2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM) | 979-8-3503-9858-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/SEEDA-CECNSM57760.2022.9932957

Security and Privacy Vulnerabilities in Human Activity Recognition systems

Vasiliki Liagkou*, Sofia Sakka*, and Chrysostomos Stylios
*Department of Informatics & Telecommunications,
University of Ioannina, Arta, Greece
liagkou@uoi.gr, sofia_sakka@yahoo.com, stylios@uoi.gr

***Abstract*—Human activity recognition systems (HARS) should allow the secure and trustworthy exchange of sensitive data between several kinds of participating parties with different aims and claims, regarding security, data protection, and trust issues. Initially in this work, a security flaw has been identified in a complete medical IoT application using wearable devices and smart sensors. Then, we list the security vulnerabilities and attempt to make suggestions on the prevention of security flaws that may appear during the implementation of HARS and we analyze a specific attack, the Man in the Middle attack, where a third malicious entity interferes with communication between two entities and is associated with key exchange protocols. Moreover, we discuss various design considerations for protecting the data that is transmitted and stored from different sources like smart wearables, mobile phones, and cloud applications by using cryptographic and privacy-preserving techniques. Finally, we show how the use of the OAuth2.0 protocol can ensure that only authenticated users interact with the HARS.**

Keywords—*Human activity recognition, security, privacy*

I. Introduction

Nowadays, the rate of diseases is increasing, although technology cannot prevent it from happening, it can make healthcare easier by equipping us with friendly medical applications. IoT emerged in healthcare [1] as well, whereby sensors are being used to monitor a patient's activities or vital senses. The procedure is called Human Activity Recognition System (HARS). To that end, mobile phones and intelligent wireless wearable devices [2] come to accomplish such a task. Medical devices connect to a mobile phone's application, collect user data and send them to a cloud platform. Then, the stored data can be shared with an authorized person who could be the doctor, the caregiver, or the patient himself.

However, such procedures that handle data, especially when it comes to personal data, require privacy and security. Although significant efforts have been made in HARS, the notions of security and privacy are of main concern. The large amount of data that is being collected can lead to security and privacy concerns [3]. General approaches which prevent privacy leakage adopted anonymity access control and transparency are presented in [4]. Also, the machine learning technology that is being applied to the collected data, poses a risk to privacy and security. To maintain these properties, several solutions that combine existing data-privacy techniques have been proposed, including differential privacy and modern cryptography techniques [5].

In Smart Healthcare Systems (SHCS), also, security and privacy and major issues as the increase in the number of sensors and devices create significant challenges. In HARS, due to the data received at any time, there is the risk of hijacking and eavesdropping attacks in communication channels. Recently blockchain methodologies have been used towards a more robust and secure system in the Industrial Internet of Things (IIoT) as we can see in [6]. Moreover, a model for cybersecurity in wearable devices is presented in [7]. In general, security considerations in wearables can be seen in [8].

In this paper, we show that it is important for a HARS to allow the secure and trustworthy exchange of sensitive data between several kinds of participating parties with different aims and claims, regarding security, data protection, and trust issues. The HARS should provide a trustworthy ecosystem to the participating entities like patients, the caregiver, and healthcare companies by guaranteeing their identities and providing them legal functionalities as well as protecting user rights. In this paper, we analyze a specific attack, the Man in the Middle attack, where a third malicious entity interferes with communication between two entities and is associated with key exchange protocols. Moreover, we show how the data that is transmitted and stored from different sources like smart wearables, mobile phones, cloud applications, and databases must be properly protected by using cryptographic and privacy- preserving techniques.

We present a real-life operating system where an IoT cloud platform is being used, named Data Collection Mechanism, which communicates with an IoT application to send the vital signs of a patient to it. We list the security vulnerabilities and we attempt to make suggestions on the prevention of security flaws that may appear during the implementation of this application. Furthermore, we present design considerations to allow the secure and trustworthy exchange of sensitive data between all the participated parties in the deployed HARS. We provide a proposal for edge-based communication to ensure the security and privacy of the data transmitted. Finally, we show how the use of OAuth2.0 protocol can ensure that only authenticated users interact with the HARS.

