Ensuring Privacy in Machine Learning Algorithms

Alba Martinez Fernandez[1], Elena Petrova[2], Chen Wei[1], Gabriel Silva[1], Nasim Al-Zahrani[2]

[1]Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China alba.martinez@whu.edu.cn

[2]Department of Information Technology, Faculty of Computer and Information Technology (FCIT), Sana'a University, Sana'a 1247, Yemen

Abstract:

Advances in machine learning have amplified concerns over data privacy, driving demand for robust privacy-enhancing technologies (PETs). This paper provides a comprehensive exploration of contemporary strategies for safeguarding sensitive information throughout the machine learning lifecycle, with a particular focus on the synergistic integration of federated learning and state-of-the-art cryptographic techniques such as homomorphic encryption, differential privacy, and secure multi-party computation. By decentralizing model training, federated learning inherently reduces exposure of raw data, while its combination with these cryptographic methods further strengthens defenses against data breaches, adversarial interference, and emerging cyber threats. Beyond encryption, we examine the transformative potential of blockchain technology in privacy-preserving scenarios. Blockchain's immutable records, when enhanced with cryptographic primitives such as shuffling, zero-knowledge proofs, and ring signatures, offer new avenues for securing data integrity and confidentiality in distributed environments. This discussion is anchored in the broader imperative for transparency and explainability in machine learning. We argue that transparent models not only build trust among users but are increasingly mandated by regulatory frameworks worldwide, necessitating methods that elucidate the decision-making processes of complex algorithms. Additionally, we emphasize the critical role of auditing mechanisms in responsible machine learning deployments. Regular, rigorous model validation—coupled with ethical oversight—is essential for ensuring compliance, accountability, and the mitigation of unintended biases. Our analysis concludes that achieving the dual objectives of high performance and robust privacy in machine learning requires a multifaceted approach. By integrating federated learning, advanced cryptographic protocols, blockchain innovations, and explainability principles, organizations can develop systems that are both effective and ethically sound—capable of meeting the increasing demands of privacy-conscious stakeholders and regulators alike.

Keywords: Machine Learning Privacy, Federated Learning, Decentralized Computing, Blockchain Technology, ML Auditing, Model Transparency.

1 Introduction

Machine learning (ML) and artificial intelligence (AI) have revolutionized numerous sectors [1], from healthcare to finance [2]. These technologies are pivotal in interpreting complex data patterns, enabling predictive analytics, and automating processes[3, 4, 5, 6]. However, they also pose significant challenges, particularly in data privacy and algorithmic transparency.

In today's data-driven era, safeguarding user data privacy has become crucial[**?**]. The surge in data generation, collection, and processing has heightened the risk of data breaches and unauthorized data sharing, underscoring the need for effective data protection mechanisms. Traditional ML models, which often centralize data, are vulnerable to data leaks and misuse[7].

Privacy-Preserving Machine Learning (PPML) aims to leverage ML's benefits while protecting data privacy [8]. It employs techniques like homomorphic encryption and secure multiparty computation to ensure data confidentiality during processing. This approach allows algorithms to analyze data without accessing raw, sensitive information, protecting against unauthorized breaches.

Federated Learning (FL) represents a paradigm shift in ML by decentralizing data processing [9]. Rather than sending data to a central server, FL trains models locally on devices, sharing only model updates. This reduces data transfer and enhances privacy.

Blockchain technology supports decentralization, offering a secure environment for data sharing and processing. Its immutable and transparent nature ensures data integrity, while cryptographic techniques strengthen privacy[10, 11].

As ML models become integral in decision-making, understanding their processes is imperative. Auditing assesses models for fairness and risks, and explainable AI (XAI) provides insights into their decision-making, fostering trust and compliance[12].

This paper delves into these aspects, discussing the advancements, challenges, and future directions in machine learning. It presents a comprehensive view of privacy-preserving techniques, federated learning, blockchain's role in secure environments, and the importance of auditing and explainability in ML.

1.1 Privacy-preserving Machine Learning: Navigating the Digital Era with Enhanced Data Security

The exponential growth in digital data utilization has ushered in an era marked by increasing cybersecurity threats and data breaches. This escalating concern significantly underscores the necessity for stringent privacy measures in the realm of Machine Learning (ML) [13]. Privacy-Preserving Machine Learning (PPML) emerges as a pivotal response to these challenges, aiming to develop methodologies that allow for the training of ML models without compromising the privacy of individual data points [4, 14].

