International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Review Paper on Machine Learning-Based Privacy Analysis in IoT Healthcare Systems

Mr. Ismail Almsallat[1], Dr. Hari Mohan Singh[2]

[1]Academic, Computer Science &IT, SHUATS, SHUATS
[2]Assistant Professor, Computer Science &IT, SHUATS, SHUATS

Abstract
The accelerated advancement of Internet of Things (IoT) technologies has led to the widespread deployment of interconnected medical devices capable of continuous physiological data acquisition, real-time monitoring, and intelligent clinical decision support. While these systems enhance diagnostic accuracy and healthcare delivery efficiency, they also expose sensitive medical data to significant security and privacy risks. This review systematically examines research published between 2016 and 2024, focusing on the application of machine learning (ML) techniques to improve the functionality, reliability, and security of IoT-based healthcare systems. The study critically analyzes state-of-the-art privacy-preserving mechanisms, secure data transmission protocols, access control models, and ML-driven anomaly detection and intrusion prevention methods for protecting patient data. Furthermore, it investigates the synergistic integration of IoT and ML architectures in healthcare environments, identifies emerging technical challenges and trends, and outlines future research directions aimed at developing robust, scalable, and privacy-aware intelligent healthcare systems.

Keywords: Internet of Things (IoT), Healthcare, Data Privacy, Machine Learning (ML), Artificial Intelligence (AI)

1. Introduction

The continuous advancement of digital technologies has profoundly influenced the healthcare sector, driving researchers and practitioners to seek innovative ways to manage health information and improve patient outcomes. Among the most transformative developments is the emergence of the **Internet of Things (IoT)** in healthcare, which integrates interconnected devices, sensors, and data analytics into medical systems. This integration enables real-time health monitoring, automated diagnosis, and data-driven decision-making, revolutionizing the delivery of healthcare services.

IoT-based healthcare systems have redefined patient care by offering **remote monitoring, early disease detection, and personalized treatment plans.** Through continuous data collection and intelligent analysis, these systems enhance the quality of care while simultaneously reducing costs and improving accessibility. For example, wearable sensors and implantable devices can track vital signs such as heart rate, blood pressure, glucose levels, and body temperature, transmitting this information to healthcare professionals for timely intervention. Such capabilities not only improve medical accuracy but also empower patients to take a proactive role in managing their health.

However, as the healthcare sector becomes increasingly digitized, **security and privacy challenges** have become more pressing. Medical data—often containing highly sensitive personal information—represents

a valuable target for cybercriminals. Unauthorized access or breaches can result in financial losses, reputational damage, and legal consequences for healthcare organizations. Studies indicate that healthcare accounted for nearly **10% of global data breaches in 2020**, with more than 25 million patient records compromised. Consequently, ensuring robust data protection is a fundamental requirement for any IoT-based healthcare framework.

To address these challenges, the integration of **machine learning (ML)** and **artificial intelligence (AI)** within IoT systems has emerged as a promising approach. Smart healthcare technologies equipped with ML algorithms can analyze large volumes of medical data, detect anomalies, and predict potential health risks while maintaining privacy safeguards. For instance, EEG-based authentication systems have been developed to enhance data security in IoT-enabled healthcare environments by providing personalized, biometric-driven access control.

Additionally, the increasing adoption of **consumer-grade health monitoring devices**, such as smartwatches and fitness trackers, has expanded the scope of IoT healthcare beyond hospitals and clinics. These devices allow individuals to monitor their daily activities and vital statistics, supporting long-term health management. Nevertheless, this growing network of connected devices also broadens the attack surface for cyber threats, making **data privacy and cybersecurity** crucial priorities in the modern healthcare ecosystem.

2. Privacy Challenges in IoT-Based Healthcare Systems

While IoT-based healthcare systems bring enormous benefits—such as real-time health monitoring, predictive diagnosis, and improved treatment precision—they also raise significant **privacy and data protection concerns**. These challenges arise from the vast amount of sensitive information continuously generated, transmitted, and analyzed by interconnected medical devices and sensors. The very features that make IoT healthcare systems powerful—constant connectivity and data exchange—also expose them to various privacy risks.

One of the primary concerns involves the **collection and use of personal health information**. IoT devices such as wearable trackers, implantable sensors, and remote monitoring systems record diverse data, including personal identifiers, medical conditions, and even geolocation. For instance, a fitness tracker that monitors heart rate, physical activity, and sleep quality can inadvertently reveal a user's underlying health issues or lifestyle patterns. When such information is transmitted across different networks and platforms, the risk of unauthorized access or data leakage increases substantially.

