IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

DataGuard: Authentication-Driven Privacy and Security in Machine Learning

[1]Harsh Shihora, [2]Khushi Shihora

[1]Designation of 1st Author: Researcher, [2]Designation of 2nd Author: Researcher & Writer
[1]Department of Information Technology, Shantilal Shah, Gujarat Technological University
[2]Department of Computer Science and Engineering, P P Savani University, Kosmba

Abstract : The increasing reliance on digital systems necessitates robust and innovative methods to ensure data privacy and security, particularly in the context of user authentication. Traditional two-factor authentication (2FA) methods, while effective, often impose burdens on users due to manual input requirements and frequent verification needs. This review explores the evolution of authentication systems through the lens of machine learning (ML), emphasizing the transition from conventional 2FA approaches to more seamless, continuous verification techniques. By leveraging environmental features such as beacon frame characteristics and Received Signal Strength Indicator (RSSI) values, ML-based systems can authenticate users with minimal effort, enhancing both security and user experience. Additionally, we investigate the integration of ML into physical layer (PHY) security, multi-factor authentication (MFA), and biometric systems, highlighting how these technologies strengthen the resilience of authentication processes against emerging cyber threats. Our analysis includes a detailed examination of the challenges and opportunities associated with deploying ML in authentication systems, particularly in terms of adversarial machine learning, scalability, and adaptability. The findings presented in this review underscore the potential of ML to revolutionize authentication, offering scalable and secure solutions for modern digital environments

Keywords: Physical Layer Security , Wireless Multiple Access Channel (W-MAC), PHY-Authentication, Internet of Things (IoT)

INTRODUCTION

In the modern digital era, the challenge of safeguarding data privacy and security has intensified due to the rapid evolution of technology and the increasing sophistication of cyber threats. Traditional security mechanisms, once considered robust, are now proving inadequate in the face of advanced and persistent attacks. This inadequacy has created an urgent need for the integration of innovative solutions to protect sensitive information and ensure secure digital interactions. This review paper delves into the application of machine learning (ML) across various domains of data privacy and security, illustrating its transformative impact on modern security practices. It highlights how ML is being leveraged to enhance security in critical areas such as physical layer security, where machine learning models improve the detection and prevention of spoofing attacks. Similarly, in the realm of biometric authentication, ML is combined with techniques like homomorphic encryption to protect biometric data, despite the challenges of computational demands.

The paper also explores the growing importance of multi-biometric systems, where machine learning enhances the accuracy and adaptability of iris recognition technologies. As the Internet of Things (IoT) expands, ML-based methods are being employed to analyze energy consumption patterns for device authentication, offering a novel approach to securing IoT environments. Additionally, the review addresses the limitations of static authentication methods, proposing continuous authentication models driven by reinforcement learning to provide dynamic and ongoing user verification. It also examines the innovative use of QR codes in authentication, and the integration of hand gesture and facial recognition in drone control, both of which demonstrate the versatility and potential of ML in enhancing security.

The paper further discusses advancements in two-factor authentication (2FA) using ML to improve scalability and user experience, and the application of ML models in mobile sensor data authentication to protect the integrity of sensor-generated data. Lastly, it explores the security challenges posed by the emerging urban metaverse environments, proposing the use of blockchain and privacy preserving ML models to safeguard these complex digital physical spaces.

Overall, this review highlights the critical role of machine learning in addressing the current challenges in data privacy and security, while also recognizing the ongoing challenges and areas for future research.

- We summarize and analyze recent research in the IoT authentication field to provide a comprehensive understanding of the current literature, providing the most used cryptographic techniques, and simulation tools.

• Open Source Contribution: This reinforcement learning (RL) gym-based environment code is made available on GitHub (GitHub: to the domain researchers to explore and utilize. https://github.com/PriyaBansal68/ContinuousAuthentication -Reinforcement-Learning-and Behavioral-Biometrics) (accessed on 18 April 2024).

• A unique PHY-authentication approach is proposed where multiple users can be authenticated without any prior information about attackers

2. RELATED WORK

The diagram illustrates the interconnectedness of physical layer security, wireless multiple access channels, PHY-authentication, and IoT devices. At the core lies the need for secure IoT communication, which is influenced by the underlying W-MAC infrastructure. Physical layer security measures, such as channel estimation and key generation, are essential for protecting data transmitted over the wireless channel. PHY-authentication techniques, often leveraging machine learning, ensure the legitimacy of communicating entities. IoT devices, with their diverse characteristics and resource constraints, require specialized security solutions. By understanding the interplay between these components, researchers and practitioners can develop effective strategies to safeguard IoT networks from various threats and ensure secure and reliable communication.