979-8-3503-9858-8/22/$31.00 ©2022 IEEE

II. Human Activity Recognition System

The objective of HARS is to provide information about human actions for analyzing the behavior of a person in a real environment. Medical experts believe that activity recognition is one of the best ways to identify and discover new medical conditions to monitor daily activities [9]. It allows computer-based applications to help users such as patients and doctors, improve self-care, and remote care treatment. As well, remote health monitoring via connected devices can save lives in cases of a medical emergency. In this section, we present a generic architecture of HARS that can help us to locate the security vulnerabilities of a HARS system. There are four main stages in the HARS process:

1) Data acquisition: this is the first stage of the system, where the mobile application collects and sends biometric data from IoT devices. As the application is about monitoring human activity, the data acquisition source is usually sensors.

2) Pre-processing: in the second stage, the mobile application communicates with the data collection mechanism by providing formatted biometrics.

3) Model training: in the third stage, the data collection mechanism sends the formatted biometric data to the Machine Learning Service for training and obtains the patient's activity as an output. The event is also stored in the data collection mechanism remote database. The patient's activity is stored in the Mobile Application remote database.

4) Performance evaluation: after the HAR model is ready, the fourth stage takes place, with the model being applied to the real data. This is the most challenging part, as its performance depends on physical factors, such as age, physique, and the approach to performing a task [10].

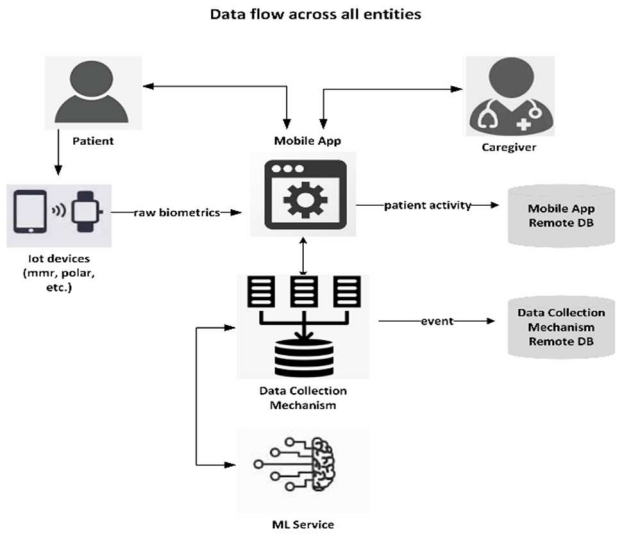

Fig. 1. A Generic Architecture of HARS

The notification of the result is pushed to the patient andncaregiver as well. The overall architecture of our deployed system isgiven in Fig.1 and it was developed and utilized via the TrackMyHealth project [11]. Regarding the system that is being proposed, it can be observed that the Mobile Device obtains readings from the Data Collection Mechanism.The readings can be stored in a Mobile Database for further processing and/or visualization. Moreover, the data can be sent to the data collection mechanism platform for manipulation and visualization as well.

III. Security and Privacy Considerations for HARS

A. Security Requirements in HARS

There are several privacy concerns about HARS because of the use of machine learning, as this approach could violate the user's privacy. As well as, if the user shares a public dataset, his anonymity is threatened. The user participates in a model training procedure with their private data and the model provider shares a publicly learned model. Thus, the privacy of the individuals' data used for training is at risk. Also, the fact that the end user shares his/her data with the service provider raises concerns about private information revealing to the service provider. Furthermore, the service provider shares query answers with the end user, so an attacker can infer the model itself by launching repeated queries [12].