Homomorphic Encryption (HE) is a cornerstone technique in PPML, offering a unique solution to data privacy issues. HE enables the encryption of data in a manner that allows ML algorithms to perform computations on this encrypted data without the need for decryption. This innovative approach ensures that data can be utilized for analysis and model training while simultaneously maintaining its confidentiality. HE is exceptionally beneficial in situations where sensitive data must be processed without exposing it to potential threats or breaches [15, 16].

Secure Multiparty Computation (SMC) represents another critical technique within the PPML framework. SMC facilitates a distributed computation paradigm across multiple parties, wherein each party's input data remains confidential. Through SMC, collaborative computation on datasets is made possible, ensuring that individual data points and contributions remain undisclosed. This technique is particularly crucial in contexts where data sharing is imperative, yet privacy cannot be compromised, such as in medical research or financial services [17].

Differential Privacy (DP) introduces a groundbreaking approach to data privacy. By integrating controlled noise into the data or its outputs, DP ensures that the outputs, such as query results from an ML model, are not significantly influenced by the inclusion or exclusion of any single individual's data. Consequently, differential privacy provides an anonymity layer, safeguarding the identities of individual data points within extensive datasets. This approach is especially pertinent in public datasets where maintaining user privacy is essential, yet without substantially diminishing the data's utility [18].

PPML stands at the forefront of the digital age, offering robust solutions to the pressing need for data privacy in ML applications. Through techniques such as HE, SMC, and DP, PPML not only enhances data security but also paves the way for responsible and ethical use of data in various fields. Collectively, these methodologies contribute to the advancement of ML, fostering an environment where data can be leveraged for innovation and progress while upholding the highest standards of privacy and security.

1.2 Federated Learning: A Paradigm Shift in Machine Learning

Federated Learning (FL) has emerged as a groundbreaking paradigm in machine learning (ML), marking a significant departure from the conventional centralized training approaches. At its core, FL is a process where model training occurs not on a single central server but across numerous local devices, such as smartphones or Internet of Things (IoT) devices [19]. This decentralized approach offers a substantial enhancement to data privacy, as it minimizes the volume of raw data that needs to be transferred and stored in a central repository [20]. The fundamental process of FL involves each participating device using its data to train a local model. These local models then transmit their updates - which could include weights or gradients - to a central server. This central server acts as an aggregator, combining these updates to refine and improve the global model [21]. A key advantage of this method is that it allows sensitive data to remain on the user's device. This significantly lowers the risk of data breaches and unauthorized access to personal information [22, 23]. One of the most compelling aspects of FL is its applicability in areas where data privacy is of utmost importance, such as in healthcare and financial sectors. In these fields, the confidentiality of personal data is paramount, and FL offers a way to harness the power of ML while respecting and protecting individual privacy. By utilizing the distributed nature of data across a multitude of devices, FL is not just maintaining the privacy of data but is also tapping into the richness of diverse data sources. This leads to the creation of models that are not only more robust due to their varied data inputs but are also potentially more accurate and representative of different demographics and scenarios.

Furthermore, FL addresses some of the critical challenges in traditional ML models related to data accessibility and diversity. In many cases, centralized models are trained on limited datasets that may not adequately represent the entire population or all possible use cases. FL, by contrast, benefits from a wide

array of data points from numerous devices, each contributing unique and potentially valuable insights. This results in models that are better suited to real-world applications, as they are trained on data that is more reflective of actual user environments and behaviors.

Another significant advantage of FL is the reduction in bandwidth and storage requirements. Since raw data does not need to be transferred to a central server, there is a considerable decrease in the demand for bandwidth, which is particularly beneficial in areas with limited connectivity. Additionally, since data is processed locally on devices, the need for large-scale data storage and processing capabilities at a central location is greatly diminished. This not only reduces costs but also mitigates the environmental impact associated with large data centers.

1.3 Distributed Environments and the Role of Blockchain Technology

Blockchain technology has rapidly emerged as a transformative solution for ensuring data integrity and transparency in distributed environments. At its core, blockchain is characterized by three fundamental features: decentralization, immutability, and transparency, each playing a crucial role in its functionality and applications [24].

