Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 04 Issue 01
2022

Research Article
https://doi.org/10.56979/401/2022/88

Security and Privacy for Future Healthcare IoT

Muhammad Kamran Abid[1*], Zia Ur Rehman Zia[2], and Shahid Farid[3]

[1]Department of Computer Science, NFC IET, Multan, 66000, Pakistan.
[2]Department of Computer Science,Institute of Southern Punjab, Multan, Pakistan.
[3]Department of Computer Science, Bahauddin Zakariya University, Multan,60800, Pakistan.
[*]Corresponding Author: Muhammad Kamran Abid. Email: kamran.abid@nfiet.edu.pk.

Received: March 11, 2022 **Accepted:** November 29, 2022 **Published:** December 29, 2022.

Abstract: Computer networks are widely used in today's society, and we utilize the Internet to connect to our home networks. IoT networks are a brand-new category of these networks where we attempt to connect various household equipment and attempt to issue orders from a distance. Hash code or message authentication code (MAC) is used for authentication, and several encryptions and decryption techniques guarantee secrecy. The cost of using traditional cryptographic security techniques in terms of computing resources like memory, processor power, and power consumption is high. There is no proper model/ framework available to address the major security issues of IoT devices. The literature address that still several gaps exist regarding security issues. To secure and protect future healthcare IoT systems, this research will provide a model that combines shallow learning with deep learning.

Keywords: IoT; Smar Healthcare; Security and Privacy

1. Introduction

The term "Internet of Things" (IoT) refers to a wide variety of devices and communication methods. Today, the word "IoT" is used increasingly to describe the idea that everything should be online. IoT will be crucial in the future due of the idea creates possibilities for novel services and inventions. Everything will be interconnected. Despite operating in areas without protection, they are capable of communicating with one another. The latter element creates serious security difficulties. IoT needs a lot of standardization right now, as well as defined designs that outline how this technology should be used and how IoT devices can communicate with one another securely. The technology and how information is collected and managed by this technology are at the heart of security concerns. In the era of smart gadgets, IoT has expanded rapidly. A wide range of industries, including enterprises, hospitals, and farming, are heavily utilizing rapidly evolving smart gadgets, such as sensors and grids. IoT consumers are exposed to several security issues since there are so many IoT devices in use[1][2]. IoT has expanded significantly during the last five years. 22 billion IoT devices were linked globally in 2018, according to a new report published in 2019. Additionally, it predicts that it would rise to 38.6 billion in 2025 and 50 billion in 2030[1]. We continually give our surfing history, location, contacts, calendar events, and health details to IoT devices[3]. The major motivations behind gathering private information are convenience and improving our quality of life through the usage of these smart gadgets.

Sadly, the ease that these devices offer us daily may also come at the expense of putting our security at risk[4]. The IoT network's smart gadgets hold extremely private and individualized data. Such information can be accessed by unauthorized persons or agents, which can have a very negative impact on the user's safety and well-being. For example, a hacker might get access to our home security cameras and violate our privacy, or they might be able to commandeer self-driving automobiles and seriously harm the driver. [5]. Security and privacy issues arise from the multiplicity of IoT devices. New and evolving IoT devices can't meet user expectations and may lose consumers if there isn't a framework that allows them to share and use information quietly and securely. IoT networks face particular difficulties concerning privacy, authentication, storage, and data processing speeds. IoT hardware is also basic and lacks necessary security software and modules. Cyberattacks can be launched by criminals because security is lacking. The Internet of Things (IoT) is a technology that links a variety of nodes and objects, including people, infrastructure, and technological devices. It improves daily life by making it simpler, safer, and more efficient. These nodes become the weakest point in the cyber-attackers chain since they are typically resource-constrained because they are a part of a vast network of various devices. Traditional encryption methods have been used to make sure the IoT network's data security. However, IoT cannot use high-level encryption algorithms. devices as a result of resource constraints. Additionally, network engineers continue to face difficulties with node security[6][7][8]. We must therefore take into account a comprehensive IoT network solution that can ensure node and data security. Artificial intelligence fields such as rule-based techniques, shallow machine learning, and deep machine learning may one day be useful for protecting Internet of Things (IoT) devices.[9][10][11].

