigm Comparison	Detailed comparison of Fog Computing, Cloudlet, and Mobile Edge Computing, proposing a decision tree for optimal selection.	Context awareness, storage and computation	Decision tree lacks dynamic adaptability for all use-cases.	Integrate dynamic adaptability based on real-time needs.
[37]	Secure Edge Computing with Microservices	Proposed independent microservices for secure management of devices and data via edge gateway.	Data management, IoT device security	Security concerns with decentralized microservices.	Enhance security layers and fault tolerance for edge gateways.
[38]	Secure Data Analytics in Edge Computing	Provided requirements for secure data analytics, highlighting threats and offering a review of existing works.	Data privacy, computational efficiency	Limited handling of evolving threats in edge environments.	Develop adaptive threat-handling mechanisms for edge analytics.
[39]	Federated Edge-Computing Architecture	Proposed cryptographically hardened Data Capsules and a federated Global Data Plane for secure data management.	Data security, federated architecture	Trust issues with third-party infrastructure providers.	Explore trustless models for federated architectures.

VI. CONCLUSION AND FUTURE SCOPE

The safety of our nation's critical infrastructures (CI) is of the utmost importance since they provide vital social services including electricity, healthcare, and transportation. A potential solution for safe data management has arisen: edge computing. This is because these infrastructures are becoming increasingly networked and dependent on real-time data. Edge computing, which decentralizes data processing and moves computation closer to the source, enhances real-time decision-making, reduces bandwidth consumption, and reduces latency. However, this distributed architecture introduces new security challenges, such as managing a wider attack surface and ensuring data integrity. Addressing these challenges requires robust security measures like encryption, access control, AI-driven anomaly detection, and blockchain-based solutions. Looking forward, research should focus on scaling edge systems across various

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

infrastructure sectors while ensuring interoperability and developing advanced AI-driven security models for automated threat response.

Additionally, the exploration of quantum-safe encryption and privacy-preserving computation techniques will be critical in securing future edge systems. Finally, global standardization efforts are needed to create consistent, reliable frameworks for integrating edge computing into critical infrastructures. Edge computing may greatly assist CIs in protecting themselves from new cyber risks and maintaining reliable operations in an increasingly digital environment by focussing on these areas.

REFERENCES

[1] C. Berger, P. Eichhammer, H. P. Reiser, J. Domaschka, F. J. Hauck, and G. Habiger, "A Survey on Resilience in the IoT: Taxonomy, Classification, and Discussion of Resilience Mechanisms," *ACM Comput. Surv.*, 2022, doi: 10.1145/3462513.

[2] F. De Felice, I. Baffo, and A. Petrillo, "Critical Infrastructures Overview: Past, Present and Future," *Sustainability (Switzerland)*. 2022. doi: 10.3390/su14042233.

[3] G. Pescaroli and D. Alexander, "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters," *Nat. Hazards*, 2016, doi: 10.1007/s11069-016-2186-3.

[4] E. Luiijf and M. Klaver, "Resilience Approach to Critical Information Infrastructures: Theories, Methods, Tools and Technologies," 2019, pp. 3–16. doi: 10.1007/978-3-030-00024-0_1.

[5] J. M. Yusta, G. J. Correa, and R. Lacal-Arántegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," *Energy Policy*, 2011, doi: 10.1016/j.enpol.2011.07.010.

[6] Madhuri, "A review on Edge computing for Internet of Things," *International Journal of Research and Analytical Reviews*. 2018.

[7] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[8] S. K. R. Anumandla, V. K. Yarlagadda, S. C. R. Vennapusa, and K. R. V Kothapalli, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Technol. \& Manag. Rev.*, vol. 5, no. 1, pp. 45–65, 2020.

[9] O. B. Ohwo, E. Publication, T. Ayanwola, and A. Oludele, "Edge Computing : A Literature Review Research Journal of Mathematics and Computer Science Edge Computing : A Literature Review," no. June, 2022.

[10] V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, Dec. 2018, doi: 10.18034/ei.v6i2.709.

[11] D. R. Ingle, M. Kulkarni, P. Shinde, and M. Tambe, "Literature review of data security measures and access control mechanisms of information security head of department," *Int. J. Creat. Res. THOUGHTS*, 2022.

[12] E. Zio, "Critical Infrastructures Vulnerability and Risk Analysis," *Eur. J. Secur. Res.*, 2016, doi: 10.1007/s41125-016-0004-2.

[13] V. V. Kumar, A. Sahoo, and F. W. Liou, "Cyber-enabled product lifecycle management: A multi-agent framework," in *Procedia Manufacturing*, 2019. doi: 10.1016/j.promfg.2020.01.247.

[14] S. j. Collier and A. Lakoff, "Vital Systems Security: Reflexive Biopolitics and the Government of Emergency," *Theory, Cult. Soc.*, 2015, doi: 10.1177/0263276413510050.