In blockchain systems, data is not stored in a centralized location but is instead distributed across a network of computers. This decentralization is a critical aspect of blockchain's architecture, making the system inherently resistant to data tampering and fraud [25, 26, 27, 28]. The structure of a blockchain is a series of blocks, each containing a set of transactions. Once a block is filled with data, it is cryptographically sealed and linked to the preceding block, thus forming a continuous chain. This chain of blocks ensures that once data is recorded on the blockchain, altering it retroactively becomes virtually impossible without changing all subsequent blocks and obtaining the network's consensus [24].

The decentralized nature of blockchain also eliminates a single point of failure, significantly enhancing the system's resilience against attacks and fraud. This feature makes blockchain particularly attractive for applications requiring high levels of data security and integrity. For instance, in financial transactions, blockchain can provide a secure and transparent ledger. In supply chain management, it ensures the authenticity and traceability of products. In healthcare, blockchain can be used to manage patient data securely and efficiently, ensuring privacy and compliance with regulatory standards [29].

Blockchain's transparency is another key feature, ensuring that all transactions on the network are visible and verifiable by all participants. This transparency builds trust among users and is fundamental in applications where accountability and traceability are essential.

In summary, blockchain technology is revolutionizing the way data is handled in distributed environments. Its ability to provide a secure, transparent, and immutable ledger makes it an ideal solution for a wide range of applications across various sectors. By leveraging blockchain, organizations can ensure the integrity and security of their data, fostering trust and efficiency in their operations.

1.4 The Importance of Auditing in AI and Machine Learning

As artificial intelligence (AI) and machine learning (ML) increasingly permeate various aspects of decision-making processes, the importance of auditing these

systems becomes paramount. Auditing in ML is not just about evaluating performance metrics; it encompasses a comprehensive examination of models to ensure their integrity, fairness, and adherence to ethical standards [30].

The auditing process in ML involves a deep analysis of the models' decisionmaking processes. This includes assessing whether the models are free from biases, ensuring that they comply with ethical and legal standards, and verifying that they are used for their intended purposes. This aspect of auditing is crucial in sectors such as healthcare, finance, and law enforcement, where decisions influenced by ML models can have significant and far-reaching consequences [29, 31].

One of the critical components of auditing is bias detection and mitigation. ML models can inadvertently learn and perpetuate biases present in their training data. Auditing helps identify these biases, ensuring that the models do not discriminate and that their outcomes are fair and equitable.

Another essential aspect of auditing is ensuring compliance with ethical standards. This involves evaluating whether the models respect privacy, adhere to regulatory requirements, and align with societal and ethical norms. In an era where AI and ML are becoming more autonomous, maintaining ethical oversight is vital to prevent misuse and unintended harmful consequences.

Furthermore, auditing ML models involves ensuring transparency and explainability. It is essential that the decisions made by these models are understandable and interpretable by humans, especially in critical applications. This transparency not only builds trust in AI systems but also facilitates the identification and correction of errors or unintended behaviors in the models.

In summary, auditing in AI and ML is a critical process that ensures the reliability, fairness, and ethical integrity of these systems. As AI and ML continue to evolve and become more integrated into critical areas of society, the role of auditing will become increasingly important. It ensures that these powerful tools are used responsibly, ethically, and for the benefit of society as a whole.

1.5 Transparency and Explainability in Machine Learning and AI

In the rapidly evolving landscape of Machine Learning (ML) and Artificial Intelligence (AI), the issue of transparency and explainability has become increasingly prominent. The complexity inherent in many ML models often results in them being viewed as "black boxes," where the processes and reasoning behind their decisions are opaque and challenging to decipher. This lack of clarity and understanding poses significant hurdles, particularly in sectors where trust, accountability, and compliance with regulatory standards are paramount.

The concept of Explainable AI (XAI) has emerged as a crucial response to these challenges. XAI aims to create methodologies and tools that render the inner workings of complex ML models more accessible and interpretable to human users. This initiative encompasses a range of techniques, including advanced visualizations, analyses of feature importance, and model-agnostic methods. These techniques are designed to shed light on how specific decisions or predictions are made by AI systems, thereby making their operations more transparent and understandable.