For IoT networks, where data freshness, consistent system localization, time synchronization, and availability are all critical security criteria, confidentiality, source authentication, and availability Self-organization and organization are treated as minor. However, maintaining personal relationships is more difficult. Data security, user identification, threat management, encryption application security, access control, network security, devices with limited resources, and latency in IoT network architecture. Many studies have been done to reduce different threats and improve the security of IoT networks, but still, there are many gaps exist regarding the security of IoT devices[12]. The Internet of Things (IoT) is a novel technology that allows sensors and control systems to create, share, and consume data with little to no human engagement through physical network connectivity and computational capabilities[13]. This encourages us to find out solutions for security using Machine Learning (ML) and Artificial Intelligence (AI)[14]. This paper presents an ML and AI base theoretical security architecture with partial validation using healthcare case study data of IoT devices.

2. Literature Review

Internet of things (IoT) devices and recent advancements in electronic technology have transformed the conventional healthcare system into a smart healthcare system. Applications including holographic communication, telesurgery, Hospital-to-Home (H2H), and Quality of Life (QoL) services will form the foundation of future healthcare systems. Telesurgery and holographic communication will require particularly difficult and time-sensitive performance requirements. Due to low data rates, current wireless designs, even 5G, cannot support intelligent healthcare applications. The 6G is expected to completely revolutionize the current healthcare system and help reduce communication barriers posed by the current wireless architecture.

Although it has been emphasized that fixing security flaws has gotten the most attention, more needs to be done in contemporary electronic healthcare systems to guarantee end-user privacy. Modern healthcare is transformed into a new arena by mixing cutting-edge digital technologies like IoT, and high computing devices to store and analyze data, personal health records, and more.[15]. Although it has been noted that fixing security vulnerabilities has received the majority of attention, more work has to be done in modern electronic healthcare systems to ensure end-user privacy. By combining cutting-edge digital technologies like IoT, high computing devices to store and analyze data, personal health records, and more, modern healthcare is converted into a new realm[16]. Healthcare system cybersecurity remains a challenge despite all of these advantages. Due to inadequate information security defenses, electronic healthcare systems are thought to be a simple target for attackers. A hacker may gain access to the system, encrypt it with ransomware, steal patient data from medical facilities and sell it, or blackmail people into exposing their personal information[17]. The computerized healthcare system has also been reported to have a higher prevalence of attackable weak points. Such an exploit was found by a security operator who was looking at the communication protocols. As a result, it is noted that before deploying any security or privacy approach, a system risk analysis should be performed[18]. Therefore, security and privacy issues must be addressed for IoT devices to operate correctly because they pose a significant threat to modern healthcare systems.

The development of machine learning (ML) as a technology platform has altered and been reflected in recent years by increases in processing capacity. Machine learning approaches have improved many fields, altered behaviors, and had an impact on real-world applications[19][20]. There were various issues before machine learning was utilized in security. One issue was that manual analysis was impractical given the volume of data. 2. As a result of security risks' quickening evolution, which preys on hurried habits, important new security concerns have evolved. 3. Emerging dangers like elusive were difficult to recognize and control. 4. Over time, cost consumption has greatly increased. 5. It costs time and money to create and implement new algorithms. 5. As a result, subject-matter specialists found it more difficult. The use of machine learning has significantly improved cyberspace security. The following advantages are 1. ML enables cybersecurity systems to thwart similar attacks by analyzing trends and adjusting to changing performance. 2. Be more proactive in your defense against threats and reactions to on-the-spot assaults. 3. To discriminate between typical and atypical models, user behavior modeling. 4. In the eyes of professionals in the danger domain, it becomes more approachable and comparable. 5. Both now and in the future, there has been good progress in the detection of Advanced Persistent Threats.