The intersection of physical layer security, wireless multiple access channel (W-MAC), PHY authentication, and IoT has been a burgeoning research area. Researchers have explored techniques like channel estimation and key generation for secure communication, cooperative jamming and artificial noise generation for enhancing security, and efficient resource allocation schemes in W-MACs. PHY authentication techniques, often leveraging machine learning, have been developed to distinguish legitimate users from malicious entities. In the IoT context, researchers have focused on lightweight authentication protocols, secure communication protocols, and addressing side-channel attacks. Specific research papers, such as those exploring machine learning approaches for PHY-authentication and secure spectrum sharing in cognitive radio networks, provide valuable insights into this field. The choice of related works to cite will depend on the specific focus of your own research and the aspects of these areas that you are exploring.

The structure of the remaining manuscript is as follows: IoT devices generate sensor data, which is collected by gateways or edge devices. After preprocessing and feature extraction, security measures like encryption and authentication are applied to protect the data. The secured data is then transmitted to a cloud or edge platform for analysis. Machine learning algorithms process the data to extract insights, leading to informed decisions and actions.

3.Models of machine learning for Physical Layer Security , Wireless Multiple Access Channel (WMAC), PHY-Authentication, Internet of Things (IoT).

3.1 Machine learning models are pivotal in enhancing security and optimizing performance within Physical Layer Security (PLS), Wireless Multiple Access Channels (W-MAC), PHY-Authentication, and the Internet of Things (IoT). By leveraging data-driven approaches, these models learn patterns, make predictions, and adapt to changing environments, making them invaluable in the complex and dynamic world of wireless communication. In the context of PLS, machine learning enhances security by identifying and exploiting subtle patterns in the wireless channel, enabling advanced techniques like anomaly detection and adaptive noise management. For instance, deep learning and reinforcement learning models can be used to detect anomalies that might indicate eavesdropping, optimize the generation of artificial noise to confuse attackers, and improve channel estimation and prediction, thereby bolstering the robustness of PLS techniques.

3.2 In W-MAC scenarios, machine learning optimizes how multiple devices share the wireless medium, enhancing both efficiency and security. Resource allocation is dynamically managed through ML models that consider usage patterns and channel conditions, while interference management is improved by predicting and mitigating potential conflicts in real-time. Access control is also enhanced through machine learning, allowing for intelligent decisions about which devices can access the channel based on their behavior and trust levels, a critical feature in securing IoT networks. Furthermore, PHY-Authentication benefits from machine learning by improving the accuracy and reliability of device identification based on physical layer characteristics. Machine learning models automatically extract relevant features from physical signals, distinguishing legitimate devices from impostors even in noisy environments, and enabling continuous authentication that adapts to real-time conditions.

3.3 In IoT networks, machine learning models are integral to security, resource management, and communication efficiency. These models power advanced anomaly detection and intrusion detection systems, identifying potential security threats by learning what constitutes normal behavior in the network. They also play a crucial role in optimizing energy consumption in IoT devices by predicting activity patterns and adjusting power usage accordingly, which is vital for extending the battery life of resource-constrained devices. Moreover, machine learning facilitates contextaware security, where security measures adapt based on environmental factors, device location, and user behavior, ensuring a tailored and robust defense against potential threats. Additionally, in distributed IoT networks, collaborative learning techniques like federated learning allow devices to improve security models collectively without compromising data privacy, demonstrating the versatility and importance of machine learning in modern wireless communication systems.