In addition, as intelligent wireless wearable devices accomplish the task of monitoring human activities, they bring new challenges and opportunities for possible attacks which will put users' safety and privacy at risk [2]. The main problem is that these devices lack authentication. Although it's supposed that wearable devices should be protected with secure authentication mechanisms, this cannot be feasible due to the limited memory [2] and processing power [13]. As wearables make more and more use of user personal data, security should be given a high priority. Wearable devices are potentially always-on and always gathering data. In this way, they are open to more threats to user-sensitive information and activities at any time anywhere without the user's consent [13]. Moreover, as mentioned above, IoT devices capture and transmit data in real- time. This fact creates problems in terms of security because there is the possibility of an attack on the communication channel. Therefore, it is very important to guarantee the following security requirements in order to ensure patient privacy [2]:

a) Confidentiality: The patient should be able to trust that information about his activity is not accessible to other legitimate users. This can be achieved through encryption schemes. Asymmetric encryption is used for the purpose of secure key distribution. In an ordinary way, the Public Key Infrastructure (PKI) method is used in the context of Transport Layer Security (TLS), as well as the Eliptic Curve Cryptography (ECC) method can also be used for efficiency purposes. Provided that the keys of all entities have securely distributed and established, using symmetric encryption, these session keys are being securely sent to all entities.

b) Integrity: Data integrity is about ensuring that data is accurate and that modifying it is the result of authorized action. Any unauthorized change should be rejected by the system. Hash functions and Message Authentication Code

(MAC) functions prevent a malicious user from modifying the data that the client sends to the server, as it is designed to detect intentional modifications.

c) Authenticity: Entities should be able to prove their identity to each other so that they are really what they claim to be or what they claim to be. Authenticity can be accomplished through digital signatures.

d) Non-repudiation: Is the use of the signature to resolve disputes. The user creates the signature using his private key completing a process with legal consequences and he should be able to verify his signature. In Section IV we present how OAuth2.0 can fulfill authenticity and non-reputation requirements in HARS.

e) Data availability: Information should be accessible to any authorized user. To ensure availability, redundant networks, servers, and applications could be used.

B. HARS Vulnerabilities

HARS stores and transmits critical information like the user's health condition, user's position, or situation. No one should be able to interfere with the system's components. The fact that the authorized users can have access to the critical data needs to be established, satisfying specific properties such as integrity and secrecy. This fact raises vulnerability because data could be stolen as it is being transmitted from the Mobile Data Base (DB) to the Cloud Application (see Fig.1) and is typically combined with personally identifiable data such as name, email, telephone number, location, so it is necessary to ensure that data is being sent to a proper account. The attacks that can take place by exploiting this security vulnerability include the man-in-the-middle attack which could cause data to be sent to a malicious server [13]. A malicious user has also the ability to intercept or modify information sent by one party to another, without those parties being aware of its presence. To carry out this attack a malicious entity could exploit different techniques such as the ones in [2], [3], [14].

In particular, at the time that the entities communicate and transfer data, the system can suffer from a man in the middle attack by following the methods of:

1. Rogue Access Point: The attacker could configure a mobile device that has the application, in order to appear legitimate and connects to the victim seeking to intercept the information passing through it
2. ARP Spoofing: The Address Resolution Protocol (ARP) is used to convert IP (Internet Protocol) addresses to physical MAC (Media Access Control) addresses on a local network. However, this protocol does not provide authentication mechanisms and therefore opens a security hole that allows a man in the middle attack to be carried out using ARP Spoofing tactics. The attacker is able to connect to the network via his mobile device except that he gives his own MAC address but spoofs the IP with that of the data collection mechanism.Therefore, when communicating between cloud platforms and devices, the device does not realize that the messages are not coming from the cloud platoform itself and that a third entity is interfering. Thus, all communication passes through the attacker who can intercept or modify data by disrupting the notions of integrity and confidentiality.
3. IP Spoofing: The attacker modifies the source address of the IP packets in order to hide the sender's identity.
4. DNS Spoofing: The attacker alters the Domain Name Server (DNS). This results in the name server returning an incorrect IP address. A victim unknowingly login into his account, giving the attacker the opportunity to steal his access credentials and other types of sensitive information.