Deep learning is a subset of machine learning that focuses on identifying increasing layers of meaningful input data representations. Learning is made possible by artificial neural networks (ANNs) with multiple layers. The concept of deep learning can be used for Malware Classification, Vulnerability Discovery and Intrusion Detection for Networks. Shallow learning models can only learn one or two representational levels of the input data. Because of their incredibly poor representational ability, they are unable to understand complex relationships between the attributes of the input data. Feature engineering is therefore essential when using shallow learning techniques. Shallow learning is used for Anomaly Detection and Features Description. IoT devices are one of the security chinks in the armor. There is a good likelihood that an attacker may utilize an IoT device to access the system because these devices are often always linked to the internet and other devices[21][22]. One of the IoT device security attacks is phishing attacks, which aim to access personal information, you can access company or financial data by convincing the end user to submit their username and password on a fake website or by installing a dangerous application.

The main challenge for the adaption of a modern sensor base network is the security and privacy of IoT devices. Table 1 clearly shows the security flaws, however, there are still a lot of issues that need to be addressed. Although the blockchain concept has addressed many security concerns, it is insufficient to meet the needs of the Internet of Things (IoT). At the industrial level, there are many IoT devices in use, but there is currently no complete model for the security and privacy of industrial IoT devices. There have been many concerns and attacks concerning security revealed in the literature, but the future of IoT still needs a lot of solutions addressing device privacy and security.

Table 1. Literature for IoT security

Paper Reference	Year Of Publication	Keywords	Solutions	Limitations
[23]	2022	authentication; confidentiality; internet of things	Asymmetric key cryptography	Very limited scope for devices authentication
[22]	2019	security issues in IoT	Identification of solutions and challenges only	No model/ framework regarding security

[24]	2022	Internet of Things, security data	Identification of industrial IoT issues	The rule of Blockchain is not clearly defined according to the future IoT security needs
[8]	2022	Internet of Things (IoT), Blockchain	Identification of issues regarding industrial IoT	No security model for 4.0 Industrial IoT
[25]	2021	IoT security	Gap identification	No proper solution exists regarding the security of modern devices on the network layer
[25]	2022	Security, IoT	detected 16 attacks for IoT wireless Security	Still, there are several Gaps in Security
[26]	2022	cyber-attacks, IoT, Security	Use of artificial intelligence (AI) for security	Need for deep learning-based IoT security solution
[27]	2021	Internet of Things, Fog computing	Acts as a middle layer between IoT device and data center, a decentralized approach	Need high computation at a different level, network resources availability, devices heterogeneity cannot be handled properly

Future Internet of Things devices will be secure and private thanks to the use of cutting-edge technologies like blockchain, artificial intelligence, and machine learning. The table2 summarizes the research on emerging methods for ensuring the security and privacy of electronic devices. In this regard, several theoretical models are offered, each of which addresses a particular security or privacy concern. A broad paradigm that successfully addresses the majority of security and privacy challenges is therefore required. Another topic that has been covered in the literature is choosing the best machine learning algorithm and dataset. Many contemporary techniques are described, although the majority of them deal with basic privacy and security concerns; on the other hand, the sophisticated security concerns that still need to be resolved are the main problem. The majority of researchers are concentrating on the security of gadgets, but privacy will soon overtake security as the most crucial problem.

Table 2. Literature regarding AI and Machine Leering

Paper Reference	Year Of Publication	Keywords	Solutions	Limitations
[21]	2021	Internet of thing (IoT), Machine Learning, Artificial Intelligence	Use of ML, AI, and deep learning model theoretical	No proper model has been purposed every technique deal with some specific issue only
[1]	2021	Internet of thing (IoT), Machine	Issues identification and available solutions using ML and Blockchain	An issue in the selection of the right ML algorithm and correct dataset for training

		Learning, blockchain		
[9]	2022	Internet of thing (IoT), Machine Learning, AI	Identification and categorization of security attacks	AI and ML approaches still need to update for providing complete security and privacy to IoT devices
[28]	2021	IoT, Features selection	Model auto selection of features	Features are tested for only the purposed model but not on any available ML model
[26]	2022	Internet of thing (IoT), Machine Learning, AI	Use of different machine learning techniques	There is a need for a comprehensive machine learning and AI base model to handle the security issues
[6]	2021	Fuzzy logic, Machine Learning protocols	Survey on the security issues layer-wise	AI and ML use is still not defined completely for handling the complex security issues
[29]	2021	Internet of thing (IoT), Machine Learning, Deep Learning, Blockchain	Anomaly detection using blockchain technology	Work on the basic level of anomaly detection only

3. Methodology

A literature review was conducted for the most recent study on security and privacy issues with IoT healthcare devices. The majority of the research will be based on articles published in the past three years that highlighted the main issues with the security and privacy of IoT medical devices. By determining the anticipated requirements for IoT healthcare devices, a theoretical model has been created.

