Authentication in the Internet of Medical Things

Subjects: Computer Science, Information Systems

Contributor: Norah Alsaeed , Farrukh Nadeem

The Internet of Medical Things (IoMT) has revolutionized the world of healthcare by remotely connecting patients to healthcare providers through medical devices connected over the Internet. IoMT devices collect patients' medical data and share them with healthcare providers, who analyze it for early control of diseases. The security of patients' data is of prime importance in IoMT. Authentication of users and devices is the first layer of security in IoMT.

Internet of Medical Things | security requirements | IoMT authentication scheme

1. Introduction

The current COVID-19 epidemic has again highlighted the importance of smart healthcare services that offer prevention, diagnosis, and treatment at a distance. Smart healthcare is not simply a technology improvement rather it provides multi-level and global changes in the healthcare arena. The smart healthcare is built around emerging technologies, such as cloud computing, Internet of Things (IoT), machine learning, and big data [1]. IoT has become an essential component to fulfill the connectivity requirements of the current smart healthcare systems. IoT, in the healthcare context, is called the Internet of Medical Things (IoMT). IoMT comprises medical devices connected to patients to sense their medical parameters and share that information with healthcare staff so that they may provide remote healthcare services. The IoMT security is an imperative need worthy of more research due to the need to safeguard the patient's sensitive information from exploitation [2]. To avoid such exploitation, and to ensure a high level of security, IoMT applications must maintain strict authentication schemes that prevent unauthorized access to patients' data, as well as the IoMT resources, and protect the entire system from various types of attacks [3][4]. Developing a strict authentication scheme within the IoMT context is challenging for three main reasons. First, IoMT devices are resource-constrained and cannot handle intensive computational and complex authentication procedures. Second, various IoMT products and vendors work through different platforms and protocols. Consequently, developing strict authentication requires deep knowledge of how different products, platforms, and protocols collectively work. Third, highly distributed IoMT devices that share medical data through the Internet make IoMT systems intrinsically prone to security violations.

1.1. Smart Healthcare

The evolution of technologies contributes to the high quality of services in the healthcare sector as patients receive faster and more personalized services [5]. Smart healthcare, or healthcare 4.0, is an intelligent healthcare asset

that uses sensing devices to gather medical data, network devices to transmit data, and an advanced infrastructure to process, store, and display that data for enhancing healthcare services. In summary, smart healthcare involves the use of cutting-edge technologies to increase the effectiveness of medical assistance and, where possible, to decrease healthcare costs. Smart healthcare provides significant capabilities, such as continuous interaction between all the relevant parties in healthcare, helping the healthcare providers make knowledgeable decisions, and supporting the dynamic allocation of healthcare resources. In short, today's healthcare services need to be personalized and available anytime, anywhere, and for everyone. This goal is met through smart healthcare [1].

1.2. IoT in Smart Healthcare

In its basic form, IoT connects physical objects to the Internet to perform related activities remotely. This connection provided features such as context-awareness capabilities, autonomous data capture, and on-line communication facilities for a specific purpose. In particular, IoMT refers to smart medical devices connected via the Internet to a central entity, usually a cloud, to automatically gather, process, and share medical data for healthcare services [6].

Smart healthcare requires the IoT paradigm to provide solutions that can capture patients' health parameters, recognize symptoms, and thus recommend preventive actions. On the other hand, IoMT applications help the healthcare industry to design and develop new medical solutions based on big data analytics that use the data generated from IoMT devices, and to take other knowledge-based measures as needed. Patients, healthcare providers, such as doctors, nurses, pharmacists, physicians, and hospitals, as well as insurance companies, can benefit directly or indirectly from IoMT applications. IoMT applications are helpful for many healthcare areas, such as remote healthcare services, medical asset management, optimization of medical inventory, patient-doctor rapport, real-time medical data analytics, augmented surgeries, and treatment [4].

1.3. IoMT Context

This section presents the overall context of IoMT systems. It includes the IoMT system architecture and the way its layers are integrated to perform tasks remotely. Moreover, the IoMT context discusses some applications related to IoMT systems. At the end, it briefly classifies the IoMT devices and describes their functions.