As it seems, the authentication of the parties, as well as encryption of the data passed in the communication between the entities are the main future for dealing with such an attack. As a result, the users' security and privacy are at risk without a strong authentication scheme in place [13].The majority of internet transaction usually uses the secure channel via the communication protocol TLS/SSL (Transport Layer Security/Secure Sockets Layer), but any two-way movement via these protocols couldbe decrypted by an opponent, without alerting the user or the application. Some strategies that reach this goal are [14], [15]:

- Malicious code injection: In systems like HARS where an application expects data from users could give a chance to an opponent to attack the system. This can be occured when the application does not have mechanisms to filter the data coming from the users. The attacker exploits this vulnerability and injects malicious code at the point where the user communicates with the application. After a successful injection attack, the attacker has access to the data, so he can modify it, delete it, and generally gain administrative privileges. Some examples of injection attacks are SQL (Structured Query Language**)** injection, HTML (HyperText Markup Language)/script, or XSS *(*Cross-Site Scripting) attacks, and modifying binary files sent by the user to gain access to their account or modify the behavior of the application.
- Internet Protocol Security (IPsec): A lot of users authenticate themselves by using the internet protocol layer and enabling various cryptographic functions that are provided by IPsec comunication protocol. HARS'access control uses IPsec functions to access to data collection andan attacker could conduct a man in the middle attack on IPSec communication after mastering apreshared key. After a succesfull attack, the opponent could also decrypt the data packet and tamper with the content of the data packet, destroying the confidentiality and authentication of the protocol [16]. Also, the malicious entity could mislead the victim (data collection mechanism) into believing that the IPsec session cannot be initiated at the other end. This leads to messages being forwarded explicitly if the host is operating in reset mode.
- Degradation attack: The entities in a HAR system communicate each other via channels that use specific security protocols. An attacker could force the entities

to use low-security features degrading the protocol level of communication. This attack can be used against Secure Shell Protocol (SSH), IPsec, and Point-to-Point Tunneling Protocol (PPTP). Some examples of degradation attacks are the following: 1) SSH V1 instead of SSH V2: the malicious entity modifies the connection parameters between the communicating parties. The attacker can force the data collection mechanism to start an SSH1 session instead of SSH2 by changing version number 1.99 to 1.51.2) PPTP: at the stage of negotiating the PPTP session configuration, the attacker can force the victim to use the least secure Password Authentication Protocol (PAP), Microsoft version of the Challenge-Handshake Authentication Protocol -MSCHAP V1 (i.e., ”revert” from MSCHAP V2 to version 1), or not use any encryption at all. The attacker can force his victim to repeat the PPTP session configuration negotiation step (send a Terminate-Ack packet), steal the password from the existing tunnel, and repeat the attack.

- SSL hijacking: This attack exploits validation vulnerabilities. When the user needs to access to the HAR system he has to validate his credentials during the Transmission Control Protocol (TCP) handshake. The attacker redirects the HTTPS (Hypertext Transfer Protocol Secure) connection as a HTTP connection, so that the credential information is passed as plain text from the user to the attacker. Passing fake authentication keys to both the user and the application during a TCP handshake creates seemingly a secure connection when, in fact, the malicious entity controls the entire session.

To withstand the above weaknesses cryptographic protocols are designed to provide communication security and are part of Transport Layer Security (TLS). These protocols use X.509 for authentication, an ITU (International Telecommunication Union) standard defining the format of public key certificates using digital signatures [15]. More specifically, the HTTPS is designed for the exchange ofkeys during the TLS handshake process and uses the Diffie-Hellman key exchange protocol. This method requires the messages exchanged to be signed with the private keys of the communicating entities, due to the RSA public key algorithm, and also the use of certificates to obtain the correct public keys. Thus, even if a certificate has been forged to correspond to a legitimate entity, the signature cannot be verified and the request will be rejected. Therefore, this method ensures that in case the communication is intercepted by a third entity, it cannot be decrypted by that entity.