4. Solution for Future IoT

The literature mentioned above has made it abundantly evident that future internet of things devices require a model or architecture that deals with security and privacy. The IoT devices' three levels of operation are classified into the first level, which deals with IoT sensors and needs physical security. The level 1 faults are primarily the fault of the device's manufacturer. The majority of level 1 problems have been fixed, and this level appears secure going forward. Numerous solutions are also available concerning network security as Figure 1 depicts the network as level 2 and is utilized for data transfer. Due to the maturity of the algorithms at that level, attackers will have less interest in that level soon.

The IoT devices in a healthcare system are networked and have level 3 storage for their data. Because information can be accessed and tempered at level 3, level 3 is about data storage and access, which is an attacker's preferred area. The information about the patients that the doctors receive comes from the sensors affixed to the patients and is stored locally by the doctors. Because these data are so private and sensitive, attackers are drawn to them. A nurse is using a predictive model to keep track of the several patients at her desk; any tampering with the data could result in a false alarm. A false alarm could simultaneously be sent to the ambulance emergency service. A fictitious call has been made to the doctor treating that patient. All of this will occur if someone gains unauthorized access to your local data storage. This situation turned into a significant barrier to the healthcare IoT environment's adaptability.

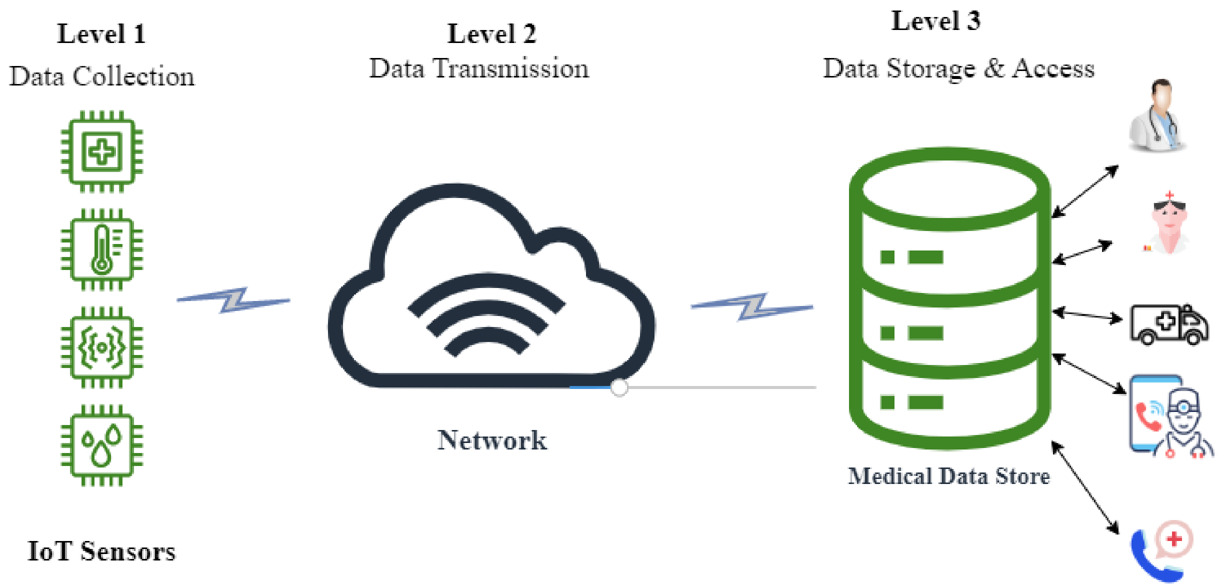

Figure 1. Architecture of Healthcare IoT