Furthermore, many IoT devices rely on **wireless communication channels** that may not be adequately secured. Transmitting medical data over unsecured Wi-Fi or Bluetooth connections exposes sensitive information to interception by cyber attackers. For example, a wireless glucose monitoring device that communicates with a healthcare provider through an unencrypted network can become a potential entry point for malicious actors seeking to steal or manipulate patient data.

Another layer of concern arises from the **lack of standardized privacy regulations** and inconsistent implementation of security measures across devices and service providers. Since healthcare IoT ecosystems often involve multiple stakeholders—patients, hospitals, cloud providers, and device manufacturers—ensuring uniform data protection practices is highly complex. Each entity may follow different security protocols, creating vulnerabilities at the integration points of the system.

To mitigate these challenges, healthcare organizations must adopt a comprehensive **data privacy framework** that combines both technological and organizational measures. Key strategies include:

- **Data Encryption:** Encrypting sensitive data both during transmission and storage ensures that intercepted information remains unreadable to unauthorized users.
- **Access Control:** Implementing role-based or biometric access mechanisms prevents unauthorized personnel from viewing or modifying patient data.
- **Consent Management Systems:** Allowing patients to specify how their data is collected, used, and shared enhances transparency and strengthens trust in IoT healthcare platforms.
- **Secure Communication Protocols:** Using technologies such as HTTPS, TLS, or blockchain-based systems can protect the integrity and confidentiality of data exchanges.

Ultimately, addressing privacy challenges in IoT-based healthcare requires a **multilayered security approach**, where privacy protection is embedded into every stage—from device design and data transmission to cloud storage and user interaction. Achieving this balance between technological innovation and ethical responsibility is vital to sustaining patient trust and enabling the full potential of IoT-driven healthcare systems.

3. Machine Learning Tasks in Cybersecurity

Machine Learning (ML), a crucial branch of Artificial Intelligence (AI), plays a transformative role in modern cybersecurity. Its ability to learn from data, recognize hidden patterns, and make intelligent predictions enables the detection and prevention of cyber threats more efficiently than traditional rule-based methods. In the context of IoT-based healthcare systems—where vast and sensitive data are exchanged in real time—ML offers automated and adaptive solutions to detect intrusions, predict attacks, and mitigate potential breaches before they occur.

Machine learning encompasses various techniques, including **data mining**, **computational statistics**, and **predictive analytics**, all of which are central to building intelligent cybersecurity models. Broadly, ML approaches can be categorized into three major types: **supervised learning**, **unsupervised learning**, and **deep learning**. Each has unique applications and advantages in securing IoT healthcare networks.

3.1 Supervised Learning

Supervised learning involves training models using labeled datasets, where the algorithm learns to associate input data with known outcomes. Once trained, the model can classify or predict unseen data based on learned patterns. In cybersecurity, supervised learning is widely applied to **intrusion detection**, **malware classification**, and **attack identification**.

For instance, classification algorithms can distinguish between normal and malicious network activity, identifying attacks such as **Denial-of-Service (DoS)** or **phishing** attempts. Common algorithms employed for these tasks include **Naive Bayes**, **Decision Trees**, **Support Vector Machines (SVM)**, **Logistic Regression**, and **Adaptive Boosting (AdaBoost)**. Each of these techniques has demonstrated strong performance in detecting abnormal behavior in large-scale IoT networks.

Regression-based methods are used for predictive analytics, such as forecasting the number of future cyber incidents or estimating network traffic fluctuations. While **classification** predicts categorical outcomes (e.g., whether an activity is malicious), **regression** predicts continuous values, helping cybersecurity professionals anticipate evolving threat patterns.

To enhance accuracy, **ensemble learning methods**—which combine multiple models to improve predictive reliability—are frequently adopted. For example, the **Random Forest** algorithm

3.2 Unsupervised Learning

Unsupervised learning operates without labeled data, focusing on discovering hidden structures and rela-

tionships within datasets. This approach is particularly useful for detecting **anomalies** or **zero-day attacks**—threats that have no prior signature and therefore cannot be identified by traditional methods.