IV. Design Considerations for HARS

As we mentioned in section A, a HARS must ensure confidentiality and integrity of shared health data, so it should consist of strong encryption procedures and authentication methods. This could be achieved by using Public Key Infrastructure (PKI) and symmetric encryption as well as to preserve the privacy of involved participants such as event data by employing data anonymization or pseudonymization techniques. In the HARS, the transmitted and stored data should be encrypted and signed. Similarly, we propose the use of strong authentication mechanisms like PKI singing methods. The singing scheme could be based on the Elliptic Curve Digital Signature Algorithm (ECDSA) and as the hash function we propose the Hash-based Message Authentication Code (HMAC) function. Along with the involvement of multiple parties/servers, we increase the difficulty of the man in the middle attack to occur, since the decryption of data will require further communication with multiple servers that will provide part of the decryption key. Besides, the authentication of new users/devices each device should obtain a unique key which it will receive from multiple servers, in order to fragment the process.

As we mentioned, the use of digital signature determines the identity of the entity that signs and is linked to the data it refers to, making it possible to detect a later modification or alteration of them. To create the digital signature, the following procedure required [17]: the user generates a digest of the message. The digest is then encrypted using the user's private key, not Data Collection Mechanism's. The encrypted digest along with the information of the digest algorithm constitutes the digital signature of the message. Finally, the digital signature is sent with the original message to data collection mechanism. Data collection mechanism checks whether the message has been modified by a third party by decrypting the signature with the public key and then comparing the messages.

We remark that adding public key encryption to the digital signature process provides a system with the security requirements mentioned in section A. Authentication of the signing entity, as the signature is created with his private key exclusively. Authentication of the message through the decryption of the signature associated with the message.Non-repudiation which is the use of the signature to resolve disputes. The user, by creating the signature with the help of his private key, completes a process with legal consequences and should be able to verify his signature. Data integrity since the signature verification fails and the receiver safely discards the message if the data is modified.

Furthermore, by using multi-party signing we can ensure that no data gets into the wrong hands since we fragment the authentication across multiple servers. This way if a device intercepts the data it will need further credentials to enter the network. More specifically, if a user wants to register on the platform, or access the data, he is logging in through a mobile device that does not follow appropriate security protocols. servers will come to the forefront to protect the platform from one-to-one connections which are the most risky. The data is encrypted and signed, in order to provide data secrecy and authenticate the transmitted messages and involved parties. Users communicate with the edge server through PKI, as we already mentioned. A completely isolated (offline) Certification Authority (CA) generates certificates for the edge server. The edge server acts as a Registration authority and accepts requests from users in order to create their certificates (the certificates will be distributed via OAuth2.0 as described in detail below).

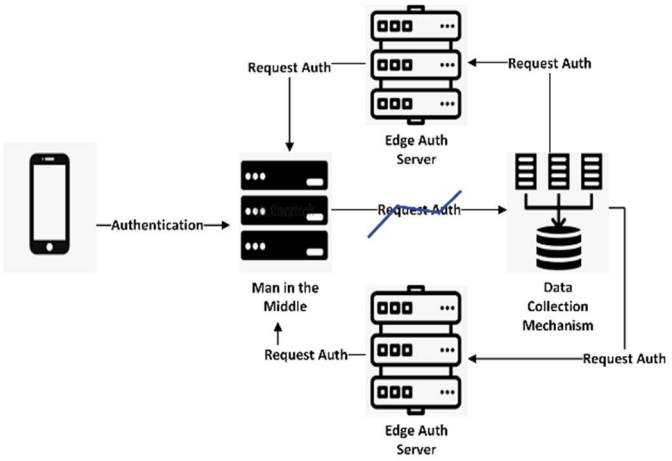

Fig. 2. Edge Architecture

We notice that if a mobile device that wants to authenticate falls victim to a man in the middle and sends data as well as its original key, then the malicious device will try to connect to the data collection mechanism. The data collection mechanism will request authentication from the edge servers and then they will ask the malicious device to provide the next keys to continue communication. So, when the authentication of the user is done involving multiple parties/servers then it will be difficult for a man in the middle attacker, since the new device will not be able to modify the data that the client sends to the server, as it is designed to detect intentional modifications.