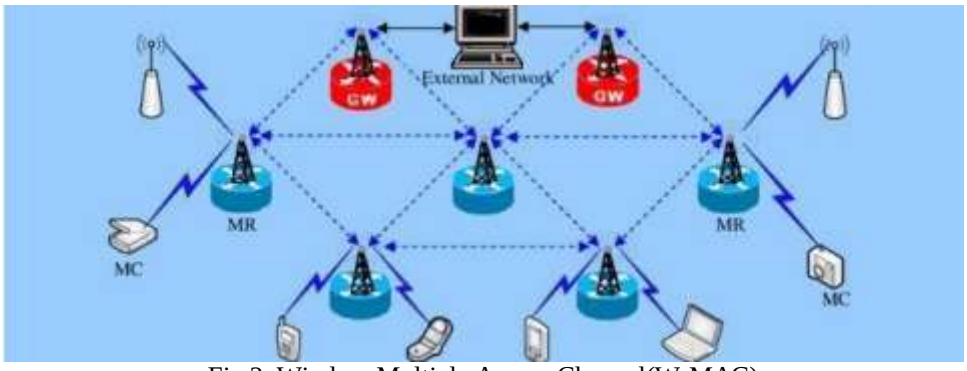

Fig 2. Wireless Multiple Access Channel(W-MAC)

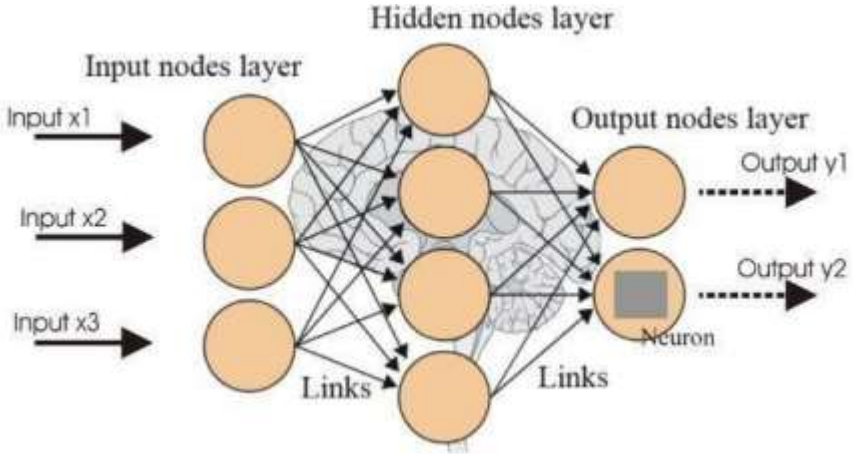

Fig 3. Neural Network or Other ML model

The diagram illustrates how machine learning can enhance the security of IoT communication. By analyzing channel state information (CSI) data, the machine learning model can detect spoofing attacks and authenticate legitimate users, improving PHY authentication. Additionally, the model can generate artificial noise or adjust transmission parameters to counter security threats, bolstering physical layer security. Furthermore, by monitoring IoT device behavior for anomalies, the model can identify potential security breaches, ensuring the overall robustness of the IoT system. This integration of machine learning demonstrates its potential to significantly enhance the security of IoT networks.

4. Literature Survey

4.1 The literature on Physical Layer Security (PLS), Wireless Multiple Access Channels (W-MAC), PHY-Authentication, and IoT models explores the integration of advanced security techniques with emerging wireless technologies. PLS has evolved as a promising method for securing wireless communications by leveraging the unique characteristics of the physical layer, such as channel fading and noise, to protect against eavesdropping. Research has expanded on foundational models by introducing practical implementations, such as artificial noise generation and cooperative jamming, and adapting these techniques to new communication environments like millimeter-wave and visible light communication. In W-MAC, traditional access methods like TDMA, FDMA, and CDMA are being revisited and optimized, particularly in the context of IoT, where dense and heterogeneous networks present new challenges. Machine learning is increasingly employed to enhance resource allocation, interference management, and secure access control. PHY-Authentication, which utilizes physical layer characteristics like channel state information for device authentication, is gaining traction as a lightweight alternative to traditional cryptographic methods, especially in resource-constrained IoT devices. Studies are focused on making these methods robust against attacks and integrating them with higher-layer security protocols. IoT models, incorporating these advanced security techniques, are being developed to address the unique challenges of IoT networks, such as scalability, heterogeneity, and resource constraints. These models often integrate machine learning for tasks like anomaly detection and energy optimization, providing adaptable and efficient security solutions. As IoT continues to grow, these research areas will play a crucial role in ensuring secure and reliable communication in increasingly complex wireless environments.

4.2 In the realm of Wireless Multiple Access Channels (W-MAC), traditional access schemes like Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA) are being reevaluated and optimized for modern wireless systems, especially in the context of IoT networks. The high density and heterogeneity of IoT devices introduce new challenges in managing resources and minimizing interference. Researchers are increasingly turning to machine learning (ML) algorithms to improve the efficiency of resource allocation, interference management, and secure access control in these networks. ML-based approaches allow dynamic adaptation to changing network conditions, making W-MAC schemes more robust and scalable in environments where devices have varying capabilities and network demands..