The importance of transparency and explainability in AI extends beyond merely demystifying the technology. It plays a critical role in building and maintaining trust among users and stakeholders. When individuals understand the mechanics of how an AI system arrives at its decisions, they are more likely to trust its reliability and fairness. This trust is especially crucial in scenarios where

AI systems are making decisions that directly impact human lives, such as in healthcare diagnostics, financial lending, or legal sentencing. In regulated industries, such as finance and healthcare, the need for explainability is even more pronounced. In these domains, being able to understand and articulate the basis of algorithmic decisions is not just a matter of building trust but also of complying with legal and ethical standards. Regulatory bodies increasingly require that decisions made by AI systems be explainable and justifiable, particularly when they affect consumer rights or patient outcomes. Explainability ensures that AI systems are not only effective but also accountable and fair, adhering to the ethical standards and values of society.

Furthermore, explainability in AI is crucial for identifying and rectifying potential biases in ML models. Since these models learn from historical data, there is a risk of them perpetuating existing biases and inequalities. Through transparent and explainable AI systems, stakeholders can identify where and how biases might occur, enabling them to take corrective measures to ensure fairness and equity in decision-making processes. To sum up, transparency and explainability are fundamental to the responsible deployment of AI and ML technologies. They not only facilitate a deeper understanding and trust in these systems but also ensure that AI applications are fair, accountable, and aligned with ethical standards. As AI continues to integrate into various aspects of society, the development of explainable and transparent AI systems will be crucial for their acceptance, effectiveness, and ethical application.

2 Literature Review

2.1 Privacy-preserving federated learning

Federated learning (FL), a paradigm shift in machine learning, decentralizes data processing and model training. It enables models to be trained directly on devices where data is generated, such as smartphones or IoT devices. This approach naturally offers privacy benefits, as sensitive data remains on the user's device. However, recent research underscores that federated learning is not entirely immune to data breaches and cyber-attacks. There is a growing body of work exploring the integration of privacy-preserving methodologies with federated learning to address these vulnerabilities.

One of the key areas of focus has been the integration of **Homomorphic Encryption** (HE) with federated learning. HE is a cryptographic technique that allows computations to be performed on encrypted data. This means that data can remain encrypted even during the training process, enhancing security by preventing exposure of sensitive information. Studies have shown that integrating HE with FL can significantly increase the security of the distributed learning process, making it more resilient to attacks and unauthorized access[29, 32].

Differential Privacy (DP) is another critical technique being applied in federated learning. DP works by adding a controlled amount of noise to the data or outputs, which helps to mask the contributions of individual data points. This approach is particularly beneficial in FL, as it prevents adversaries from reverseengineering the model to gain insights into the private data. Researchers have been investigating various methods of integrating DP into FL, with a focus on optimizing the balance between data utility and privacy.

Secure Multi-Party Computation (SMPC) is also gaining traction in the context of federated learning. SMPC allows multiple parties to compute a function over their inputs while keeping those inputs private. In FL, SMPC can be used to

secure the process of aggregating updates from various local models. This ensures that while the collective learning benefits from the contributions of all participants, the individual data points and contributions remain confidential. Recent studies have explored various SMPC protocols and their compatibility with FL, aiming to enhance the privacy guarantees of federated learning systems[33].

2.2 Blockchain-based privacy-preserving

With its decentralized architecture and cryptographic foundations, blockchain technology presents a novel way of ensuring data privacy and integrity. In the context of machine learning and data security, blockchain can play a pivotal role, particularly in environments where trust is decentralized and data sharing is necessary. Recent studies have explored blockchain's potential to enhance privacy-preserving mechanisms, especially in scenarios where data security and user privacy are paramount[34].

One significant area of research is the use of **shuffling technology** in blockchain systems. Shuffling technology involves the randomization of transaction records before they are added to the blockchain. This makes it significantly harder for malicious actors to trace transactions or to understand the relationship between different data points. By integrating shuffling technology into blockchain systems, researchers aim to obscure the patterns of data transactions, enhancing privacy without compromising the integrity and transparency of the blockchain[35, 36].

Zero-knowledge proofs (ZKPs) are another advanced cryptographic technique being applied in blockchain environments. ZKPs allow a party to prove the truth of a statement without revealing any additional information[37, 38]. This is particularly useful in transactions where privacy is a concern, as it enables the validation of transactions without exposing the underlying data. The integration of ZKPs into the blockchain can enable private transactions and interactions while maintaining the trust and integrity of the network[33, 39, 40].