Clustering algorithms, a subset of unsupervised learning, group data points based on similarity measures to uncover patterns of normal and abnormal behavior. Techniques such as **Partitioning Clustering**, **Hierarchical Clustering** (e.g., single-linkage and complete-linkage methods), and **Bottom-Up Clustering** are often employed in **Intrusion Detection Systems (IDS)** to distinguish between legitimate and suspicious network activities.

By automatically identifying deviations from normal behavior, unsupervised models enhance the adaptability and resilience of IoT healthcare systems. They are especially effective in environments where new types of attacks frequently emerge, ensuring that anomaly detection remains proactive rather than reactive.

4. IoT Healthcare Systems

The integration of the **Internet of Things (IoT)** into healthcare has redefined how medical services are delivered, monitored, and managed. By connecting smart devices, sensors, and data analytics platforms, IoT healthcare systems enable continuous patient monitoring, rapid diagnosis, and personalized treatment plans. This transformation has significantly improved clinical efficiency, reduced operational costs, and enhanced patient outcomes across multiple medical domains.

IoT applications in healthcare facilitate **real-time communication** between patients, healthcare providers, and medical infrastructure. For instance, wearable devices and implantable sensors can track vital health indicators such as heart rate, blood glucose levels, and blood pressure, transmitting this information to healthcare professionals for immediate evaluation. This continuous data flow allows for **early disease detection**, **remote patient management**, and **timely intervention**, reducing hospital readmissions and improving overall healthcare accessibility.

Moreover, IoT healthcare systems enable **data-driven decision-making** through the integration of advanced analytics and machine learning. Physicians can make informed clinical judgments based on real-time data insights, while predictive algorithms help anticipate potential health complications before they escalate. For chronic disease management—such as diabetes, cardiovascular disorders, and respiratory illnesses—IoT devices play a crucial role in maintaining continuous observation and ensuring patient adherence to treatment plans.

From an operational standpoint, IoT enhances the efficiency of healthcare systems by **automating administrative and monitoring tasks**. Smart hospital environments can track equipment usage, monitor patient movement, and manage energy consumption, leading to more efficient resource allocation. Additionally, integrating IoT with **electronic health records (EHRs)** ensures seamless data synchronization across departments, reducing manual errors and improving coordination among medical teams.

However, despite these advancements, several challenges persist—most notably **data privacy, interoperability, and regulatory compliance**. The vast interconnection of devices increases the potential for security breaches, while inconsistent data standards across manufacturers complicate integration efforts. Furthermore, strict regulations such as the **Health Insurance Portability and Accountability Act (HIPAA)** and the **General Data Protection Regulation (GDPR)** impose stringent requirements on how patient data must be collected, stored, and shared.

To fully harness the potential of IoT in healthcare, stakeholders must strike a balance between **innovation and security**. Developing unified standards, implementing strong encryption protocols, and adopting privacy-preserving data analytics are essential to building reliable and secure IoT healthcare systems. With these measures in place, IoT will continue to transform healthcare into a more **proactive, personalized, and intelligent ecosystem**.

5. Security in IoT

Security remains one of the most critical and challenging aspects of the **Internet of Things (IoT)** ecosystem. Due to the interconnected nature of IoT devices, hackers or malicious entities can easily exploit vulnerabilities within the network, leading to unauthorized data access, manipulation, or system disruption. In the healthcare sector, where IoT devices handle highly sensitive medical information, ensuring data confidentiality and integrity is of paramount importance.

Given these risks, researchers and developers have proposed several **security mechanisms** to protect IoT infrastructures from cyber threats. One notable contribution is the **IoT-oriented Data Placement (IDP) method** with privacy preservation, which focuses on optimizing data access time, improving resource utilization, and reducing energy consumption—all while ensuring strict data privacy. This approach employs the **Non-dominated Sorting Genetic Algorithm II (NSGA-II)** to achieve privacy preservation and energy efficiency through multi-objective optimization. By processing trusted computations locally on the user's health profile, the method minimizes the exposure of sensitive information and enhances system performance.

Another innovative approach is the integration of **Radio-Frequency Identification (RFID) encryption techniques**, which protect medical data transmitted across IoT networks. RFID-based security ensures that patient information shared between devices and healthcare servers remains encrypted and inaccessible to unauthorized users. Similarly, **cloud-based recommender systems** can incorporate trusted computation protocols to provide secure and personalized health recommendations without compromising user privacy.

