JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 07 Issue 02
2024
Research Article
https://doi.org/10.56979/702/2024

A Review Paper on AI-Based User Privacy & Security Concerns in Smart Wearable IOT Devices

Muhammad Faheem Younas[1*], Muhammad Muzammal Farooq[1], Gohar Mumtaz[1], and Zeeshan Mubeen[2]

[1]Faculty of Computer Science and Information Technology, Superior University, Lahore, 54000, Pakistan.
[2]Riphah International University, Lahore, 54000, Pakistan.
[*]Corresponding Author: Muhammad Faheem Younas. Email: mrfaheemrajpoot@gmail.com

Received: June 08, 2024 **Accepted:** August 19, 2024 **Published:** September 01, 2024

Abstract: Smart technologies including wearables have emerged as the bridge between artificial intelligence (AI) and the internet of things (IoT). On the one hand, it has changed the way people regarding efficiency and utility provision. On the other hand, the very fact relationships become deep and interconnected as they are, raised great issues of privacy and security concerns that are now in need of seeking reliable solutions from both scholars and practitioners. The current review focuses on the state of the art of privacy and security issues as an effect of AI in smart wearable IoT devices, the existing, and further, advanced AI technologies that are still undeveloped for the purpose. The results were aggregated through ten studies wherein each posed relatable problems and solutions regarding smart wearable IoT devices security. A comprehensive table with challenges, solutions, AI methods, datasets, and limitations of the studies is also provided.

Keywords: Smart Wearables IOT Devices; IOT Security and Privacy; AI Security, IOT Data Protection; Wearable Tech Security; IOT Security Devices.

1. Introduction

While the idiot-box is largely passive in nature, it is clear that the Internet of Things is growing exponentially. With expected subscription claims of above 35 billion by the end of 2023 to be related to the IOTs and so, time will see an increase of the number of internet connected devices all over the world. Most offices, and homes quite literally have transformed the way people use technology, especially with the latest developments in smart wearable gadgets. These smart devices from simple fitness bands to sophisticated medical devices obtain great deals of sensitive information putting the users into risks of privacy invasion and data breaches.

As quoted by one of the experts in the field, 'When you are in the information age, information has become one's asset and the information has to be secured since more and more heterogeneous data are being and will be realized out of the IOT devices.' Adding AI into this ecosystem complicates the situation further in that AI models are trained on this data and applied to the ecosystem. That poses a challenge, while AI brings additional usefulness to the body of smart devices, the collection and application of smart device data through AI, gives rise to new problems of privacy.

Thus, this particular strategy will give a determination on how issues concerning privacy and security surrounding the artificially intelligent smart wearable IoT gadgets will be addressed. Special attention will also be given to defending the population's personal data, through an overview of existing literature. This review will present the current state of research on the screen of domestic violence and propose a few new directions for investigations.

2. Security and Privacy Challenges in IOT

The involvement of IoT in conjunction with Artificial Intelligence (AI) raises several issues, especially in relation to security and privacy, which are made worse by the diverse structures of IoT systems and the varying operational environments of these devices. The most concerning among these include:

Data Breach: This concerns the wrongful invasion of privacy using IoT technologies through data breaches; the growing number of IoT gadgets amplifies the number of attack surfaces unprotected. Given that many IoT devices are used in the medical field, there is a lot of sensitive information that if unauthorized will create a big privacy concern.

Lack of Security in the Connections: Data sent over the network between IoT units and cloud networked devices is transmitted without much regard to encryption. This is dangerous particularly with smart wearable devices that generate and send data over a network throughout its use.

Absence of Regulations: As no universal requirements have been applied, where the Internet of Things is concerned, different procedures have been brought about to all security measures, therefore further making it complicated in securing all the devices and systems.

Insider Threats: Breaches of data by employees, either willfully or inadvertently, is still a very significant threat to the safety of an organization. There are intelligent systems that minimize the likelihood of these occurrences by monitoring the behavior and access patterns of the end-users but their efficacy cannot be guaranteed.

Data Siloing and Integration Issues: IoT devices produce a lot of data, which in turn is housed in a number of standalone silos. It makes it fairly difficult to assimilate and assess all the data collected. Such asset fragmentation may be an impediment in creating an adequate security strategy that requires an understanding, and integration, of data movements.