Due to the importance and sensitivity of the data, an attacker with malice becomes involved with local data storage, as depicted in figure 2. The security of the system as well as patient privacy will be violated by this move. In a medical setting, confidentiality is of utmost significance, and no one consents to share their data with others. For the future healthcare IoT context, basic approaches like encryption, decryption, hashing, firewalls, etc. are insufficient. Modern techniques can be used to solve contemporary problems. Currently, security policies and regulations are created manually. Over time, an attacker can readily identify the flaws, which results in a security and privacy breach. For a system to be the most secure, it must have the ability to predict the future and update its state continuously.

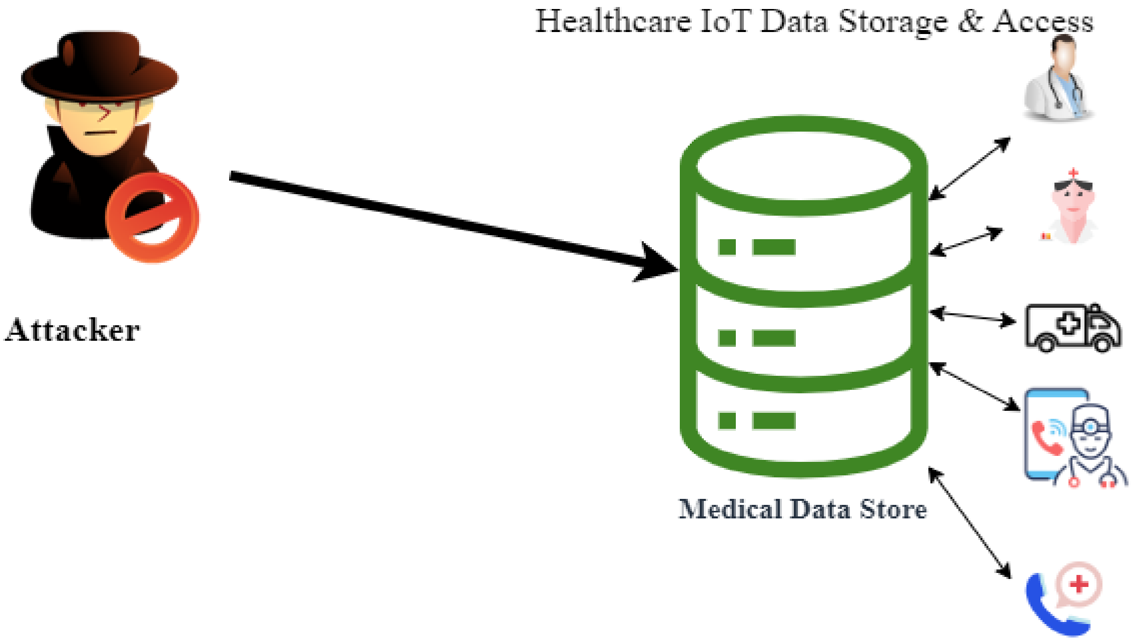

Figure 2. Attacker model for Healthcare IoT

The purpose model, which is based on the shallow and deep learning techniques previously outlined, will address the majority of security and privacy issues for the eventual adoption of IoT devices in healthcare systems. The theoretical view of the intended model is depicted in Figure 3, where shallow learning is employed to detect anomalies, which identify the type of access request and categorize it as a normal request or abnormality. Deep learning is utilized for intelligent decision-making when an abnormal request is sent to the decision-maker.

4.1 Shallow Learning Use

In this case, considerable processing is required if every request is deemed anomalous and a deep learning model is employed to provide a solution. Delay matters a lot because future surgeries will be performed online. Shallow learning uses fewer layers and less processing to make decisions, which facilitates the smooth execution of actual requests. On the other hand, even superficial learning is insufficient for making decisions regarding various abnormalities. Deep learning decisions are incorporated into shallow learning for future decisions, and policies are changed.