V. The Initialization of OAuth2.0 Protocol

Figure 3 shows the authentication steps of the basic assets of a HAR using the OAuth2.0 protocol. The numbers distinguish the series of actions. We place these steps in the order of their execution starting with how the keys and certificates are generated. Next, we describe the process of the registration, how mutual authentication is performed, and howthe keys are shared between the entities. Finally, we mention how certificates are issued and how secure communication between them is achieved. We present the total of the steps as detailed below.

Initially, in step 1 there is the key generation. The private key, unlike the public key, is never transferred between entities. In each entity, we should store the specific key and take care of its security. In step 2, the certification is created and in step 3 the auth server certificate registration takes place. The data collection mechanism sends registration information to auth server. In step 5 the auth server registers data collection mechanism and sends him an ID. Thereafter in step 6, we have the mutual TLS between the data collection mechanism and auth server. The data collection mechanism presents to auth server the X.509 certification and the public key. The auth server does the same with data collection mechanism. In the next step, the data collection mechanism requires token from authserver to access to the protected resource. The auth server sends the access token to the data collection mechanism. Also, hashes the certification that the data collection mechanism has presented and integrates it into the access token. The next step is the data collection mechanism certificate registration. Then, we have mutual TLS between data collection mechanism and ML Service. Data collection mechanism uses the same certification and the same public key which had presented to auth server. ML Service presents the X.509 certification and his public key to data collection mechanism. Finally, the data collection mechanism presents the access token to authserver. In step 12 the ML Service communicates with authserver to verify the hash of the certification. In step 13 the token information is returned. In the end, the ML Service returns the information (e.g. the activity) to data collection mechanism if and only if the hash of the certification in the access token goes along with the hash presented by data collection mechanism during the mutual TLS process.