1.3.1. IoMT Architecture

Figure 1 illustrates the IoMT layers. The IoMT architecture operates mainly through four layers [7], as described below.

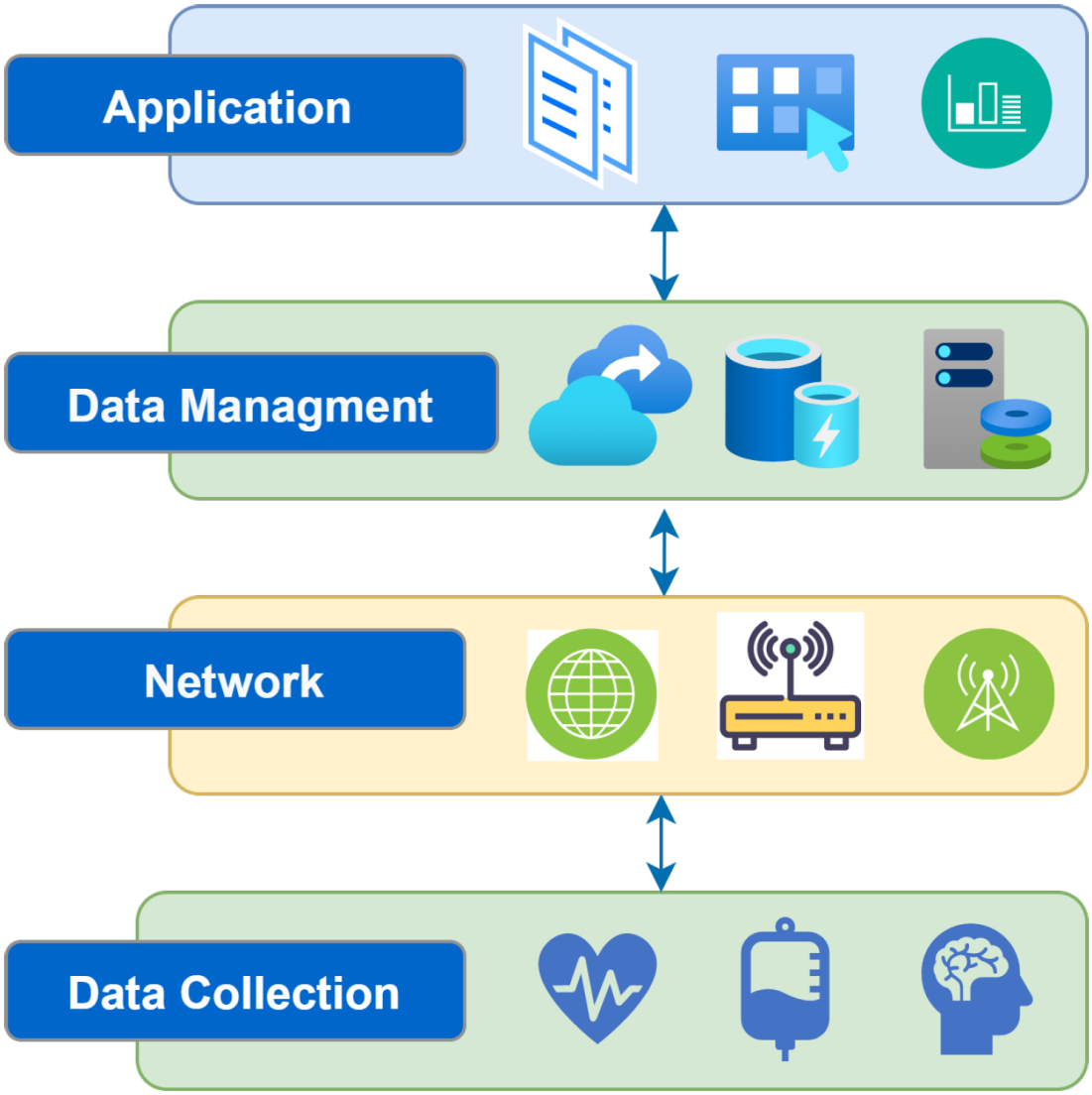

Figure 1. IoMT system architecture.