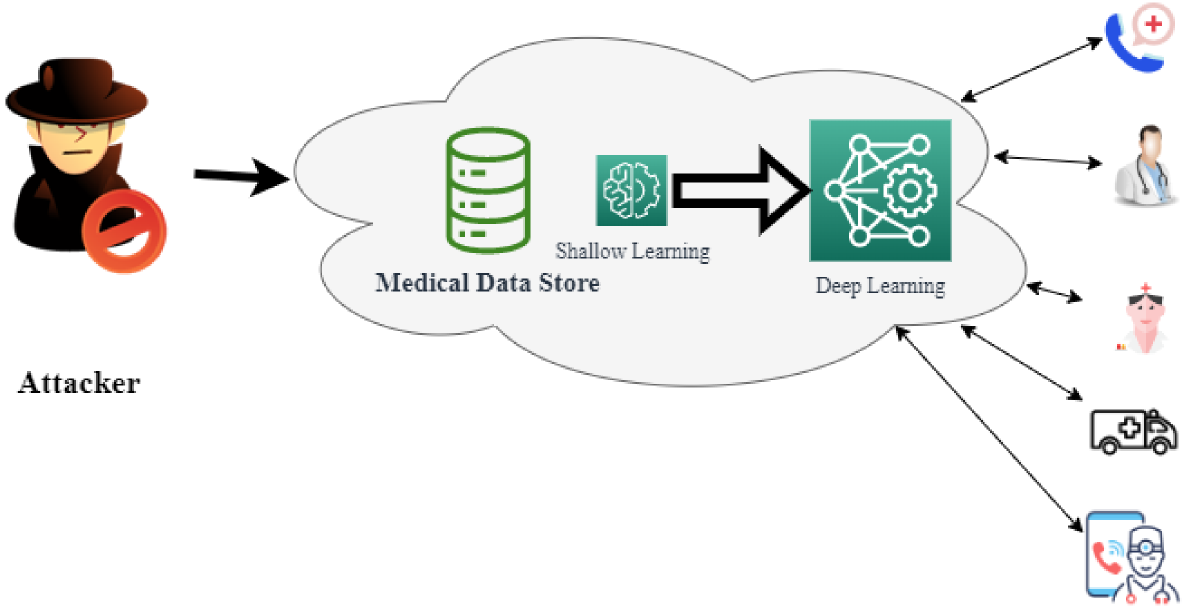

Figure 3. Security Architecture using Deep Learning and Shallow Learning

4.2 Deep Learning Use

If anomalies are found, an intelligent judgment must be made, and deep learning models are employed for further actions. Utilizing deep learning techniques, the system will automatically update the security regulations. The majority of security difficulties can be resolved by implementing an intelligent decision-making system, which will be updated before an attacker finds any flaws. There will be less of a high danger of security breaches. There are many deep learning algorithms accessible, but choosing the best one is very difficult and reduces security risk even further.

4.3 Dealing with the privacy

As was previously mentioned, in the future, the privacy of Healthcare IoT devices will be more crucial than their security. As shown in figure4, the local medical data repository will merge with worldwide data, which will be utilized to make predictions and construct models. Customers' privacy will be violated if a local data store shares all of their info with the world. The patient's attributes are also stored locally; by submitting them to the global data store, these attributes will eventually become public. This privacy breach will require some fundamental solutions. The request from an external network, such as global data, is likewise handled as an anomaly in our designed model, and this anomaly is sent to the deep learning model. By concealing the patient's features from aggregate data, the deep learning model will make an educated conclusion. Patient privacy is improved since personal data about the patient, such as name and ID, is not shared globally.

