Journal of Informatics and Web Engineering
Vol. 3 No. 3 (October 2024) eISSN: 2821-370X

Editorial: Artificial Intelligence and Cybersecurity in Pervasive Computing

Ji-Jian Chin[1*]
[1]School of Computing, Engineering and Mathematics, University of Plymouth, Drake Circus, Plymouth PL4 8AA, United Kingdom
**corresponding author: (ji-jian.chin@plymouth.ac.uk; ORCiD:0000-0001-9809-6976)*

Abstract – Pervasive computing, or ubiquitous computing, is rapidly increasing in capacity and capabilities. With the Internet of Things (IoT) becoming an integral part of daily life and the growing availability of edge computing resources, automation guided by data is advancing applications in healthcare, manufacturing, automotive, and other areas. It's natural that pervasive computing will intersect with artificial intelligence (AI) and cybersecurity. AI can improve detection, prediction, and anticipative responses to human needs, while cybersecurity addresses topics like misuse prevention, ethics, policies, and governance. This issue features seven articles on these intersections, including four AI articles exploring natural language processing and computer vision, and three cybersecurity articles covering cryptography, medical devices, and maritime security.

Keywords—Pervasive, Ubiquitous, Cybersecurity, Artificial Intelligence, Machine Learning, Maritime Security

Received: 10 September 2023; Accepted: 01 October 2024; Published: 16 October 2024

1. INTRODUCTION

In recent years, the number of devices with computational capabilities has rapidly increased due to advancements in the Internet of Things. As the number of computing devices grows in both quantity and power, pervasive computing is becoming more integrated into daily life. From smart homes that manage and predict our needs to wearable devices that monitor our health, the boundaries between the digital and physical worlds are blurring. Advances in artificial intelligence, robust networks, and sensors are transforming computing from a tool into an omnipresent, invisible force that significantly influences how we perceive and interact with the world.

While pervasive computing brings unprecedented convenience and efficiency, it also raises critical questions about privacy, security, and the nature of human agency in an increasingly digitized world. This issue explores some of these questions, particularly within the dynamic fields of artificial intelligence and security.

1.1 What Is Pervasive Computing?

Ubiquitous computing, also known as pervasive computing is the idea that computing capabilities are built into everyday objects and devices everywhere [2]. It involves the deployment of numerous small, interconnected devices, such as sensors, actuators, and microprocessors, that work together to collect, process, and transmit data. This technology aims to create a more connected and intelligent world where technology is unobtrusive and responsive to our needs.

Key characteristics of pervasive computing include:

- Uniquity: Devices are everywhere, often embedded in objects and environments.
- Invisibility: Technology becomes a natural part of our surroundings.
- Proactivity: Devices detect, anticipate, and respond to our needs without human involvement.
- Context awareness: Devices understand their application context using location, time, user preferences, and other data.
- Interconnectivity: Devices communicate and collaborate seamlessly to provide comprehensive services.

Applications of pervasive computing revolve around smart homes, wearable devices, IoT, and smart cities. In smart homes, these computing devices power automated lighting, heating, home security systems, and appliance operations. Wearable devices include fitness trackers, smartwatches, and vision augments that aid in perception. IoT sensors collect data and automate actions in fields such as agriculture, healthcare, and manufacturing. These technologies form the core services of smart cities, improving efficiency, sustainability, and quality of life (see Figure 1).