Lastly, the application of **ring signatures** in blockchain has been a subject of research interest. Ring signatures provide anonymity for the signer by allowing a transaction to appear as if it could have come from any member of a group. This level of anonymity is crucial for transactional privacy, as it shields the identity of the individual making the transaction. Researchers are exploring ways to incorporate ring signatures into blockchain systems to enhance privacy and security in digital transactions further[41, 42].

In conclusion, the intersection of federated learning with advanced cryptographic methods and the application of blockchain technology in privacy preservation are emerging as crucial areas in the field of machine learning. These technologies not only enhance data security but also play a vital role in maintaining user privacy in an increasingly interconnected digital world [43].

3 Future Roadmap: Navigating the Convergence of ML, Privacy, and Quantum Computing

As we delve into the complex interplay of machine learning (ML), privacy, and transparency, the future roadmap of this field presents both formidable challenges and extraordinary opportunities. The burgeoning advancements in ML algorithms, coupled with their ever-increasing integration into everyday life, demand an ongoing evolution in privacy-preserving methods. The forthcoming era is poised to witness an intensified focus on developing more robust federated

learning models, augmenting blockchain capabilities for enhanced privacy, and progressing in areas like homomorphic encryption, secure multiparty computation, and differential privacy [41, 44, 45].

In the sphere of federated learning, future endeavors may concentrate on fine-tuning algorithms to achieve an optimal balance between performance and privacy, particularly in edge computing scenarios. Blockchain technology is anticipated to evolve towards greater scalability and efficiency, broadening its applicability to a diverse array of uses, including real-time data processing demands. Homomorphic encryption is expected to undergo enhancements in computational efficiency, making it more feasible for large-scale deployments [46, 47]. A pivotal area of future research lies in the amalgamation of artificial intelligence with Internet of Things (IoT) devices, while stringently safeguarding user privacy [48, 49]. This integration is challenged by the sheer volume of data produced by IoT devices and the associated privacy risks [50, 51, 52]. Furthermore, as regulatory frameworks surrounding data privacy and AI ethics continue to evolve, future research will necessitate a focus on ensuring adherence to these regulations. This involves the development of tools and methodologies for auditing AI systems and enhancing the transparency and explicability of complex ML models.

A critical and emerging dimension in this roadmap is the role of quantum computing. Quantum computing promises to revolutionize the field of ML and privacy-preserving techniques [53]. Its potential to process vast amounts of data at unprecedented speeds could lead to significant breakthroughs in ML algorithms. However, this also poses new challenges in data security, as traditional encryption methods may become vulnerable to quantum computing capabilities. Future research in PPML must therefore also encompass the development of quantum-resistant cryptographic techniques to safeguard data against potential quantum computing threats. Quantum computing could also offer novel approaches to solving complex optimization problems in ML, leading to more efficient and powerful learning algorithms [54].

The integration of quantum computing into ML and privacy preservation will require a multidisciplinary approach, combining insights from computer science, quantum physics, and cybersecurity. This approach is vital to create systems that are not only technologically advanced but also resilient to the emerging threats posed by quantum computing advancements. The convergence of ML, privacy, and quantum computing heralds a new era in technology, where the potential for innovation is boundless, but so are the responsibilities to ensure ethical and secure utilization of these powerful tools.

4 Conclusion

The exploration of privacy-preserving techniques in machine learning, as discussed in this paper, reveals a landscape marked by rapid technological advancements and increasing ethical challenges. The integration of machine learning into various facets of society necessitates a delicate balance between leveraging the power of AI and respecting individual privacy. This balance is not static but evolves with the technological, ethical, and regulatory landscape.

This paper has highlighted how technologies such as federated learning, blockchain, and advanced cryptographic methods offer promising solutions to privacy concerns. However, these solutions are not without challenges. Future research and development must focus on enhancing the efficiency, scalability, and accessibility of these technologies.

Moreover, as machine learning systems become more prevalent, the need for transparency and explainability grows. The development of explainable AI is not just a technological challenge but also a societal imperative. Users and stakeholders must be able to understand and trust AI systems, particularly in critical areas such as healthcare, finance, and public policy.