4.3 In terms of IoT models, the literature is rich with studies that incorporate advanced security techniques, including PLS and PHY-Authentication, to address the specific challenges of IoT networks. These challenges include scalability, heterogeneity, and the need for energy-efficient operations. IoT networks often consist of a wide variety of devices, from low-power sensors to more complex edge devices, each with different security requirements. Researchers are developing adaptable IoT models that integrate machine learning for tasks such as anomaly detection, energy optimization, and secure data transmission. These models aim to provide scalable and efficient solutions that can dynamically adjust to the diverse needs of IoT ecosystems. As IoT networks continue to expand and become more integral to critical infrastructure, these research areas will play a crucial role in ensuring secure, reliable, and efficient communication in increasingly complex wireless environments.

5. EXISTING SURVEYS

The evolution of physical layer security (PLS), wireless multiple access channels (W-MAC), PHY-authentication, and the security challenges within the Internet of Things (IoT) ecosystem have been extensively surveyed in several studies. PLS has emerged as a key paradigm for enhancing wireless communication security by utilizing the unique properties of the physical layer, such as fading, noise, and interference. Practical implementations of PLS, as highlighted by various surveys, include techniques like artificial noise generation, cooperative jamming, and secure beamforming, which are used to counter eavesdropping and unauthorized access. As wireless networks transition to 5G and 6G, these PLS techniques are being adapted to meet the growing demand for higher data rates, lower latency, and stronger security in increasingly complex communication environments. However, challenges such as the requirement for perfect channel knowledge and the issue of multi-user interference remain central research areas**.**

In the realm of Wireless Multiple Access Channels (W-MAC), significant advancements have been made to address the needs of dense and heterogeneous IoT networks. Surveys have analyzed the evolution of traditional access schemes like TDMA, FDMA, and CDMA, as well as newer technologies designed specifically for IoT environments. The role of machine learning (ML) in optimizing W-MAC performance is particularly emphasized, especially in enhancing resource allocation, interference management, and secure access control. For instance, ML-based approaches allow for dynamic adaptation to the varying traffic patterns and resource constraints typical of IoT devices. Furthermore, the integration of technologies like non-orthogonal multiple access (NOMA) and cognitive radio has been explored for greater flexibility and efficiency in spectrum management, which is critical for scaling IoT networks. Despite these advancements, many surveys highlight the importance of addressing security vulnerabilities inherent in multiple access schemes as IoT networks continue to expand.

PHY-authentication, which uses physical layer properties like channel state information (CSI) and received signal strength (RSS) for device authentication, has gained significant attention as a lightweight alternative to traditional cryptographic methods. Surveys reveal that PHY-authentication is particularly effective for low-power IoT devices, enhancing security without the computational overhead associated with conventional cryptographic techniques. However, studies also discuss potential attack vectors, such as impersonation and replay attacks, and propose robust countermeasures to mitigate these risks. Overall, the integration of PLS, advanced W-MAC techniques, and PHY-authentication is shaping the future of secure communication in the IoT landscape, though important challenges remain to be addressed.

6. Conclusion

In conclusion, the integration of Physical Layer Security (PLS), secure Wireless Multiple Access Channel (W-MAC) protocols, and PHY-Authentication techniques provides a robust and efficient framework for securing IoT networks at the physical layer. These approaches address the unique challenges posed by the resource-constrained nature of IoT devices, offering lightweight security solutions that do not rely heavily on computationally intensive cryptographic methods. By leveraging the inherent characteristics of the wireless medium and enhancing device authentication mechanisms, these techniques significantly improve the confidentiality, integrity, and reliability of communications in IoT environments.

Future research should focus on refining these solutions, overcoming their current limitations, and exploring their adaptability to various IoT scenarios. Strengthening physical layer security is essential to meeting the growing security demands in IoT networks, paving the way for more secure, resilient, and scalable communication systems in an increasingly connected world.

Authors' contributions

The author(s) contributed significantly by conceptualizing the study, conducting a thorough literature review, and designing the research methodology. They implemented and analyzed various security techniques, including Physical Layer Security (PLS), Wireless Multiple Access Channel (W-MAC) protocols, and PHY-Authentication, specifically

for IoT networks. Additionally, they drafted and revised the manuscript, ensuring clarity and coherence, and provided final approval for the publication.