The increasing reliance on cloud and edge computing within IoT frameworks further underscores the need for **robust encryption, authentication, and access control mechanisms**. By adopting decentralized and privacy-preserving computing models, healthcare providers can significantly reduce the risk of data breaches and cyberattacks. These systems rely on cryptographic methods and secure key management to prevent data tampering and ensure secure communication between devices.

In summary, maintaining strong security in IoT healthcare environments requires a **multi-layered defense strategy**. This includes secure data placement algorithms, energy-efficient cryptographic solutions, and advanced authentication protocols. Continuous monitoring and regular updates of IoT firmware are also essential to mitigate vulnerabilities and protect against evolving cyber threats. Ultimately, security in IoT is not a one-time implementation but an **ongoing process**—one that must evolve alongside technological advancements and emerging risks.

6. Security, Privacy, and System Requirements for IoT–Cloud Health Systems

The integration of **cloud computing** with the **Internet of Things (IoT)** has given rise to powerful e-health systems that can manage, process, and analyze large volumes of medical data. However, this interconnected ecosystem also introduces complex **security and privacy challenges**. Safeguarding patient information within cloud-enabled IoT healthcare networks requires robust security frameworks grounded in classical security principles such as **Confidentiality, Integrity, and Availability (CIA)**, along with advanced mechanisms like **access control**, **authentication**, and **data anonymization**.

Based on a comprehensive review of recent studies, the key security requirements for IoT–cloud healthcare systems can be summarized as follows:

- **Confidentiality:** Confidentiality ensures that sensitive information exchanged between senders and receivers remains inaccessible to unauthorized parties. In IoT–cloud healthcare systems, confidentiality must be maintained throughout the entire communication chain—from wearable devices and local gateways to cloud-based platforms. Encryption protocols, such as TLS and AES, are commonly used to secure data during transmission and storage, protecting patient records from eavesdropping and interception.
- **Data Integrity:** Data integrity guarantees that the information transmitted between devices and servers remains accurate, consistent, and free from unauthorized alteration. In IoT–cloud environments, integrity checks should be conducted at every communication node to detect tampering or manipulation attempts. Techniques such as digital signatures and blockchain-based verification enhance the trustworthiness of shared health data.
- **Availability:** Availability ensures that healthcare services and data remain continuously accessible to authorized users, even under malicious attacks or system failures. Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks pose major threats to IoT–cloud systems. To maintain service continuity, redundancy, load balancing, and intrusion prevention systems are critical components of a secure infrastructure.
- **Access Control:** Access control mechanisms define who can view, modify, or share medical data within the network. Role-based and attribute-based access control (RBAC/ABAC) models are frequently implemented to regulate access privileges, ensuring that only verified users—such as doctors, patients, and administrators—can interact with sensitive data. Effective access control minimizes the risk of internal misuse and unauthorized exposure.
- **Anonymization:** Data anonymization is a vital privacy-preserving technique that removes or masks personally identifiable information (PII) from medical datasets. By using anonymous authentication protocols, healthcare systems can share and analyze medical data without revealing patient identities, thus upholding ethical and legal data protection standards.
- **Authentication:** Authentication validates user and device identities to ensure that only legitimate entities can access healthcare networks. Multi-factor authentication (MFA), biometric verification, and cryptographic keys are widely used to enhance the reliability of authentication processes.
- **Resistance to Attacks:** IoT–cloud systems must be resilient against a wide range of cyberattacks, including spoofing, phishing, malware injection, and man-in-the-middle (MitM) attacks. Employing intrusion detection systems (IDS), anomaly detection algorithms, and federated security architectures can strengthen resistance to such threats.

The following table summarizes the major **security requirements** and their corresponding functions, as discussed in the reviewed literature.

Table 1. Security Requirements for IoT–Cloud Health Systems

Security Function	Description	References
Access Control	Restricts or limits user access to sensitive data.	[3,6,9,13,18,25]
Anonymization	Preserves user privacy through anonymous authentication.	[2,8,9,14]
Authenticity	Verifies and validates user credentials.	[5,12–15,17,23]

Security Function	Description	References
Confidentiality	Prevents unauthorized access to private data.	[2,3,15,24]
Data Integrity	Ensures that transmitted data remains unaltered.	[3,24]
Resistance to Attacks	Prevents or mitigates malicious intrusions.	[7,14]

7. Review of Recent Related Studies

The concept of **smart healthcare systems** represents the convergence of advanced technologies—such as the Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), and data analytics—to create an intelligent, interconnected medical ecosystem. These systems aim to enhance patient care, optimize hospital operations, and improve the overall efficiency and quality of healthcare services. Through real-time monitoring, predictive analytics, and automated decision support, smart healthcare solutions are steadily transforming traditional healthcare models into data-driven, patient-centric frameworks.