3. Literature Review of Existing Studies

The following table summarizes ten studies that investigated different sides of the AI-powered privacy and security concerns of a smart wearable IoT device:

Table 1. Literature Review

Sr No	Challenges	Solutions/Results	AI Approaches	Datasets	Limitations
1	Unauthorized data access in IoT environments	There has been the development of AI-based anomaly detection systems which have been shown to monitor and detect the abnormal data access patterns hence blocking unauthorized access into the IoT systems.	Such data including past access logs and present access logs are processed using tried and tested machine learning models usually supervised in a bid to get insights regarding ongoing security issues.	Anonymized user behavior data from large-scale IoT deployments, primarily in healthcare environments.	High computational costs and potential delays in real-time detection due to the complexity of models.
2	Insecure Communication Channels	A top-down adoption of end-to-end encryption protocols has remained a key measure aimed at protecting the data being exchanged between the IoT devices and the cloud servers.	For such services, lenses such as Advanced Encryption Standard (AES) and RSA algorithm are incorporated during data transfer for depth protection of the data.	Synthetic datasets simulating IoT communication traffic under various network conditions.	Encryption involves additional latency and large amounts of processing power which may not be available in devices with resource-constraints.
3	Absence of commonly	There are ongoing initiatives for the			

	accepted security policy	development of acceptable security policies for those who would be utilizing the IoT because of the importance of having the same level of security.	Using emerging IoT security regulations, software agents based on policy modeling are being created and incorporated into IoT infrastructure.	Compliance with the Industry requirements for progress and existing active standards among policy datasets.	Playground: Several highly dissimilar types of IoT & Device manufacturers who have little to nothing in common, slow reaching out to the larger world, thus a diffusive approach to security measures.
4	Insider Threats and Privilege Misuse	There are AI-based systems that have been developed to track user behavior, and user access rights aimed at detecting and eliminating potential insider threats.	AI-powered behavioral analysis tools utilize unsupervised learning to detect deviations from normal access patterns, indicating possible misuse.	Access logs from healthcare systems, which are rich in metadata about user actions and access times.	Potential biases in AI decision-making can lead to false positives, undermining trust in the system.
5	Data Siloing and Integration Challenges	AI-driven strategies focus on breaking down data silos by enabling seamless data integration across various IoT platforms through federated learning techniques.	Federated Learning approaches allow for data processing and analysis across distributed IoT nodes without requiring data centralization.	Multisource IoT datasets collected from a variety of smart devices in healthcare, smart homes, and industrial IoT.	Communicatio n overhead and potential inconsistencies in data due to asynchronous updates across nodes.
6	Inadequate Data Anonymizati on Techniques	Advanced anonymization techniques are being developed to ensure that personal data remains protected while still being useful for AI analysis.	Differential Privacy techniques are increasingly used to add noise to data, preserving individual privacy while enabling aggregate data analysis.	Medical IoT data, which includes sensitive information such as patient records and real-time monitoring data.	Trade-offs between data utility and privacy, particularly in ensuring that anonymization does not degrade data quality excessively.

7	Dynamic Nature of IoT Environments	In order to counter the continuously evolving or rather unpredictable nature of IOT, new privacy-preserving methods are being researched and designed.	Continuous Learning AI models which adapt to new threats without constant updates of the systems to the manual input.	Real-time IoT data streams from a variety of sources, including smart homes, vehicles, and industrial systems.	Maintaining consistent privacy measures in environments where the IoT landscape changes rapidly and unpredictably.
8	Resource Constraints on IoT Devices	Optimization of AI algorithms is critical for enabling efficient operation on resource-constrained IoT devices, such as smart wearables.	Lightweight AI models, designed to function with minimal computational resources while still delivering accurate predictions.	Resource-constrained device data, including energy consumption logs and processing capacity metrics.	The need to balance model complexity and accuracy, which can be difficult to achieve on devices with limited computational power.
9	Privacy-Preserving AI Integration in IoT	AI systems are being aligned with global privacy regulations and standards to ensure that IoT deployments do not infringe on user rights.	To address the concerns posed by the user, Interpretability By Design (XAI) concepts are emerging that demonstrate how this process reaches its conclusions.	Additional materials help to better understand the regulation of compliance since they give datasets related to regulatory compliance and these include the guidance Mozilla Corporation594 states it is developing upon the GPDR, HIPAA etc.	There is frequent change in privacy requirements which means that companies have difficulties in maintaining AI systems compliant with the set regulations at all times.
10	Data Collection by Smart Wearables without Consent	User-oriented methods are being developed that permit users greater control over information gathered	Decentralized Identity Systems (DID) in which the user retains their identity and data and is therefore	Self-generated and operational data, such as biometric and motion activity	Difficulty in adoption, since users' are busy people and cannot be expected to

	from their wearable gadgets.	free from the control of centralized entities.	information from wearable gadgets.	adopt new systems with such drastic behavior modification requirements.