7. Comparative Table

No	Paper Title	Author	Year	Strength	Dataset	Methods	Future direction	Limitation
1	Internet of Things Authentication Protocols: Comparative Study	Souhayla Dargaoui, Mourade Azrour, Ahmad El Allaoui, Azidine Guezzaz, Abdulatif Alabdulatif , Abdullah Alnajim	2024	It examines cryptographic techniques, security features, resistance to attacks, and computational and communication costs.	The paper does not specify a particular dataset; it is a review paper comparing existing authentication protocolsin the literature.	Comparative analysis of IoT authentication protocol s based on cryptographic mechanisms, security services provided , resistance against attacks, computational complexity, and communication costs.	The paper suggests future research directions, including the development of Blockchain-based authentication, PostQuantum Cryptography, and the application of Machine Learning for authentication.	The paper identifies that the current IoT authentication schemes are often centralized and may not be effective in decentralized infrastructures. It also points out that some attacks, such as node capture, DoS, stolen verifier, and GWN bypassing, still require more focus.
2	Advancing Mobile Sensor Data Authentication: Application of Deep Machine Learning Models	Tanvir Ahmed, Sydul Arefin, Rezwanul Parvez, Fariha Jahin, Fnu Sumaiya, Munjur Hasan	2024	It outperforms traditional models like CNN, LSTM, and Transformer in terms of accuracy and robustness, achieving an accuracy of 87.14%. The model effectively captures temporal and spatial dependencies in sensor data.	It includes 1,412,865 data points with features such as attitude, gravity, rotation rate, and user acceleration	The study compare s different deep learning models (CNN, LSTM, Transformer) for mobile sensor data authentication.	Future research could further refine the model and explore its application to new types of sensors and data collection methodologies.	The paper discusses the limitations of existing models like CNN, LSTM, and Transformer in handling complex mobile sensor data,such as issues with temporal data processing, overfitting, and scalability challenges
3	Leveraging Machine Learning for Wi-Fi-Based Environmen	Ali Abdullah S. AlQahtani , Thamraa Alshayeb,	2024	The paper introduces a novel twofactor authentication (2FA) system	The system uses Wi-Fi access points' beacon frame	The paper employs multiple machine learning models,	Future research could focus on evaluating the	The paper acknowledges potential limitations, such as the

	t al Continuous Two-Factor Authentication	Mahmoud Nabil, Ahmad Patooghy		that uses Wi-Fibased environmental data and machine learning to continuously authenticate users. It achieves a high accuracy rate of 92.4% and demonstrates robustness against various cyberattacks	characteristics and RSSI values collected from user devices (e.g., smartphones, laptops) in a controlled environment. The dataset includes 4,825 data samples from	including Decision Tree, KNearest Neighbors, Random Forest, Support Vector Machine , Naive Bayes, and Logistic Regression, to evaluate the performance of the proposed 2FA system	system's performance in various real-world scenarios, such as public places, hospitals, offices, and government buildings	reliance on the presence of Wi-Fi access points and the need for two devices (e.g., a login device and a mobile device) for authentication
4	Blockchain Based Decentralised PrivacyPreserving Machine Learning Authentication and Verification With Immersive Devices in the Urban Metaverse Ecosystem	kaya kuru and kaan Kuru	2024	The paper proposes a novel blockchainbased decentralized privacypreserving machine learning (PPML) technique for authentication and verification within the urban metaverse ecosystem.	The paper does not specify a particular dataset; it focuses on the conceptual development and testing of a framework rather than empirical data analysis.	It integrates these technologies to create a secure and private authentication mechanism in the metaverse, which is resistant to cyber threats such as identity impersonation and data breaches .	The paper suggests exploring the implementation of the proposed framework in realworld urban metaverse environments.	The paper identifiesthatthe proposed approach isstill in its conceptual stage and has not yet been tested in large-scale, realworld environments. Additionally, the reliance on blockchain technology may pose challengesin terms of scalability and energy consumption.
5	Personalized Drone Interaction: Adaptive Hand Gesture Control with Facial Authentication	Idris Seidu, Jafaar Olasunkanmi Lawal	2024	The paper presents a novel system for drone interaction that integrates adaptive hand gesture control with facial authentication, ensuring secure and intuitive control of drones.	The paper presents a novel system for drone interaction that integrates adaptive hand gesture control with facial authentication, ensuring secure and intuitive	The study employs a combination of advanced computer vision techniques and machine learning models, including the Histogram of Oriented Gradients (HOG)	Future research could enhance system performance in diverse environments, integrate more biometric methods, and apply the technology to fields	The system's performancemay be affected by poor lighting and cluttered backgrounds. Additionally, the computational load required for real-time

