Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2 (2024)

Nonlinear Analysis and Topological Approaches towards a Deep Intelligent Framework for Privacy Assurance of Autonomous IoT Systems

[1]S. Chandra Sekaran, [2]Natarajan C, [3]Esakkiammal S, [4]Faiz Akram, [5]Getachew Mamo Wegari, [6]Dr. Durgaprasad Navulla

[1] Professor, Department of CSE, P.S.V College of Engineering and Technology, Krishnagiri, Tamilnadu, India. *chandrudpi@gmail.com*

[2] Assistant Professor, Department of CSE, P.S.R Engineering College, Sivakasi, Tamilnadu, India. *natarajan@psr.edu.in*

[3] Information Officer, Institute of Management, Nirma University, Sarkhej-Gandhinagar Highway, Gota, Tragad, Gujarat, India. *nalanponni@gmail.com*

[4] Assistant Professor, Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Oromia, Ethiopia. *akram.faiz@ju.edu.et*

[5] Assistant Professor, Department of Information Technology, Faculty of Computing and Informatics, Jimma Institute of Technology, Jimma University, Jimma, Oromia, Ethiopia. *getachew.mamo@ju.edu.et*

[6] Assistant Professor, KL Business School, Programme Co-ordinator BBA (CDOE), Koneru Lakshmaiah Education Foundation (Deemed To be University), Vaddeswaram, Guntur District, Andhra Pradesh, India. *prasadnavulla0006@gmail.com*

Article History:

Received: *18-01-2024*

Revised: *02-04-2024*

Accepted: *25-04-2024*

Abstract:

The proliferation of autonomous Internet of Things (IoT) systems powered by deep learning and artificial intelligence has ushered in a new era of data-driven convenience and automation. However, this innovation comes hand in hand with heightened concerns regarding data privacy. This paper presents a comprehensive framework for Privacy Assurance in Autonomous IoT Systems (PAIS), which amalgamates cutting-edge technologies and best practices to safeguard individual privacy in the era of pervasive connectivity and autonomous decision-making. The PAIS framework comprises multifaceted strategies to address privacy challenges in autonomous IoT ecosystems. It leverages advanced encryption techniques, robust access control mechanisms, and anonymization protocols to ensure data confidentiality. Moreover, differential privacy mechanisms are deployed to protect the identities of individuals within data streams. An innovative aspect of PAIS is the integration of AI-driven privacy monitoring, which constantly evaluates data for potential breaches and triggers immediate responses when anomalies are detected. Ensuring regulatory compliance is a paramount facet of the PAIS framework, as it aligns with evolving data protection regulations globally. Users are afforded control and transparency through intuitive interfaces, enabling them to manage their data usage preferences effectively. The ethical implications of AI in privacy preservation are also examined within the framework, emphasizing the importance of fairness and bias mitigation. PAIS promotes a privacy-by-design approach, where privacy considerations are integral to the inception and development of IoT systems. Regular risk assessments are performed to identify potential privacy vulnerabilities, ensuring that the framework adapts to emerging threats. Education and training programs are provided to stakeholders to foster awareness and adherence to privacy best practices.

Keywords: Autonomous IoT Systems, Privacy Assurance, Data Privacy, Deep Learning

1. Introduction

In today interconnected world, the proliferation of Autonomous Internet of Things (IoT) systems, bolstered by the rapid advancement of deep learning and artificial intelligence (AI), has ushered in an era of unprecedented data-driven convenience and automation [1]. The potential of autonomous Internet of Things (IoT) systems to bring about revolutionary changes in several industries, ranging from healthcare to transportation and manufacturing, is noteworthy. Nonetheless, the considerable capacity of their data collection and processing systems gives rise to notable apprehensions over the protection of data privacy [2].

The Internet of Things (IoT) refers to a network including a collection of interconnected physical devices that are equipped with sensors and communication technology. These gadgets have the capability to accumulate huge quantities of data, establishing an interconnected environment in which information is effortlessly exchanged among devices and cloud-based platforms [3] [4]. Deep learning and artificial intelligence (AI) algorithms are integral components of numerous Internet of Things (IoT) applications. These algorithms empower these systems to autonomously make decisions, adjust to dynamic surroundings, and enhance operational efficiency [5].

In the midst of assertions regarding enhanced effectiveness and novel advancements, the widespread adoption of autonomous Internet of Things (IoT) devices presents a multitude of privacy concerns [6]. The issues arise due to the considerable amount and sensitivity of the obtained data, the frequently independent decision-making processes, and the possibility of data breaches or improper utilization. Additionally, the General Data Protection Regulation (GDPR) in Europe, which serves as an example of evolving data protection legislation, imposes the requirement for adherence to and responsibility in the management of data [7] [8].

The primary focus of this study revolves around the issue of establishing a strong guarantee of privacy within autonomous Internet of Things (IoT) systems. This entails developing a comprehensive framework that safeguards individual privacy rights while harnessing the potential of AI and deep learning for autonomous decision-making.