Smart healthcare encompasses a wide range of innovations, including **robotics, edge computing, federated learning (FL), cloud integration, and secure communication protocols**. Together, these technologies facilitate remote diagnosis, telemedicine, and continuous health management. Figure 2 in the original work illustrates how these technologies form the core components of an integrated smart healthcare architecture.

Healthcare is a multifaceted domain involving hospitals, clinics, pharmacies, insurance providers, medical device manufacturers, and regulatory authorities. The literature reviewed in this section highlights key developments in IoT-based healthcare monitoring systems, with a focus on data privacy, cybersecurity, and intelligent automation. Table 2 summarizes recent studies that address various aspects of IoT-driven healthcare innovation.

Key Studies in IoT-Based Healthcare and Federated Learning

1. **"Federated Learning in Healthcare: Model Misconducts, Security, Challenges, and Applications"**
   This study presents an in-depth exploration of **federated learning (FL)** as a method for privacy-preserving data sharing in healthcare. The authors highlight FL's potential to enable collaborative model training without transferring raw patient data, thereby reducing privacy risks. The paper also discusses challenges related to data heterogeneity, communication efficiency, and model poisoning attacks, suggesting future directions for improving the scalability and trustworthiness of FL in medical research.
2. **"Secure and Efficient Smart Healthcare System Based on Federated Learning"**
   This work proposes a **dynamic secret-sharing mechanism** combined with strong user authentication to address privacy and performance issues in FL-based healthcare systems. The authors demonstrate that their model enhances both communication efficiency and data protection, making federated learning more practical for real-world medical applications. Experimental results confirm the approach's effectiveness in maintaining security while ensuring minimal latency in data processing.
3. **"A Survey on Federated Learning: Challenges and Applications"**
   This comprehensive survey reviews the latest advances in FL across various domains, including healthcare, IoT, and finance. The authors emphasize FL's capacity to transform medical data analysis

by enabling decentralized learning while maintaining data confidentiality. They call for further research to improve communication protocols and enhance privacy-preserving model aggregation techniques.

4. **"Healthcare System Based on Random Forest Classifier and IoT"**
   In this study, researchers developed an IoT-based healthcare framework employing a **Random Forest Classifier** to facilitate intelligent diagnosis and patient monitoring. Tested on eight disease datasets, the system achieved a peak accuracy of **97.26%** on dermatological data. The findings underscore Random Forest's robustness and accuracy, making it a reliable choice for IoT-based medical decision support systems.
5. **"A Fog-Based Privacy-Preserving Federated Learning System for Smart Healthcare Applications"**
   This paper introduces a **fog computing–enabled FL framework** designed to process medical imaging data, particularly heterogeneous CT scans. The system enhances privacy and computational efficiency by performing data aggregation closer to the data source, reducing latency and transmission costs. The authors propose integrating FL with blockchain technology in future research to further strengthen system security and cost-effectiveness.
6. **"Federated Learning: Strategies for Improving Communication Efficiency"**
   This study investigates methods to enhance communication efficiency within FL-based IoT systems. The authors discuss model compression, parameter quantization, and asynchronous updates as strategies to reduce overhead while maintaining model accuracy. Such approaches are crucial for healthcare IoT networks, where limited bandwidth and energy constraints are common challenges.
7. **"Federated Learning for Internet of Things: A Comprehensive Survey"**
   This work provides a detailed examination of the intersection between **IoT and federated learning**, analyzing opportunities and challenges across domains such as smart healthcare, transportation, and smart cities. The authors identify key research gaps, particularly regarding privacy guarantees, device heterogeneity, and energy optimization in distributed healthcare networks.
8. **"Modeling and Simulation of IoT Systems in Healthcare Applications"**
   The study explores the use of IoT technologies for monitoring and treating various medical conditions, including diabetes, hypertension, and stroke rehabilitation. It emphasizes the use of **ECG and PPG sensors** integrated with smartphones for convenient, continuous blood pressure monitoring. The authors highlight the growing importance of user-friendly and cost-effective IoT solutions for home-based healthcare management.
9. **"A Federated Learning-Based Privacy-Preserving Smart Healthcare System"**
   This research introduces **ADDETECTOR**, a privacy-preserving system for detecting Alzheimer's disease using voice data from smart devices. The system leverages **differential privacy (DP)** and an FL framework to secure model updates during transmission. Results show that ADDETECTOR achieves high diagnostic accuracy while maintaining strong privacy protection, demonstrating the potential of FL for sensitive neurological applications.