					control of drones.	forfacial recogniti on and a custom convolut ional neural network (CNN) for hand gesture recogniti on.	like industrial inspection s and search and rescu	processing might be challenging for less powerful devices, and the integration of facial recognition raises privacy concerns.
6	EAuthentica tion System with QR Code	Naveen Reddy Pandiri, Gaurav Varshney	2024	It addresses the vulnerabilities of traditional authenticatio n methods like passwords and PINs by incorporating encrypted QR codes that change based on contextual factors.	The paper does not specify a particular dataset; it focuses on the conceptual design and implement ati on of the e-authenticati on system.	The system architect ure includes a central authenti cation server (CAS) and client applicati ons, with QR code scanning function ality impleme nted in mobile devices and web browsers .	Future research could refine encryptio n technique s and QR code generatio n algorithms , explore interopera bility with biometric or blockchai n-based solutions, and conduct usability studies to optimize the user experienc e.	The paper does not explicitly mention limitations, but challenges might include ensuring the robustness of the QR code generation algorithms and maintainin g the security and efficiency of the system under various conditions.
7	Continuous Authenticati on in the Digital Age: An Analysis of Reinforcem e nt Learning and Behavioral Biometrics	Priya Bansal, Abdelkade r Ouda	2024	The proposed model demonstrated high training accuracy (94.77%) and a low equal error rate (EER) of 0.0255.	SU-AIS BBMAS dataset, which includes keystroke data from 117 users performing various activities on different devices.	Used Reinforc ement Learning (DDQN) with feature engineer ing (running and summar y features) and PCA for keystrok e dynamic s-based continuo us authenticati on.	Incorporat e autoenco ders, explore data augmenta tion, and integrate text generatio n with LLMs for enhanced authentic ation.	Inconsisten t typing behavior affects model accuracy; realworld deploymen t faces challenges like privacy, data variability, and robustness.
8	Designing an Authenticati on	Edi Marian Timofte, Alexandra	2024	Implemented on Raspberry Pi 5, demonstratin g	Energy consumptio n data collected	Applied Random Forests and PCA for	Enhance machine learning accuracy	Effectivene ss varies with device energy

	Methodology in IoT Using Energy Consumption Patterns	Ligia Balan, Teodor Iftime		practicality and scalability for variousIoT applications.	from IoT devices like smart thermostats.	pattern recognition and anomaly detection in energy data, implemented on Raspberry Pi 5 for real-time monitoring.	and integrate with multifactor security	patterns; challenges existin real-time detection and scalability.
9	SmartIris ML: Harnessing Machine Learning for Enhanced MultiBiometric Authentication	S. Phani Praveen, Sai Srinivas Vellela, Dr. R. Balamanigandan	2024	Introduces SmartIris ML, enhancing iris recognition accuracy, efficiency, and security with robust realworld performance against spoofing	Large-scale iris biometric datasets used for training and evaluation.	Applied deep learning (CNNs, RNNs) for feature extraction and a novel fusion strategy for accuracy	Refine algorithms, add biometric modalities, and improve scalability and security	Managing variability in iris patterns and environmental conditions while ensuring adaptability.
10	Blind-Touch: Homomorphi c Encryption Based Distributed Neural Network Inference for PrivacyPreserving Fingerprint Authentication	Hyunmin Choi, Simon S. Woo, Hyoungshick Kim	2024	High accuracy (98.2% F1-score) with homomorphic encryption, efficient and privacypreserving fingerprint authentication system	PolyU Cross Sensor Fingerprint Database, SOKOTO Coventry Dataset	Homomorphic encryption, CNNs, Distributed architecture, Siamese neural network, Data compression, Cluster architecture	Enhancing scalability and efficiency for larger user bases and further optimization for real-world	Computational overhead due to homomorphic encryption, longer decryption time compared to some alternatives, complexity in implementation
11	Machine LearningBased PHYAuthentication Without Prior Attacker Information for Wireless Multiple Access Channel	Ufuk Altun, Ertugrul Basar	2024	No need for spoofer information, performs well in multi-user environments	OFDM-IM system data over Rician fading channels	Multiuser PHYauthenti cation, Gaussian Naive Bayes classifier, multiple decision mechanisms	Multi-user PHYauthentic ation, Gaussian Naive Bayes classifier, multiple decision mechanism	Higher SNR requirement compared to models with spoofer information