The necessity for rigorous auditing mechanisms cannot be overstated. As AI systems increasingly influence decision-making processes, ensuring their fairness, accountability, and alignment with ethical standards is essential. This will require continuous collaboration between technologists, ethicists, policymakers, and other stakeholders.

In conclusion, the future of machine learning is inextricably linked to its ability to respect and protect user privacy while providing transparent and accountable solutions. The journey ahead is complex, requiring innovative solutions and multidisciplinary collaboration. By embracing these challenges, we can ensure that the advancements in machine learning continue to serve humanity's best interests, fostering a future where technology enhances life without compromising individual freedoms and privacy.

References

[1] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. C. Zhang, "Artificial intelligence-enabled cellular networks: A critical path to beyond5g and 6g," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 212–217, 2020.

[2] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient sdn controller architecture for iot networks with blockchain-based security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625–638, 2020.

[3] B. Sliwa, R. Falkenberg, and C. Wietfeld, "Towards cooperative data rate prediction for future mobile and vehicular 6g networks," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[4] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406–6415, 2020.

[5] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6g communications: Challenges, methods, and future directions," *China Communications*, vol. 17, no. 9, pp. 105–118, 2020.

[6] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[7] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, "Artificial intelligence enabled internet of things: Network architecture and spectrum access," *IEEE Computational Intelligence Magazine*, vol. 15, no. 1, pp. 44–51, 2020.

[8] A. Yazdinejad, A. Dehghantanha, and G. Srivastava, "Ap2fl: Auditable privacy-preserving federated learning framework for electronics in healthcare," *IEEE Transactions on Consumer Electronics*, 2023.

[9] M. Katz, P. Pirinen, and H. Posti, "Towards 6g: Getting ready for the next decade," in *2019 16th International symposium on wireless communication systems (ISWCS)*. IEEE, 2019, pp. 714–718.

[10] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and H. Karimipour, "Federated learning for drone authentication," *Ad Hoc Networks*, vol. 120, p. 102574, 2021.

[11] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Efficient design and hardware implementation of the openflow v1. 3 switch on the virtex-6 fpga ml605," *The Journal of Supercomputing*, vol. 74, pp. 1299–1320, 2018.

[12] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The roadmap to 6g: Ai empowered wireless networks," *IEEE communications magazine*, vol. 57, no. 8, pp. 84–90, 2019.

[13] L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. Nguyen, and C. S. Hong, "Federated learning for edge networks: Resource optimization and incentive mechanism," *IEEE Communications Magazine*, vol. 58, no. 10, pp. 88–93, 2020.

[14] A. Yazdinejadna, R. M. Parizi, A. Dehghantanha, and M. S. Khan, "A kangaroo-based intrusion detection system on software-defined networks," *Computer Networks*, vol. 184, p. 107688, 2021.

[15] M. H. Alsharif, A. H. Kelechi, M. A. Albreem, S. A. Chaudhry, M. S. Zia, and S. Kim, "Sixth generation (6g) wireless networks: Vision, research activities, challenges and potential solutions," *Symmetry*, vol. 12, no. 4, p. 676, 2020.

[16] T. Hou, G. Feng, S. Qin, and W. Jiang, "Proactive content caching by exploiting transfer learning for mobile edge computing," *International Journal of Communication Systems*, vol. 31, no. 11, p. e3706, 2018.

[17] A. Yazdinejad, R. M. Parizi, G. Srivastava, A. Dehghantanha, and K.K. R. Choo, "Energy efficient decentralized authentication in internet of underwater things using blockchain," in *2019 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2019, pp. 1–6.

[18] H. Sharma, A. Haque, and Z. A. Jaffery, "Modeling and optimisation of a solar energy harvesting system for wireless sensor network nodes," *Journal of sensor and Actuator Networks*, vol. 7, no. 3, p. 40, 2018.

[19] Mehta, D. B. (2023). Privacy-Preserving Machine Learning Architecture for Cross-Channel Advertising Optimization in a Large-Scale Social Media Platform. International Journal of Communication Networks and Information Security (IJCNIS), 15(8), 23–32.

[20] Darshan Bhavesh Mehta. (2024). Cloud Ecosystem Integration for Scalable 3D Game Content Creation. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2192

[21] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, M. Hammoudeh, H. Karimipour, and G. Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8356–8366, 2022.