Overall, these studies reflect the rapid evolution of IoT and federated learning in healthcare. The integration of secure communication protocols, privacy-preserving algorithms, and intelligent learning models is reshaping how medical data is utilized. While substantial progress has been made, challenges such as **data interoperability, communication overhead, and model transparency** continue to drive future research in the quest for safer and smarter healthcare systems.

8. Conclusion

The review presented in this paper highlights the transformative potential of the **Internet of Things (IoT)** and **Federated Learning (FL)** in shaping the future of healthcare. Together, these technologies have redefined how medical data is collected, processed, and secured, paving the way for smarter, more efficient, and patient-centered healthcare systems. IoT enables real-time monitoring and personalized care through interconnected devices and sensors, while federated learning allows for decentralized model training without compromising sensitive patient information.

The integration of **Machine Learning (ML)** and **Artificial Intelligence (AI)** into IoT healthcare systems has made it possible to analyze massive datasets, detect anomalies, and predict health risks with remarkable precision. However, as the healthcare ecosystem becomes increasingly digital, concerns surrounding **data privacy, cybersecurity, and regulatory compliance** have become more complex and critical. The reviewed studies demonstrate that robust security mechanisms—such as encryption, authentication, access control, and privacy-preserving learning—are indispensable for protecting patient data in this highly connected environment.

Despite significant advancements, several challenges remain unresolved. Issues such as **interoperability among heterogeneous devices**, **communication efficiency**, and **trust management** in distributed networks require further exploration. Additionally, balancing the trade-off between data utility and privacy remains a major research priority. Future work should focus on developing **lightweight, scalable, and explainable AI models** that can operate securely on edge and fog computing platforms while maintaining transparency and fairness in decision-making.

In conclusion, the convergence of IoT, ML, and FL is driving a paradigm shift in healthcare—transforming it from a reactive system to a **predictive, preventive, and personalized ecosystem**. By addressing privacy and security concerns through intelligent design and ethical governance, future IoT healthcare systems can achieve both **technological excellence and public trust**. The path forward lies in continuous innovation, interdisciplinary collaboration, and the responsible use of emerging technologies to ensure a secure and sustainable digital healthcare future.

References

1. C. Milana, A. Ashta, Artificial intelligence techniques in finance and financial markets: A survey of the literature, Strateg. Chang. 30 (3) (2021) 189–209.
2. J. Jumper, R. Evans, A. Pritzel, T. Green, M. Figurnov, O. Ronneberger, K. Tunyasuvunakool, R. Bates, A. Žídek, A. Potapenko, et al., Highly accurate protein structure prediction with AlphaFold, Nature 596 (7873) (2021) 583–589.
3. F. Urbina, F. Lentzos, C. Invernizzi, S. Ekins, Dual use of artificialintelligence-powered drug discovery, Nat. Mach. Intell. 4 (3) (2022) 189–191.
4. D. Lee, S.N. Yoon, Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges, Int. J. Environ. Res. Public Health 18 (1) (2021) 271.
5. A. Qayyum, J. Qadir, M. Bilal, A. Al-Fuqaha, Secure and robust machine learning for healthcare: A survey IEEE Rev. Biomed. Eng., 14 (2020), pp. 156-180
6. Y. Zhang, T. Gu, and X. Zhang, "Mdldroid: a chainsgd-reduce approach to mobile deep learning for personal mobile sensing," in 2020 19th ACM/IEEE International Conference on Information Processing in Sen or networks (IPSN). IEEE, 2020, pp. 73–84.