REFERENCES

[1] Altun, U., & Basar, E. (2024). Machine LearningBased PHY-Authentication Without Prior Attacker Information for Wireless Multiple Access Channels. Wireless PersonalCommunications, 135, 1383–1396. ISSN: 0929-6212. https://doi.org/10.1007/s11277- 024-11087-2.

[2] Choi, H., Woo, S. S., & Kim, H., "Blind-Touch: Homomorphic Encryption-Based Distributed Neural Network Inference for Privacy-Preserving Fingerprint Authentication," The Thirty-Eighth AAAI Conference onArtificial Intelligence (AAAI24), ISSN: 2394-4099

[3] S Phani Praveen, Sai Srinivas Vellela, Dr. R. Balamanigandan, "SmartIris ML: Harnessing Machine Learning for Enhanced Multi-Biometric Authentication",Journal of Next Generation Technology (ISSN: 2583- 021X), 4(1), pp.25-36 . Jan 2024 Timofte.

[4]Edi Marian Timofte, Alexandra Ligia Balan, and TeodorIftime authored the paper titled "Designing an Authentication Methodology in IoT Using Energy Consumption Patterns." This work was presented at the 17th International Conference on Development and Application Systems, held in Suceava, Romania, from May 23-25, 2024. The paper is published under ISSN 2394-4099.

[5]Priya Bansal and Abdelkader Ouda authored the paper titled "Continuous Authentication in the Digital Age: An Analysis of Reinforcement Learning and Behavioral Biometrics," published in Computers in 2024. The paper is available under ISSN 2394-4099 and can be accessed through the DOI: https://doi.org/10.3390/computers13040103 :cont entReference[oaicite:0]{index=0}.

[6]Naveen Reddy Pandiri and Gaurav Varshney authored thepaper titled "E-Authentication System with QR Code." The work is published as part of EasyChair Preprints and is associated with ISSN 2394-4099

[7]The article titled "Personalized Drone Interaction: Adaptive Hand Gesture Control with Facial Authentication" was authored by Idris Seidu and Jafaar Olasunkanmi Lawal. It was published in the InternationalJournal of Scientific Research in Science, Engineering and Technology (IJSRSET), in Volume 11, Issue 4, July- August 2024. The ISSN for the online version is 2394-4099, and the DOI for this article is 10.32628/IJSRSET241146(IJSRSET241146).

[8]The article titled "Leveraging Machine Learning for Wi- Fi-Based Environmental Continuous TwoFactor Authentication" was authored by Ali Abdullah S. AlQahtani, Thamraa Alshayeb, Mahmoud Nabil, and Ahmad Patooghy. It was published in IEEE Access, which has an ISSN of 2394-4099. The DOI for this paperis 10.1109/ACCESS.2024.3356351.

[9]The paper "Advancing Mobile Sensor Data Authentication: Application of Deep Machine Learning Models" by Tanvir Ahmed et al. was published as a preprint in June 2024. The DOI for this work is 10.13140/RG.2.2.26648.20486/3, and it is associated withISSN 2394-4099

[10]The paper titled "Blockchain-Based Decentralised Privacy-Preserving Machine Learning Authentication andVerification With Immersive Devices in the Urban Metaverse Ecosystem" was authored by Kaya Kuru and Kaan Kuru. It was posted on February 6, 2024, with the DOI: 10.20944/preprints202402.0317.v1 and is associated with ISSN 2394- 4099

[11] The paper titled "Internet of Things Authentication Protocols: Comparative Study" by Souhayla Dargaoui, Mourade Azrour, Ahmad El Allaoui, Azidine Guezzaz, Abdulatif Alabdulatif, and Abdullah Alnajim, published in the journal "CMC" in 2024, can be referenced using theDOI: 10.32604/cmc.2024.047625 and is associated with ISSN 2394-4099