[15] N. Anand, A. Gupta, and H. Appel, "Temporality, Politics, and the Promise of Infrastructure," *Promise Infrastruct.*, 2018.

[16] W. Bijker, A. Hommels, and J. Mesman, "Studying Vulnerability in Technological Cultures," in *Vulnerability in Technological Cultures*, 2019. doi: 10.7551/mitpress/9209.003.0002.

[17] C. Pursiainen, "Critical infrastructure resilience: A Nordic model in the making?," *Int. J. Disaster Risk Reduct.*, 2018, doi: 10.1016/j.ijdrr.2017.08.006.

[18] J. Johansson and H. Hassel, "An approach for modelling interdependent infrastructures in the context of vulnerability analysis," *Reliab. Eng. Syst. Saf.*, 2010, doi: 10.1016/j.ress.2010.06.010.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

[19] C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," *Int. J. Crit. Infrastruct. Prot.*, 2015, doi: 10.1016/j.ijcip.2014.12.002.
[20] A. A. Mirani, G. Velasco-Hernandez, A. Awasthi, and J. Walsh, "Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review," *Sensors*. 2022. doi: 10.3390/s22155836.
[21] R. Basir *et al.*, "Fog computing enabling industrial internet of things: State-of-the-art and research challenges," *Sensors (Switzerland)*. 2019. doi: 10.3390/s19214807.
[22] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*. 2021. doi: 10.1109/ACCESS.2021.3053233.
[23] M. Satyanarayanan, P. Bahl, R. Cáceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, 2009, doi: 10.1109/MPRV.2009.82.
[24] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, "Fog Computing: Principles, architectures, and applications," in *Internet of Things: Principles and Paradigms*, 2016. doi: 10.1016/B978-0-12-805395-9.00004-6.
[25] R. Mahmud, R. Kotagiri, and R. Buyya, "Fog Computing: A taxonomy, survey and future directions," in *Internet of Things*, 2018. doi: 10.1007/978-981-10-5861-5_5.
[26] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*. 2017. doi: 10.1016/j.jnca.2017.09.002.
[27] S. Hamdan, M. Ayyash, and S. Almajali, "Edge-computing architectures for internet of things applications: A survey," *Sensors (Switzerland)*. 2020. doi: 10.3390/s20226441.
[28] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet Things J.*, 2016, doi: 10.1109/JIOT.2016.2579198.
[29] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," *IEEE Communications Surveys and Tutorials*. 2017. doi: 10.1109/COMST.2017.2745201.
[30] S. Vyas and D. Bhargava, "Challenges, Opportunities and Future Trends in Smart Health," in *Smart Health Systems*, 2021. doi: 10.1007/978-981-16-4201-2_10.
[31] A. Lefebvre, B. Bakhtiari, and M. Spruit, "Exploring research data management planning challenges in practice," *IT - Inf. Technol.*, 2020, doi: 10.1515/itit-2019-0029.
[32] D. Agrawal, A. El Abbadi, S. Antony, and S. Das, "Data management challenges in cloud computing infrastructures," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010. doi: 10.1007/978-3-642-12038-1_1.
[33] G. E. Eksi, B. Tekinerdogan, and C. Catal, "Software security management in critical infrastructures: a systematic literature review," *Turkish Journal of Electrical Engineering and Computer Sciences*. 2022. doi: 10.55730/1300-0632.3841.
[34] H. P. Begam and M. Mohamed, "Secured data management paradigm for mobile grid environment using surrogate objects," in *Proceedings - 2012 IEEE 13th International Conference on Mobile Data Management, MDM 2012*, 2012. doi: 10.1109/MDM.2012.77.
[35] K. Fan, Q. Pan, J. Wang, T. Liu, H. Li, and Y. Yang, "Cross-domain based data sharing scheme in cooperative edge computing," in *Proceedings - 2018 IEEE International Conference on Edge Computing, EDGE 2018 - Part of the 2018 IEEE World Congress on Services*, 2018. doi: 10.1109/EDGE.2018.00019.
[36] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *GIoTS 2017 - Global Internet of Things Summit, Proceedings*, 2017. doi: 10.1109/GIOTS.2017.8016213.
[37] W. Jin, R. Xu, T. You, Y. G. Hong, and D. Kim, "Secure edge computing management based on independent microservices providers for gateway-centric IoT networks," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3030297.
[38] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, 2019, doi: 10.1109/JIOT.2019.2897619.
[39] N. Mor, R. Pratt, E. Allman, K. Lutz, and J. Kubiatowicz, "Global data plane: A federated vision for secure data in edge computing," in *Proceedings - International Conference on Distributed Computing Systems*, 2019. doi: 10.1109/ICDCS.2019.00164.