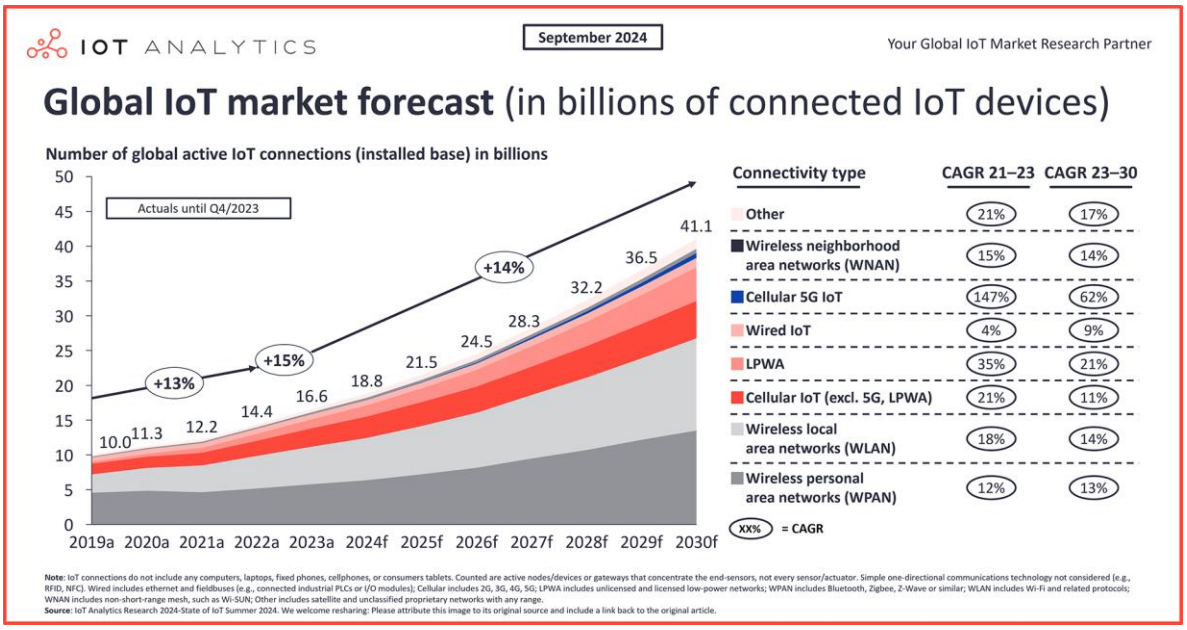

Figure 1. Global IoT Market Forecast (in billions of connected IoT devices) [1]

1.2 Recent Developments In Pervasive Computing

The main areas of pervasive computing usually revolve around hardware and devices, software, network and connectivity, applications and services, human-computer interaction and ethical/social implications. As this preface is written, several exciting advances in tech have just been recently announced: (1) the launch of ChatGPT 4o with capacity for deep reasoning [3], (2) Meta's Orion glasses that provide a new state-of-the-art augmented reality experience [4], and (3) Llama 3.2, the open source large language model was released for fine-tuning and deployment, featuring multimodal models that can reason on high resolution images [5]. Naturally, research in pervasive computing with intersect with the main areas of cybersecurity and AI, which remain the focus of this special editorial.

Outside of AI and cybersecurity, one main area of work receiving attention in pervasive computing is edge computing, with a lot of research focusing on reducing energy of computing devices while bringing computing power closer to where the data is produced by IoT devices. Several examples of research in edge computing include Sharghivand et al.'s work in proposing an edge computing matching framework with guaranteed quality of service, where the authors propose a novel two-sided matching solution for edge services that consider quality of service requirements in terms of service response time to circumvent strict quality of service restrictions imposed for remote execution of applications at the edge [6]. Another more recent work in edge computing by Tocze

and Nadim-Tehrani is an article which advocates for further studies beyond energy efficiency to examine the resource impact of edge computing itself [7].

For recent works touching on AI in pervasive computing, Kumar et al.'s work in developing trustworthy AI in the age of pervasive computing and big data formalizes the requirements of trustworthy AI systems through an ethics perspective [8]. Gou et al. takes a deeper look at a cognitive medical decision support system in an pervasive computing environment, presenting a uniquely flexible medical decision support system to enhance end-user confidence through ubiquitous IoT devices within the context of HCI [9]. Lastly, Bimpas et al. provides a survey on advancements, applications and open challenges in 2024 that focuses on different tools, techniques and applications developed to leverage the benefits of pervasive computing for ambient intelligence [10]. Works such as these offer much insight into applications of AI from both technical and ethical perspectives within the context of pervasive computing.

In the recent works in the area of cybersecurity, on the other hand, Ahuja et al.'s article looks at privacy and security considerations in healthcare when it comes to navigating IoT and pervasive computing challenges, with the intention of informing healthcare professionals and organisations in dealing with evolving privacy and security issues within the context of pervasive computing [11]. Taking a more general approach, Ahmady et al. provide a review of cybersecurity measures involving IoT, with specific attention to the integration of AI, machine learning and risk management especially when dealing with the security of interconnected devices [12]. Lastly, Pasdar provides an examination of threat models in IoT-enhanced combat systems, with a deeper look at the integration of blockchain, machine learning, game theory, protocols and algorithms within these systems [13]. These are some works that delve into the cybersecurity aspects of pervasive computing.

Finally, we recommend anyone interested in a textbook that offers a historical perspective on the origins and evolution of pervasive computing to have a closer look at Raju's recent work in [14].