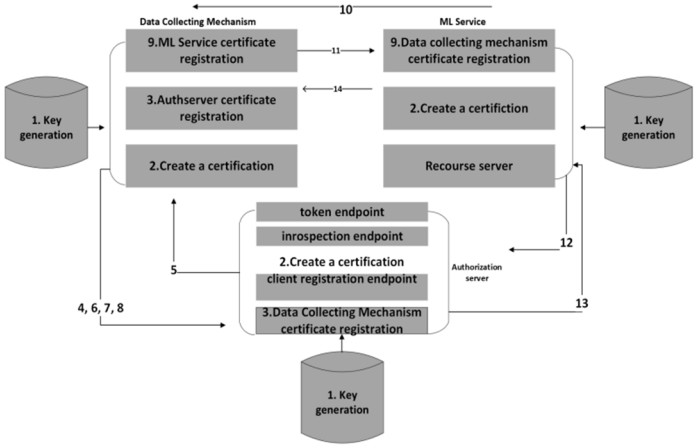

Fig.3: OAuth2.0 Authentication Scheme for HARS

VI. Related Work

There are very few attempts in the literature to address privacy issue in HARS, the majority try to solve the privacy violation by the learning procedure ([18], [19], [21], [22], [23], [24], [25], [26]) or to protect a specific component like databases by using cryptographic mechanisms ([27],[28]). In addition to the discussed malicious actions/attacks that could be performed by unauthorized users against privacy-confidentiality and integrity properties, there are also cases where an authorized user, e.g. another doctor or nurse, could see a patient's data. We believe that the use of Privacy enhancing technologies (PETs [29]) provide an identity-based management scheme in HARS via internet providers, smartphones, and the cloud, and it can be applied to all components of our architecture (see Fig.1). Privacy attribute-based credentials (P-ABCs [30]) that allow users to disclose certified information, minimally authenticating with online service providers can provide an identity management scheme for authenticating the actions of all actors of HARS. PET technology could be used for utilizing centralized identity management schemes for providing trust mechanisms. Blockchain technology could also preserve user's privacy by providing a distributed trust management scheme. We plan to deploy an already identity management scheme that is based on blockchain technology ([31],[32]) for providing an access control system and data sharing policies to the already operated HARS system.

VII.CONCLUSION

In this work, we propose a paper, whereby a security flaw has been identified in a complete medical IoT application using wearable devices and smart sensors. This work aims to utilize edge network devices to prevent attacks from the mobile application to the data collection mechanism IoT cloud platform and provides a method for defending against security flaws. As such we are giving a brief description of the ongoing work. In future work, we aim to put our suggestion to the test and propose methods that can recognize and deal with a number of attacks.

ACKNOWLEDGMENT

This research work is funded by the Operational Programme "Epirus" 2014-2020, under the project "Integrated Support System for elderly people with health problems and lonely workers using Portable Devices and Machine learning Algorithms – TrackMyHealth", Co-financed by the European Regional Development Fund (ERDF).

REFERENCES

[1] "S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna,M. Hassan, and A. Seneviratne, “A survey of wearable devices and challenges,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2573–2620, 2017."

[2] "R. R. Selmic, V. V. Phoha, and A. Serwadda, Wireless Sensor Networks. Springer, 2016.".

[3] "R. Bavithra, “Mitm attacks through arp poisoning.” ".

[4] "Haris, M., Haddadi, H. and Hui, P. 2014. Privacy leakage in mobile computing: tools, methods, and characteristics, available at: https://arxiv.org/ abs/1410.4978.".

[5] "X. Liu et al., "Privacy and Security Issues in Deep Learning: A Survey," in IEEE Access, vol. 9, pp. 4566-4593, 2021, doi: 10.1109/ACCESS.2020.3045078".

[6] "W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, “Blockchain-based reliable and efficient certificateless signature for iiot devices,” IEEE transactions on industrial informatics, 2021."

[7] "G. Gómez, E. Espina, J. Armas-Aguirre, and J. M. M. Molina, “Cybersecurity architecture functional model for cyber risk reduction in iot based wearable devices,” in 2021 Congreso Internacional de Innovacio´n y Tendencias en Ingenierıa ".

[8] "M. Haghi, K. Thurow, and R. Stoll, “Wearable devices in medical internet of things: scientific research and commercially available devices,” Healthcare informatics research, vol. 23, no. 1, pp. 4–15, 2017."

[9] "D. Ravi, C. Wong, B. Lo, and G. Z Yang, “A deep learning approach to on-node sensor data analytics for mobile or wearable devices,” IEEE journal of biomedical and health informatics, vol. 21, no. 1, pp. 56–64, 2016.View at: Publisher Site | Google Scholar"."

[10] "Gupta, N., Gupta, S.K., Pathak, R.K. et al. Human activity recognition in artificial intelligence framework: a narrative review. Artif Intell Rev (2022). https://doi.org/10.1007/s10462-021-10116-x".

[11] "Integrated Support System for elderly people with health problems and lonely workers using Portable Devices and Machine learning Algorithms – TrackMyHealth", Co-financed by the European Regional Development Fund (ERDF).

[12] "Jung, Im. (2020). A review of privacy-preserving human and human activity recognition. International Journal on Smart Sensing and Intelligent Systems. 13. 1-13. 10.21307/ijssis-2020-008."

[13] "Ching, Ke & Mahinderjit Singh, Manmeet (Mandy). (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. International Journal of Network Security & Its Applications. 8. 19-30. 10.5121/ijnsa.2016.8302".