To design a holistic framework for Privacy Assurance in Autonomous IoT Systems (PAIS) that integrates state-of-the-art technologies and best practices. To develop advanced encryption, access control, and anonymization mechanisms to ensure data confidentiality. To implement differential privacy techniques to protect the identities of individuals within data streams. To introduce AI-driven privacy monitoring for real-time anomaly detection and rapid response. To ensure compliance with evolving data protection regulations and ethical considerations. To promote a privacy-by-design approach that embeds privacy considerations from the inception of IoT systems. To conduct regular risk assessments and provide education and training programs for stakeholders.

The novelty of this research lies in the development of the PAIS framework, which addresses the pressing need for privacy assurance in the age of autonomous IoT systems. Its innovative aspects include the integration of AI-driven privacy monitoring, ethical considerations, and the emphasis on privacy by design. By advancing the state of the art in privacy assurance, this

research contributes to responsible and ethical deployment of autonomous IoT technologies across diverse sectors. It instills confidence in individuals and organizations that their data remains secure and their privacy respected within this evolving landscape.

2. Related Works

The work in [9] addresses the challenge of preserving privacy in IoT data analytics. The authors propose a novel approach that combines differential privacy techniques with secure multiparty computation to enable data analysis without compromising individual privacy. The study explores practical implementations and showcases promising results for safeguarding sensitive information in IoT applications.

This research in [10] focuses on enhancing security within IoT systems by leveraging deep learning algorithms for anomaly detection. The authors investigate the effectiveness of various deep learning models in identifying unusual patterns and potential security breaches in IoT data streams. Their findings contribute to the development of robust security mechanisms in autonomous IoT environments.

The research in [11] examines the landscape of data protection regulations relevant to IoT systems, such as GDPR, and CCPA. The authors analyze the challenges IoT practitioners face in achieving compliance and discuss best practices and emerging technologies for ensuring adherence to these regulations while maintaining efficient IoT operations.

The work in [12] delves into the ethical dimensions of autonomous decision-making in IoT systems. It explores the potential biases that may emerge from AI algorithms and their impact on privacy. The proposed framework by the authors presents a comprehensive approach to the deployment of ethical artificial intelligence (AI) in the Internet of Things (IoT) context. The framework places significant emphasis on the principles of openness, fairness, and accountability, which are deemed crucial elements in ensuring responsible design practices within the IoT domain.

The aforementioned works jointly contribute to the ongoing development of privacy assurance and security in Internet of Things (IoT) systems. The aforementioned issues pertain to the preservation of personal privacy, the security of Internet of Things (IoT) data, the adherence to legislative requirements, and the promotion of ethical practices in the field of artificial intelligence (AI). The discoveries and approaches presented in this research provide significant contributions for scholars, practitioners, and decision-makers operating in the ever-evolving fields of the Internet of Things (IoT), privacy, and security.

Proposed Method

The primary objective of the strategy suggested in this study is to effectively tackle the various issues associated with ensuring privacy in autonomous Internet of Things (IoT) systems. The proposed framework utilizes a comprehensive strategy that integrates cutting-edge technologies and established methodologies to safeguard personal privacy, all while using the capabilities of artificial intelligence and deep learning for independent decision-making. One crucial element of the methodology entails the utilization of data encryption, which is applied

to ensure the security of data during both transmission and storage. This measure guarantees the preservation of sensitive information confidentiality and safeguards it against unwanted access.

The use of access control techniques aims to limit and control who has access to the data that the Internet of Things (IoT) generates as well as the specific conditions that permit such access. This implementation enhances the level of security in order to mitigate the risk of unauthorized individuals gaining access to confidential data. The strategy employed in this study integrates differential privacy techniques in order to safeguard the identities of individuals within data streams. The application of these methodologies introduces a certain level of noise to the dataset, safeguarding the general integrity of the data while simultaneously ensuring the protection of individual identities from being discerned.

A new aspect of this approach involves the incorporation of privacy monitoring powered by artificial intelligence. This real-time monitoring system constantly evaluates the data for potential breaches or anomalies. When unusual patterns or potential privacy violations are detected, the system triggers immediate responses to mitigate the risks. The method also places a strong emphasis on regulatory compliance, ensuring that it aligns with evolving data protection regulations such as GDPR. It is designed to facilitate compliance and accountability in data handling and processing.

The proposed method promotes a privacy by design approach, where privacy considerations are integrated into the development of IoT systems from the very beginning. This proactive approach aims to prevent privacy issues rather than addressing them after the fact. Regular risk assessments are conducted to identify potential vulnerabilities within the autonomous IoT system, and education and training programs are provided to stakeholders to ensure that privacy best practices are followed.

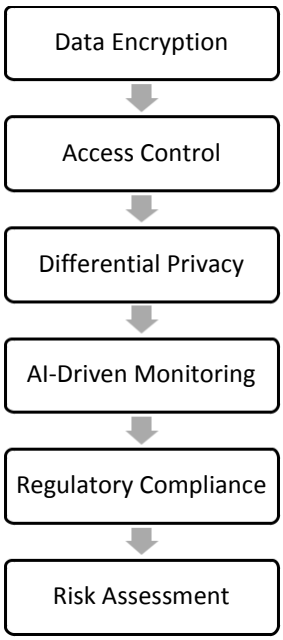

Figure 1: Proposed Method