2. IN THIS THEMATIC ISSUE

Continuing the theme presented beforehand in Section 1, this issue features seven novel papers centered around artificial intelligence and cybersecurity. The following is a preview of these articles, grouped into the two main domains of AI and cybersecurity.

2.1 Artificial Intelligence

There are a total of five papers that research on AI in this issue.

Zaman et al.'s work entitled "Intelligent Abstractive Summarization of Scholarly Publications with Transfer Learning," [15] explores two models for generating titles from the abstracts of scientific articles using abstractive summarization techniques. The study implements a Gated Recurrent Unit (GRU) encoder with a greedy-search decoder, as well as a Transformer-based model. Both models are evaluated against a baseline Long Short-Term Memory (LSTM) model. The Transformer model demonstrates superior performance with a ROUGE-1 score of 0.2881 compared to the LSTM's 0.1033. The paper highlights the advantages of abstractive summarization over extractive methods, noting that it produces more concise and coherent summaries. A key aspect is the use of attention mechanisms in the GRU and Transformer models, which effectively manage longer sequences of text. Previous works like Paulus et al.'s deep reinforcement model for abstractive summarization [16] and Vaswani et al.'s transformer architecture [17] are referenced to contextualize the study's contributions.

Following a similar vein, Sarwar et al.'s work entitled "HybridEval: An Improved Novel Hybrid Metric for Evaluation of Text Summarisation" [18] reevaluates the evaluation method for text summarization tasks with two state-of-the-art assessment measures – Recall-Oriented Understudy for Gisting Evaluation (ROUGE) and Bilingual Evaluation Understudy (BLEU). HybridEval, the proposed algorithm organizes phrases into six distinct groups to evaluate text summarization problems that utilizes wieighted sum of cosine scores from InferSent's SentEval algorithms [19] to achieve high accuracy.

In Goel et al.'s work entitled "Sibling Discrimination Using Linear Fusion on Deep Learning Face Recognition Models" [20], an interesting perspective on the study of distinguishing siblings using facial recognition, advancing work on human identification. The authors propose a non-invasive alternative to traditional methods, leveraging on deep learning to distinguish siblings based on partial facial features. Their techniques include a combination of advanced deep learning models such as VGG19, VGG16, VGGFace [21] and FaceNet [22], and a linear fusion technique for high accuracy and reliability.

Finally, crossing the bridge between AI and cybersecurity, Kim et al's work entitled "Conditional Deployable Biometrics: Matching Periocular and Face in Various Settings" [23] showcases concepts designed to deliver consistent performance across various biometric matching scenarios that include intra-modal, multimodal and cross-modal applications. The authors developed CBD-NET a deep neural network specially tailored for periocular and face biometric modalities to realize this. Benchmarking on five in-the-wild datasets, the effectiveness of CBD-NET is demonstrated with drastic performance improvements in comparison with baseline networks.

2.2 *Cybersecurity*

As we delve into the area of cybersecurity, a total of three papers in this editorial are presented covering very different fields.

The first, entitled "Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker" by Jimoh and Al-juboori [24], studies and improves on the cybersecurity framework of pacemaker devices, first identifying potential vulnerabilities and introducing effective strategies to counter them. The authors cover a myriad of vulnerabilities including unauthorized entry, data breaches and life-threatening device malfunctions. The authors also employs a quantitative research approach, utilizing the WUSTL-EHMS-2020 dataset [25] to train machine learning GBM and SVM models for predicting cyber threats. The authors then showed that the GBM model significantly outperformed SVM across evaluation metrics.

The second paper by Teh et al entitled "Towards Analysable Chaos-based Cryptosystems: Constructing Difference Distribution Tables for Chaotic Maps" [26] examines how a novel method using chaotic maps that facilitates cryptanalysis can be used to provide third-party cryptanalysis efforts on complex chaos-based cryptosystems. This is done using a fixed-point representation in place of floating-point, thus allowing the computation of chaotic maps using straightforward binary operations. The authors also demonstrate the creation of a chaos-based substitution function that is constructed using fixed-point representation and enables of conventional cryptanalysis using the difference distribution table. Finally, the authors show a proof-of-concept that applies the method to the logistic map, demonstrating the feasibility of designing analysable chaos-based cryptographic components with well-understood security margins.