1.3.2. IoMT Applications

With rapid technological advancement, the various IoMT applications are exponentially increasing. Hundreds of applications are available for IoMT systems. These applications can be categorized as shown in **Figure 2** [4]:

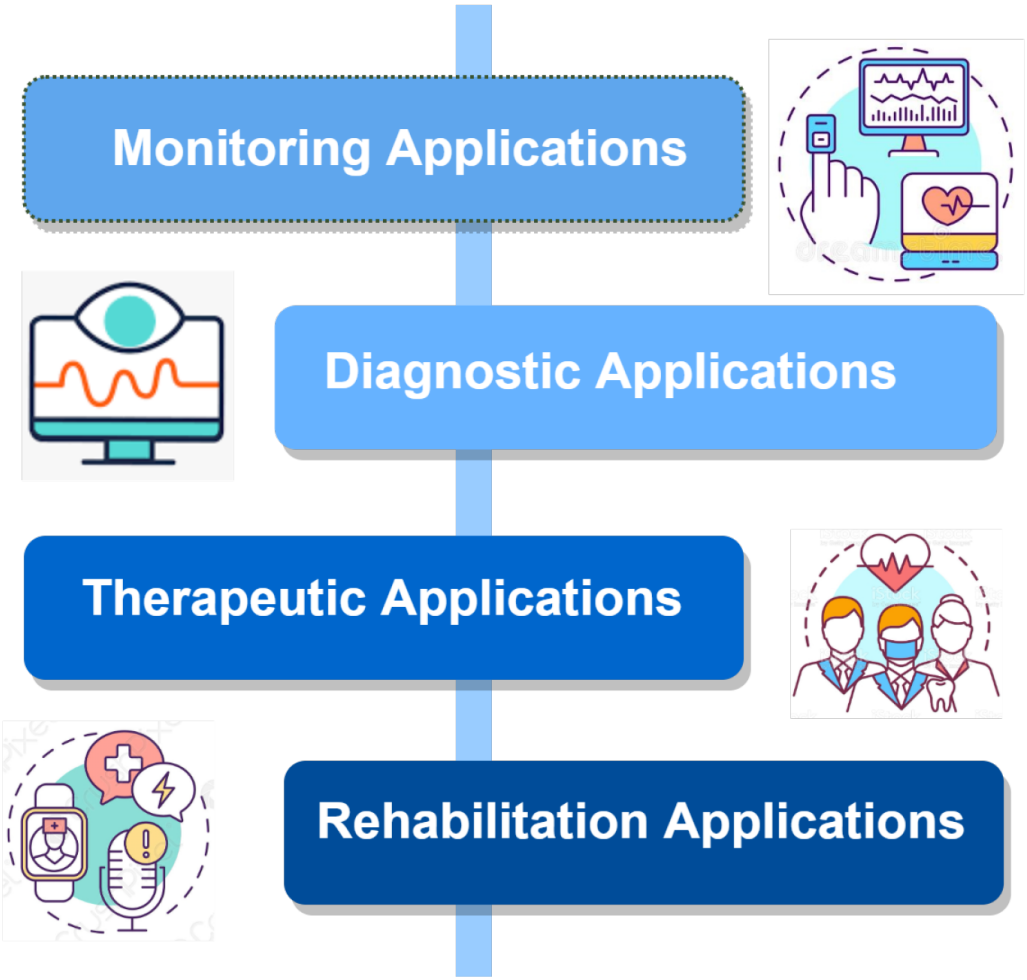

Figure 2. IoMT applications.