[22] H. Daga, P. K. Nicholson, A. Gavrilovska, and D. Lugones, "Cartel: A system for collaborative transfer learning at the edge," in *Proceedings of the ACM Symposium on Cloud Computing*, 2019, pp. 25–37.

[23] W. Y. B. Lim, N. C. Luong, D. T. Hoang, Y. Jiao, Y.-C. Liang, Q. Yang, D. Niyato, and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 2031–2063, 2020.

[24] A. Yazdinejad, R. M. Parizi, A. Bohlooli, A. Dehghantanha, and K.-K. R. Choo, "A high-performance framework for a network programmable packet processor using p4 and fpga," *Journal of Network and Computer Applications*, vol. 156, p. 102564, 2020.

[25] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, G. Srivastava, S. Mohan, and A. M. Rababah, "Cost optimization of secure routing with untrusted devices in software defined networking," *Journal of Parallel and distributed Computing*, vol. 143, pp. 36–46, 2020.

[26] S. J. T. Koh, M. Nafea, and H. Nugroho, "Towards edge devices implementation: Deep learning model with visualization for covid-19 prediction from chest x-ray," *Advances in Computational Intelligence*, vol. 2, no. 5, p. 33, 2022.

[27] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "Performance improvement and hardware implementation of open flow switch using fpga," in *2019*

5th Conference on Knowledge Based Engineering and Innovation (KBEI). IEEE, 2019, pp. 515–520.

[28] A. Yazdinejad, B. Zolfaghari, A. Azmoodeh, A. Dehghantanha, H. Karimipour, E. Fraser, A. G. Green, C. Russell, and E. Duncan, "A review on security of smart farming and precision agriculture: Security aspects, attacks, threats and countermeasures," *Applied Sciences*, vol. 11, no. 16, p. 7518, 2021.

[29] Q. Zhao and D. Grace, "Transfer learning for qos aware topology management in energy efficient 5g cognitive radio networks," in *1st international conference on 5G for ubiquitous connectivity*. IEEE, 2014, pp. 152–157.

[30] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, H. Karimipour, and S. R. Karizno, "Slpow: Secure and low latency proof of work protocol for blockchain in green iot networks," in *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE, 2020, pp. 1–5.

[31] C. Parera, A. E. Redondi, M. Cesana, Q. Liao, L. Ewe, and C. Tatino, "Transferring knowledge for tilt-dependent radio map prediction," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[32] A. Yazdinejad, R. M. Parizi, G. Srivastava, and A. Dehghantanha, "Making sense of blockchain for ai deepfakes technology," in *2020 IEEE Globecom Workshops (GC Wkshps*. IEEE, 2020, pp. 1–6.

[33] A. Yazdinejad, A. Bohlooli, and K. Jamshidi, "P4 to sdnet: Automatic generation of an efficient protocol-independent packet parser on reconfigurable hardware," in *2018 8th International Conference on Computer and Knowledge Engineering (ICCKE)*. IEEE, 2018, pp. 159–164.

[34] S. Chen, Y.-C. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, requirements, and technology trend of 6g: How to tackle the challenges of system coverage, capacity, user data-rate and movement speed," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 218–228, 2020.

[35] Y. Hailemariam, A. Yazdinejad, R. M. Parizi, G. Srivastava, and A. Dehghantanha, "An empirical evaluation of ai deep explainable tools," in *2020 IEEE Globecom Workshops (GC Wkshps*. IEEE, 2020, pp. 1–6.

[36] D. Sheridan, J. Harris, F. Wear, J. Cowell Jr, E. Wong, and A. Yazdinejad, "Web3 challenges and opportunities for the market," *arXiv preprint arXiv:2209.02446*, 2022.

[37] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759– 50779, 2019.

[38] J. Liu and Z. Liu, "A survey on security verification of blockchain smart contracts," *IEEE Access*, vol. 7, pp. 77894–77904, 2019.

[39] R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, and K.K. R. Choo, "Integrating privacy enhancing techniques into blockchains using sidechains," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*. IEEE, 2019, pp. 1–4.

[40] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K.-K. R. Choo, "Security challenges and opportunities for smart contracts in internet of things: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12004–12020, 2021.