

4th INTERNATIONAL CONFERENCE ON
AI ML, DATA SCIENCE AND
ROBOTICS

NOVEMBER 28-29 | PORTO, PORTUGAL



Chukwuemeka Nwachukwu

University of Bradford, UK

AI-DRIVEN ANOMALY DETECTION IN CLOUD COMPUTING ENVIRONMENTS

Abstract: The rapid adoption of cloud computing has changed the way businesses manage and store data, but it has also introduced new security challenges. One of the most pressing concerns in cloud environments is the detection of anomalies, which can signal potential security breaches, system failures, or performance issues. Traditional anomaly detection methods often fall short due to the complexity, scalability, and dynamic nature of cloud infrastructures. In recent years, Artificial Intelligence (AI)-driven anomaly detection techniques, particularly those leveraging machine learning and deep learning, have shown promise in overcoming these limitations. This paper reviews AI-driven approaches to anomaly detection in cloud computing environments, exploring their applications in enhancing cloud security, optimizing performance, and ensuring efficient resource management. The paper examines the strengths of various AI techniques, including supervised and unsupervised learning, deep learning, and hybrid models, highlighting their capacity to detect complex, previously unknown anomalies. Despite their advantages, implementing AI-based systems in cloud environments presents challenges, including data quality issues, scalability concerns, and computational resource requirements. Solutions such as federated learning and model optimization techniques are explored as methods to address these challenges. Furthermore, the paper discusses future research directions, including the integration of AI-driven anomaly detection with emerging technologies like blockchain and IoT, and the potential for advancements in self-supervised learning and explainable AI (XAI). This review concludes by emphasizing the critical role of AI in securing cloud infrastructures and the promising future of anomaly detection in the cloud computing landscape.

Keywords: Cloud Computing, Anomaly Detection, Artificial Intelligence, Machine Learning, Deep Learning, Security

Biography: Chukwuemeka Nwachukwu is a Digital Project manager and Business Consultant. He has held diverse leadership roles in several organizations and he sits on the Advisory Board of three African startups. He holds a MSc in applied artificial intelligence and Data Analytics from the University of Bradford, United Kingdom. Researches on the intersection of AI and health care where he works to improve patient experience as a digital project manager with the NHS. He is the CTO at Mcheritage Consulting (www.mcheritageconsulting.com) - a Consulting firm committed to building lives and businesses, where he specializes in using evidence-based research, innovative ideas and tested strategies to solve complex business problems and improve financial education.

4th INTERNATIONAL CONFERENCE ON
AI ML, DATA SCIENCE AND
ROBOTICS

NOVEMBER 28-29 | PORTO, PORTUGAL



Chukwuebuka Akwiwu-Uzoma

University of Dundee, Dundee, United Kingdom

AI-Enhanced Consumer Insights: Leveraging Behavioural Analytics for Hyper-Personalised Marketing Strategies

Abstract: The Internet of Things (IoT) has rapidly transformed home automation systems, offering convenience, efficiency, and enhanced control over household devices. From smart thermostats and lighting systems to security cameras and refrigerators, IoT technology enables users to monitor and control various aspects of their homes remotely. However, the widespread adoption of IoT in home automation systems brings with it a complex array of social implications. This paper examines the social impact of IoT technology in residential settings, focusing on privacy, security, and the potential for social inequalities. It explores how IoT-enabled devices collect vast amounts of personal data and the risks this poses to individual privacy, including the potential for unauthorized access, data breaches, and surveillance. Furthermore, the study analyses the security vulnerabilities inherent in these systems and the potential for cyberattacks, which could compromise users' safety and autonomy. The paper also delves into the social divide created by the unequal access to IoT technologies, examining how socio-economic factors may limit certain demographic groups from benefiting from smart home innovations. Additionally, the impact of IoT on social relationships, particularly the role of automation in reducing human interaction and fostering dependency on technology, is discussed. Through this analysis, the paper provides a comprehensive understanding of the broader societal challenges posed by IoT in home automation systems, offering insights into ethical, policy, and regulatory considerations that need to be addressed for a more equitable and secure IoT-enabled future.

Keywords: IoT, Home Automation, Privacy, Security, Social Inequality, Technology Dependency

Biography: Chukwuebuka Akwiwu-Uzoma is a data leader with expertise in AI, data engineering, cloud computing, and security, backed by an MSc in Data Science and Engineering from the University of Dundee. Currently spearheading Power Analysis Data Platform development in the Semiconductor industry, where he optimizes energy efficiency for mobile, automotive, and server computing systems.

A researcher and thought leader in sustainable computing, Chukwuebuka transforms complex data infrastructures into actionable business insights. He is a sought-after speaker and mentor, partnering with organizations like the Global Mentorship Initiative to develop the next generation of data leaders.