Finally for the last paper by Kam et al. entitled "In Search of Suitable Methods for Cost-Benefit Analysis of Cyber Risk Mitigation in Offshore Wind: A Survey" [27], the authors evaluate the results of a systematic literature review on existing proposed solutions for cost benefit analysis on cybersecurity risk mitigation measures for offshore wind cyber physical systems. The authors describe the methodology for their systematic literature review in detail, and in the process, discover a lack of studies conducted on cost-benefit analysis research in the area. The authors show current works lack detailed cost modeling for offshore wind beyond general breakdowns encompassing capital, maintenance and labour or installation expenses. The authors then propose opportunities for research to be done in the field to obtain larger data sets for further study.

3. CONCLUSION

As computing becomes more widespread in our daily lives, the link between AI and cybersecurity becomes increasingly crucial. The articles in this collection explore how AI is improving common tech systems while also exploring new security advancements related to pervasive computing. We hope these articles will provide fresh insights into how AI and cybersecurity advancements in pervasive computing can lead to the creation of smart programs and security measures that work together to create a more connected and secure future. By understanding these advancements, we can build a safer and more efficient digital world.

ACKNOWLEDGEMENT

The author wishes to thank all contributors, reviewers and copyeditors who supported this special issue. A special thanks to Prof. Su-Cheng Haw for her guidance in the preparation and completion of this guest editorial, and to Multimedia University for an opportunity to contribute to the Journal of Informatics and Web Engineering. Lastly, the author is grateful to the University of Plymouth for the allocation of research time for the completion of this work.

AUTHOR CONTRIBUTIONS

Ji-Jian Chin: Completed the entire article

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

Our publication ethics follow The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org/

REFERENCES

[1] "State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally," IoT Analytics. Accessed: Sep. 29, 2024. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[2] A. Ltd, "What is Ubiquitous Computing?," *Arm | The Architecture for the Digital World*. 2024. [Online]. Available: https://www.arm.com/glossary/ubiquitous-computing

[3] "Fine-tuning now available for GPT-4o." [Online]. Available: https://openai.com/index/gpt-4o-fine-tuning/

[4] "Introducing Orion, Our First True Augmented Reality Glasses," *Meta*. [Online]. Available: https://about.fb.com/news/2024/09/introducing-orion-our-first-true-augmented-reality-glasses/

[5] "Llama 3.2," Meta Llama. [Online]. Available: https://www.llama.com/

[6] N. Sharghivand, F. Derakhshan, L. Mashayekhy, and L. Mohammadkhanli, "An Edge Computing Matching Framework With Guaranteed Quality of Service," *IEEE Transactions on Cloud Computing*, vol. 10, no. 3, pp. 1557–1570, 2022, doi: 10.1109/TCC.2020.3005539.

[7] K. Tocze and S. Nadjm-Tehrani, "The Necessary Shift: Toward a Sufficient Edge Computing," *IEEE Pervasive Computing*, vol. 23, no. 2, pp. 7–16, 2024, doi: 10.1109/MPRV.2024.3386337.

[8] A. Kumar, T. Braud, S. Tarkoma and P. Hui, "Trustworthy AI in the Age of Pervasive Computing and Big Data," *IEEE International Conference on Pervasive Computing and Communications Workshops*, 2020, pp. 1-6, doi: 10.1109/PerComWorkshops48775.2020.9156127.

[9] H. Gou, G. Zhang, E. P. Medeiros, S. K. Jagatheesaperumal, and V. H. C. de Albuquerque, "A Cognitive Medical Decision Support System for IoT-Based Human-Computer Interface in Pervasive Computing Environment," *Cognitive Computation*, vol. 16, no. 5, pp. 2471–2486, 2024, doi: 10.1007/s12559-023-10242-4.

[10] A. Bimpas, J. Violos, A. Leivadeas, and I. Varlamis, "Leveraging pervasive computing for ambient intelligence: A survey on recent advancements, applications and open challenges," *Comput. Network*, vol. 239, p. 110156, 2024, doi: 10.1016/j.comnet.2023.110156.

[11] L. Ahuja, R. Simon, and A. Thakur, "Privacy and Security Considerations in Healthcare: Navigating the Challenges of IoT and Ubiquitous Computing," *Smart Technologies in Healthcare Management*, CRC Press, 2024.

[12] E. Ahmady, A. R. Mojadadi, and M. Hakimi, "A Comprehensive Review of Cybersecurity Measures in the IoT Era," *Journal of Social Science Utilizing Technology*, vol. 2, no. 1, 2024, doi: 10.70177/jssut.v2i1.722.