[14] "A. Mallik, “Man-in-the-middle-attack: Understanding in simple words,” Cyberspace: Jurnal Pendidikan Teknologi Informasi, vol. 2, no. 2, pp. 109–134, 2019."

[15] "Gangan, Subodh. “A Review of Man-in-the-Middle Attacks.” ArXiv abs/1504.02115 (2015): n. pag.".

[16] Yunxiao Sun, Bailing Wang, Hongri Liu, Yuliang Wei, Di Wu, Jing Wang, "Detecting IKEv1 Man-in-the-Middle Attack with Message-RTT Analysis", Wireless Communications and Mobile Computing, vol. 2022, Article ID 2605684, 7 pages, 2022. https://doi.org/10.1155.

[17] "J. Chandrashekhara and ., Anu V B and ., Prabhavathi H and ., Ramya B R, A Comprehensive Study on Digital Signature (MAY 20, 2021). International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-9, Issue-3, May 2021 https://doi.org/10.21276/ijircst.2021.9.3.7 Article ID IRP1149, Pages 43-47 www.ijircst.org, Available at SSRN: https://ssrn.com/abstract=3879974.)".

[18] "N. Phan, Y. Wang, X. Wu and D. Dou, "Differential privacy preservation for deep auto-encoders: an application of human behavior prediction," 2016.".

[19] "M. Bun and T. Steinke, "Concentrated differential privacy: Simplifications, extensions, and lower bounds," 2016.".

[20] "H. Ajakan, P. Germain, H. Larochelle, F. Laviolette and M. Marchand, "Domain-adversarial neural networks," arXiv preprint arXiv:1412.4446, 2014.".

[21] "Y. Iwasawa, K. Nakayama, I. Yairi and Y. Matsuo, "Privacy Issues Regarding the Application of DNNs to Activity-Recognition using Wearables and Its Countermeasures by Use of Adversarial Training.," 2017.".

[22] "H. Edwards and A. Storkey, "Censoring representations with an adversary," arXiv preprint arXiv:1511.05897, 2015.".

[23] "M. Malekzadeh, R. G. Clegg, A. Cavallaro and H. Haddadi, "Protecting sensory data against sensitive inferences," 2018.".

[24] "S. A. Osia, A. Taheri, A. S. Shamsabadi, K. Katevas, H. Haddadi and H. R. Rabiee, "Deep private-feature extraction," IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 1, pp. 54-66, 2018.".

[25] "M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar and L. Zhang, "Deep learning with differential privacy," 2016.".

[26] "N. Papernot, M. Abadi, U. Erlingsson, I. Goodfellow and K. Talwar, "Semi-supervised knowledge transfer for deep learning from private training data," arXiv preprint arXiv:1610.05755, 2016.".

[27] "R. Wang, F. Chen, Z. Chen, T. Li, G. Harari, S. Tignor, X. Zhou, D. Ben-Zeev and A. T. Campbell, "StudentLife: assessing mental health, academic performance and behavioral trends of college students using smartphones," 2014.".

[28] "M. Juuti, S. Szyller, S. Marchal and N. Asokan, "PRADA: protecting against DNN model stealing attacks," 2019.".

[29] "J. Camenisch, "Identity management tools for protecting online privacy," 2011.".

[30] "K. Rannenberg, J. Camenisch and A. Sabouri, "Attribute-based credentials for trust," Identity in the Information Society, Springer, 2015.".

[31] "J. B. Bernabe, J. García-Rodríguez, S. Krenn, V. Liagkou, A. Skarmeta and R. Torres, "Privacy-Preserving Identity Management and Applications to Academic Degree Verification," 2022.".

[32] "V. Liagkou, A. Skarmeta and R. Torres, "Privacy-Preserving Identity Management and Applications to Academic Degree Verification," Privacy and Identity Management , p. 33, 2022.".