4. Results

The results show that there are still major obstacles to overcome even though AI technology offers creative ways to improve security and privacy in smart wearable IoT devices. Even with current enhanced anomaly detection and encryption solutions, major hazards still come from unauthorized data access and unsecured communication connections. Sophisticated AI models are difficult to execute due to resource constraints of IoT devices, and seamless integration is hampered by the fragmented nature of data storage. Moreover, the adoption of decentralized identity systems is sluggish since they necessitate significant behavioral changes from users, despite their promise of improved user control over data. All things considered, the difficulty is striking a balance between strong security and the real-world limitations of device capabilities and user compliance.

5. Conclusion

While the global demand for AI-based Internet of Things' smart gadgets increased notably especially in the aspect of smart wearables, various privacy and security issues arose. To tackle such difficulties, there is a need for an integrated approach that utilizes the technologies of artificial intelligence for security, the unification of the expert-enforcement measures, and the levers of vigilance. The study suggests that more efforts need to be directed toward creating advanced AI based solutions that can be tailored to the ever evolving IoT landscapes. In addition, there is an urgent need for international requirements that will assist in implementing the measures of protecting privacy and security within the various IoT systems.

Along these lines, future developments should aim at designing more advanced networks and the corresponding artificial intelligence, which will not only increase security but also give the users confidence and trust which is essential if the advantages of smart wearable Internet of Things devices are to be realized without compromising the privacy constraints.

References

1. Braga, R., Mota, E., & Passito, A. (2010). Lightweight DDoS flooding attack detection using NOX/OpenFlow. In Proceedings of the IEEE 35th Conference on Local Computer Networks (LCN) (pp. 408-415). IEEE.
2. Cao, Y., Chen, S., Hou, P., & Brown, D. (2015). FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation. In Proceedings of the IEEE International Conference on Networking, Architecture and Storage (NAS) (pp. 2-11). IEEE.
3. Li, J., Ma, Q., Chan, A., & Man, S. S. (2019). Health monitoring through wearable technologies for older adults: Smart wearables acceptance model. Applied Ergonomics, 75, 162-169. https://doi.org/10.1016/j.apergo.2018.10.006
4. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52, 452-459.
5. Nagra, A. A., Khan, A. H., Abubakar, M., Faheem, M., Rasool, A., Masood, K., & Hussain, M. (2024). A gene selection algorithm for microarray cancer classification using an improved particle swarm optimization. Scientific Reports, 14(1), 19613.
6. Sodhro, A. H., Pirbhulal, S., & de Albuquerque, V. H. C. (2019). Artificial intelligence-driven mechanism for edge computing-based industrial applications. IEEE Transactions on Industrial Informatics, 15(7), 4235-4243.
7. Wang, M., Zhu, T., Zhang, T., Yu, S., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks, 6(3), 281-291.
8. Firouzi, F., Farahani, B., & Daneshmand, M. (2020). AI-driven data monetization: The other face of data in IoT-based smart and connected health. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2020.3027971
9. Majumder, S., Aghayi, E., Noferesti, M., Memarzadeh-Tehran, H., Mondal, T., Pang, Z., & Deen, M. J. (2017). Smart homes for elderly healthcare—recent advances and research challenges. Sensors, 17(11), 2496.
10. Choi, D. H., & Shon, D. (2019). Future changes to smart home based on AAL healthcare service. Journal of Asian Architecture and Building Engineering, 18(3), 190-199.
11. Siraj, M. A., Rehman, A., Aziz, O., & Khan, M. F. (2021). Systematic Literature Review: Smart Drone for Early Smoke Detection in Forest Using IOT. Journal of Computing & Biomedical Informatics, 2(01), 80-88.
12. Garbuio, M., & Lin, N. (2019). Artificial intelligence as a growth engine for health care startups: Emerging business models. California Management Review, 61(2), 59-83.
13. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science & Engineering, 46(2).