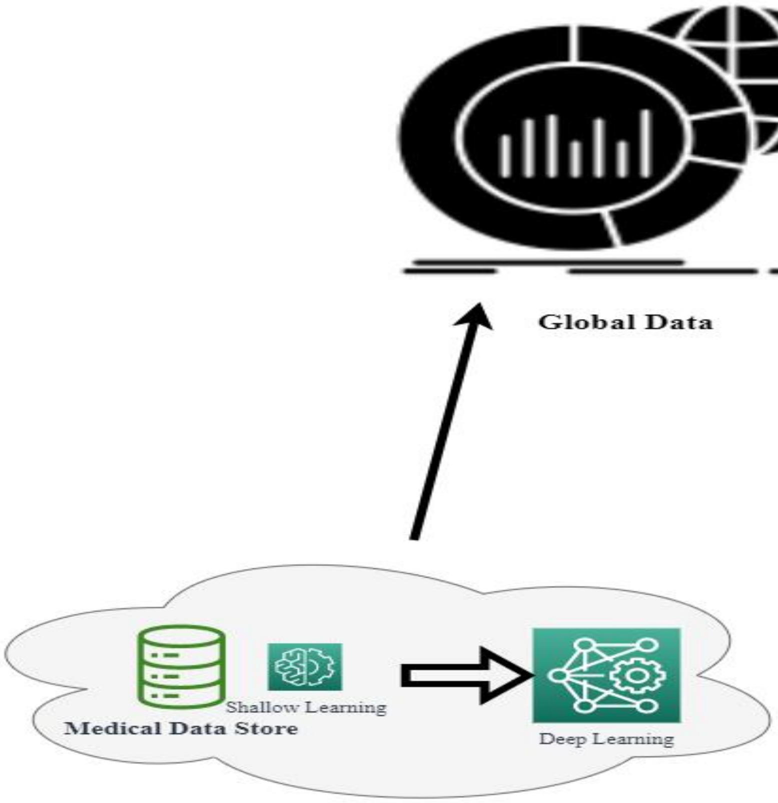

Figure 4. Privacy Only Architecture

As data become a part of any big data or global data, the risk of privacy violations increasing too much needs to be addressed locally. The intended model uses deep learning models to locally handle the request; personal attributes are only shared locally. Because the information included in these attributes plays a crucial function locally for any doctor, nurse, patient emergency service, etc., it is not possible to deal with them by deleting the data.

5. Conclusion

The quickly developing smart devices, such as sensors and grids, are being extensively used by hospitals. Due to the prevalence of IoT devices, users are at risk for security and privacy vulnerabilities. The future security and privacy concerns cannot be regarded as being as straightforward as those of the present since they cannot be resolved using straightforward conventional methods. this led to the discovery of contemporary methods like deep learning. A theoretical model that combines shallow learning and deep learning methods has been described. This approach will handle security and privacy issues more effectively, and it will also handle issues with future privacy as privacy becomes more essential. The approach presents the idea of addressing privacy locally since patient privacy faces additional obstacles as data becomes a part of the global data set.

5.1 Future Work

The theoretical model presented in this research needs to be put into practice and should be compared to privacy models based on blockchains. In that concept, federated learning can likewise take the role of shallow learning in operation. The choice of the Deep Learning model is equally crucial for the right outcomes.

References:

1. Liang, X.; Kim, Y. A Survey on Security Attacks and Solutions in the IoT Network. 2021 IEEE 11th Annu. Comput. Commun. Work. Conf. CCWC 2021 2021, 853–859, doi:10.1109/CCWC51732.2021.9376174.
2. M Kamran Abid An Analysis of Cloud Computing Security Problems. Int. J. Inf. Syst. Comput. Technol. 2022, Vol. 1 No.
3. Akbar, S.; Ahmad, K.T.; Abid, M.K.; Aslam, N. Wheat Disease Detection for Yield Management Using IoT and Deep Learning Techniques. 2022, 10, 80–89.
4. Aldowah, H.; Rehman, S.U.; Umar, I. Security in Internet of Things : Issues , Challenges , and Solutions Security in Internet of Things : Issues , Challenges and Solutions; Springer International Publishing, 2019; ISBN 9783319990071.
5. Li, H.; Zhou, X. Study on Security Architecture for Internet of Things *. 2011, 2011–2012.
6. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Member, S.; Ahmed, M.R.; Khan, R.T.; Member, S.; Mahmud, M.; Member, S. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks : A Comprehensive Survey. 2021, 9.
7. Badidi, E.; Ragmani, A. ScienceDirect An Architecture Architecture for for QoS-Aware QoS-Aware Fog Fog Service Service Provisioning Provisioning. Procedia Comput. Sci. 2020, 170, 411–418, doi:10.1016/j.procs.2020.03.083.
8. Paliwoda, B.; Krzysztof, W.; Biega, M. Challenges and Opportunities — A Review. 2022.
9. Abdullahi, M.; Baashar, Y.; Alhussian, H.; Alwadain, A.; Aziz, N. Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods : A Systematic Literature Review. 2022, 1–27.
10. Mubashir Ali Lung Cancer Detection using Supervised Machine Learning Techniques. Lahore Garrison Univ. Res. J. Comput. Sci. Inf. Technol. 2022, 6, 49–68, doi:10.54692/lgurjcsit.2022.0601276.
11. Kanwal, A.; Ahmad, K.T.; Abid, M.K.; Aslam, N. Detection of Heart Disease Using Supervised Machine Learning. 2022, 6246, 58–70.
12. Ahmed, S. IoT Based Smart Systems using Machine Learning (ML) and Artificial Intelligence (AI): Vulnerabilities and Intelligent Solutions. 2022, 56–61.
13. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors 2021, 21, doi:10.3390/s21113654.
14. Liagkou, V.; Stylios, C.; Pappa, L.; Petunin, A. Artificial Intelligence and Cybernetics. 2021, 1–23.
15. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. applied sciences IoT Privacy and Security : Challenges and Solutions. 2020, 1–17.
16. Hameed, S.S.; Hassan, W.H.; Latiff, L.A. A systematic review of security and privacy issues in the internet of medical things ; the role of machine learning approaches. 2021, 1–44, doi:10.7717/peerj-cs.414.
17. Alshehri, F.; Muhammad, G.; Member, S. A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. 2021, 9, doi:10.1109/ACCESS.2020.3047960.
18. Bout, E.; Loscri, V.; Gallais, A.; Bout, E.; Loscri, V.; Gallais, A.; Machine, H.; Bout, E.; Loscri, V.; Gallais, A. How Machine Learning changes the nature of cyberattacks on IoT networks : A survey To cite this version : HAL Id : hal-03390359 How Machine Learning changes the nature of cyberattacks on IoT networks : A survey. 2021.
19. Kuntla, G.S. Security and privacy in machine learning : A survey. 2021, 22, 224–240.
20. Mazhar, N.; Salleh, R.; Hossain, M.A.; Zeeshan, M. SDN based Intrusion Detection and Prevention Systems using Manufacturer Usage Description : A Survey. 2020, 11.
21. Education, M. Securing Industrial Infrastructure against Cyber-Attacks Using Machine Learning and Artificial Intelligence at the Age of Industry 4 . 0. 2021, 12, 6581–6594.
22. Sabri, M.S. Internet of Things (IoT): Security Issues and Challenges Internet of Things (IoT): Security Issues and Challenges. 2021.
23. Kumar, V.; Malik, N.; Singla, J.; Jhanjhi, N.Z.; Amsaad, F.; Razaque, A. Light Weight Authentication Scheme for Smart Home IoT Devices. 2022.
24. Raimundo, R.J. applied sciences Cybersecurity in the Internet of Things in Industrial Management. 2022.
25. Millar, S.; Llc, R. IoT Security Challenges and Mitigations : An Introduction. 1–5.
26. Sarker, I.H.; Khan, A.I.; Abushark, Y.B.; Alsolami, F. Internet of Things (IoT) Security Intelligence : A Comprehensive Overview , Machine Learning Solutions and Research Directions. 2022, doi:10.20944/preprints202203.0087.v1.
27. Sabireen, H.; Neelanarayanan, V. A Review on Fog Computing : Architecture , Fog with IoT , Algorithms and Research Challenges. ICT Express 2021, 7, 162–176, doi:10.1016/j.icte.2021.05.004.
28. Nimbalkar, P.; Kshirsagar, D. Feature selection for intrusion detection system in Internet-of-Things (IoT). ICT Express 2021, 7, 177–181, doi:10.1016/j.icte.2021.04.012.
29. Using, N.; Learning, M. A Comprehensive Study of Anomaly Detection Schemes in IoT Networks Using Machine Learning Algorithms. 2021, 1–13.