[13] A. Pasdar, N. Koroniotis, M. Keshk, N. Moustafa, and Z. Tari, "Cybersecurity Solutions and Techniques for Internet of Things Integration in Combat Systems," *IEEE Transactions on Sustainable Computing*, pp. 1–20, 2024, doi: 10.1109/TSUSC.2024.3443256.

[14] V. Raju, "Origins and Evolution of Pervasive Computing: A Historical Perspective," *Ubiquitous Computing and Technological Innovation for Universal Healthcare*, IGI Global, 2024, pp. 1–32. doi: 10.4018/979-8-3693-2268-0.ch001.

[15] F. Zaman, M. Afzal, P.S. Teh, R. Sarwar, F. Kamiran, N.R. Aljohani, R. Nawaz, M.U. Hassan, and F. Sabah, "Intelligent Abstractive Summarization of Scholarly Publications with Transfer Learning," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 256–270, 2024. doi: 10.33093/jiwe.2024.3.3.16

[16] R. Paulus, C. Xiong, and R. Socher, "A Deep Reinforced Model for Abstractive Summarization," *International Conference on Learning Representations*, 2018. [Online]. Available: https://openreview.net/forum?id=HkAClQgA-

[17] A. Vaswani *et al.*, "Attention Is All You Need," arXiv.org. 2024. [Online]. Available: https://arxiv.org/abs/1706.03762v7

[18] R. Sarwar, B. Ahmad, P.S. Teh, S. Tuarob, T. Thaipisutikul, F. Zaman, N.R. Aljohani, J. Zhu, S.U. Hassan, R. Nawaz, A.R. Ansari, M.A.B. Fayyaz, "HybridEval: An Improved Novel Hybrid Metric for Evaluation of Text

Summarization," *Journal of Informatics and Web Engineering,* vol. 3, no. 3, pp. 233–255, 2024. doi: 10.33093/jiwe.2024.3.3.15.

[19] A. Conneau, D. Kiela, H. Schwenk, L. Barrault, and A. Bordes, "Supervised Learning of Universal Sentence Representations from Natural Language Inference Data," *Conference on Empirical Methods in Natural Language Processing*, M. Palmer, R. Hwa, and S. Riedel, Eds., Copenhagen, Denmark: Association for Computational Linguistics, 2017, pp. 670–680. doi: 10.18653/v1/D17-1070.

[20] R. Goel, M. Alamgir, W. Wahab, M. Alamgir , I. Mehmood , H. Ugail , A. Sinha, "Sibling Discrimination Using Linear Fusion on Deep Learning Face Recognition Models," *Journal of Informatics and Web Engineering,* vol. 3, no. 3, pp. 214–2 32., 2024. doi: 10.33093/jiwe.2024.3.3.14

[21] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition," 2015, *arXiv*: arXiv:1409.1556. doi: 10.48550/arXiv.1409.1556.

[22] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A Unified Embedding for Face Recognition and Clustering," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823. doi: 10.1109/CVPR.2015.7298682.

[23] J. Kim, T.S. Ng, and A.B.J Teoh, "Conditional Deployable Biometrics: Matching Periocular and Face in Various Settings," *Journal of Informatics and Web Engineering,* vol. 3, no. 3, pp. 302–313, 2024. doi: 10.33093/jiwe.2024.3.3.19.

[24] S. T. Jimoh and S. Al-Juboori, "Cyber-Securing Medical Devices Using Machine Learning: A Case Study of Pacemaker," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 271–289. 2024. doi: 10.33093/jiwe.2024.3.3.17

[25] A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study," *IEEE Access*, vol. 8, pp. 106576–106584, 2020, doi: 10.1109/ACCESS.2020.3000421.

[26] J. S. Teh and A. Abba, "Towards Analysable Chaos-based Cryptosystems: Constructing Difference Distribution Tables for Chaotic Maps," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 290-301. 2024, doi: 10.33093/jiwe.2024.3.3.18

[27] Y. H.-S. Kam, K. Jones, R. Rawlinson-Smith, and K. Tam, "In Search of Suitable Methods for Cost-Benefit Analysis of Cyber Risk Mitigation in Offshore Wind: A Survey," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 314-328, 2024, doi: 10.33093/jiwe.2024.3.3.20.

BIOGRAPHIES OF AUTHORS

Ji-Jian Chin completed his PhD in cryptography from Multimedia University and is currently lecturing at the University of Plymouth. His main research interests are in identification schemes without certificates and has worked extensively on both theoretical proofs and practical deployments of such schemes. Ji-Jian Chin can be contacted at ji-jian.chin@plymouth.ac.uk