7. K. Hao, "How Apple personalizes Siri without hoovering up your data," 2019. [Online]. Available: https://www.technologyreview.com/2019/12/ 11/131629/apple-ai-personalizes-siri-federated-learning/
8. J. Benet, "IPFS-content addressed, versioned, P2P file system," arXiv preprint arXiv:1407.3561, 2014.
9. C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Theory of Cryptography Conference (TCC), 2006, pp. 265–284.
10. C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2006, pp. 486–503.
11. H. Niavis, N. Papadis, V. Reddy, H. Rao, and L. Tassiulas, "A blockchain-based decentralized data sharing infrastructure for off grid networking," in Proc. IEEE Int. Conf. Blockchain Cryptocurr. (ICBC), 2020, pp. 1–5.
12. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Artif. Intell. Statist., 2017, pp. 1273–1282.
13. H. Fang and Q. Qian, "Privacy preserving machine learning with homo morphic encryption and federated learning," Future Internet, vol. 13, no. 4, p. 94, 2021.
14. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," in Proc. Decent. Bus. Rev., 2008, p. 21260
15. H. S. Chen, J. T. Jarrell, K. A. Carpenter, D. S. Cohen, and X. Huang "Blockchain in healthcare: A patient-centered model," Biomed. J. Sci. Techn. Res., vol. 20, no. 3, 2019, Art. no. 15017.
16. F. Wang, A. Preininger, AI in health: state of the art, challenges, and future directions, Yearb. Med. Inform. 28 (2019) 016–026.
17. Y. Xu, G. Xu, C. Ma, Z. An, An advancing temporal convolutional network for 5G latency services via automatic modulation recognition, IEEE Trans. Circuits Syst. II (2022).
18. L.O. Gostin, National Health Information Privacy: Regulations under the Health Insurance Portability and Accountability Act, JAMA 285 (2001) 3015–3021.
19. Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (2015) 436–444.
20. D.C. Nguyen, et al., Federated Learning for Smart Healthcare: A Survey, ACM Comput. Surv. 55 (2022) 1–37.
21. L. L. Văduva, A.-M. Nedelcu, D. Stancu, C. Bălan, I.-M. Purcărea, M. Gurău, and D. A. Cristian, ''Digital technologies for public health services after the COVID-19 pandemic: A risk management analysis,'' Sustainability, vol. 15, no. 4, p. 3146, Feb. 2023.
22. A. A. Alqahtani, M. M. Ahmed, A. A. Mohammed, and J. Ahmad, ''3D printed pharmaceutical systems for personalized treatment in metabolic syndrome,'' Pharmaceutics, vol. 15, no. 4, p. 1152, Apr. 2023.
23. S. Basak and K. Chatterjee, ''Smart healthcare surveillance system using IoTandmachinelearningapproachesfor heart disease,'' in Proc. Advanced Smart Comput. Inf. Secur., 1st Int. Conf. (ASCIS). Rajkot, India: Springer, Nov. 2023, pp. 304–313.
24. X.Su,L.An,Z.Cheng,andY.Weng,''Cloud–edgecollaboration-basedbi level optimal scheduling for intelligent healthcare systems,'' Future Gener. Comput. Syst., vol. 141, pp. 28–39, Apr. 2023.
25. K.A.Awan,I.U.Din,A.Almogren,andJ.J.P.C.Rodrigues, ''AutoTrust: A privacy-enhanced trust-based intrusion detection approach for Internet of Smart things,'' Future Gener. Comput. Syst., vol. 137, pp. 288–301, Dec. 2022.

26. K. A.Awan,I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "HoliTrust—A holistic cross-domain trust management mechanism for service-centric Internet of Things," IEEE Access, vol. 7, pp. 52191–52201, 2019.
27. M.S.Islam,M.A.B.Ameedeen,M.A.Rahman,H.Ajra,andZ.B.Ismail, "Healthcare-chain: Blockchain-enabled decentralized trustworthy system in healthcare management industry 4.0 with cyber safeguard," Computers, vol. 12, no. 2, p. 46, Feb. 2023.
28. K. A. Awan, I. U. Din, A. Almogren, H. Almajed, I. Mohiuddin, and M. Guizani, "NeuroTrust—Artificial-neural-network-based intelli gent trust management mechanism for large-scale Internet of Medi cal things," IEEE Internet Things J., vol. 8, no. 21, pp. 15672–15682, Nov. 2021.
29. H. Malik, T., Anees, A. and Naeem, R. A. Naqvi, and W.-K. Loh, "Blockchain-federated and Deep-learning-based ensembling of capsule network with incremental extreme learning machines for classification of COVID-19 using CT scans," Bioengineering, vol. 10, no. 2, p. 203, Feb. 2023.
30. T.-F. Lee, I.-P. Chang, and G.-J. Su, "Compliance with HIPAA and GDPR in certificateless-based authenticated key agreement using extended chaotic maps," Electronics, vol. 12, no. 5, p. 1108,