1.3.3. IoMT Devices

D. Hemanth et al. [7] classified IoMT devices according to their position, such as in-community, in-hospital, in-clinic, in-home, and onbody devices. In this paper, IoMT devices are classified according to their distance from patients, as shown in **Figure 3** [8][9][10]:

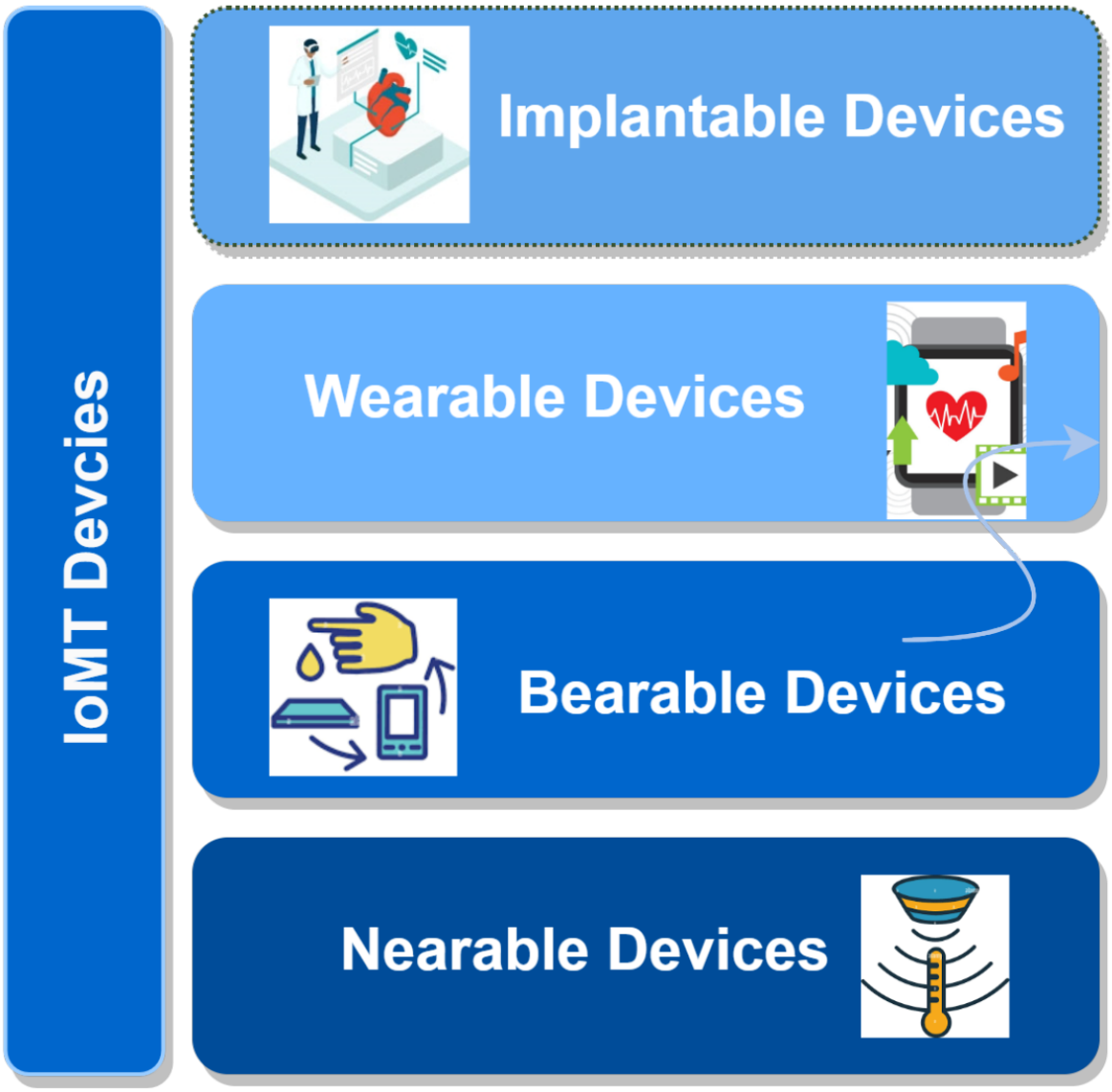

Figure 3. IoMT devices.

1.4. IoMT Security Requirements

The security requirements of the IoMT are divided into three levels: information security, function security, and access control, as illustrated in **Figure 4**. It is worth mentioning that the security requirements are interlinked and affected by each other [3]. The security requirements at these three levels are described as is detailed in the following section.

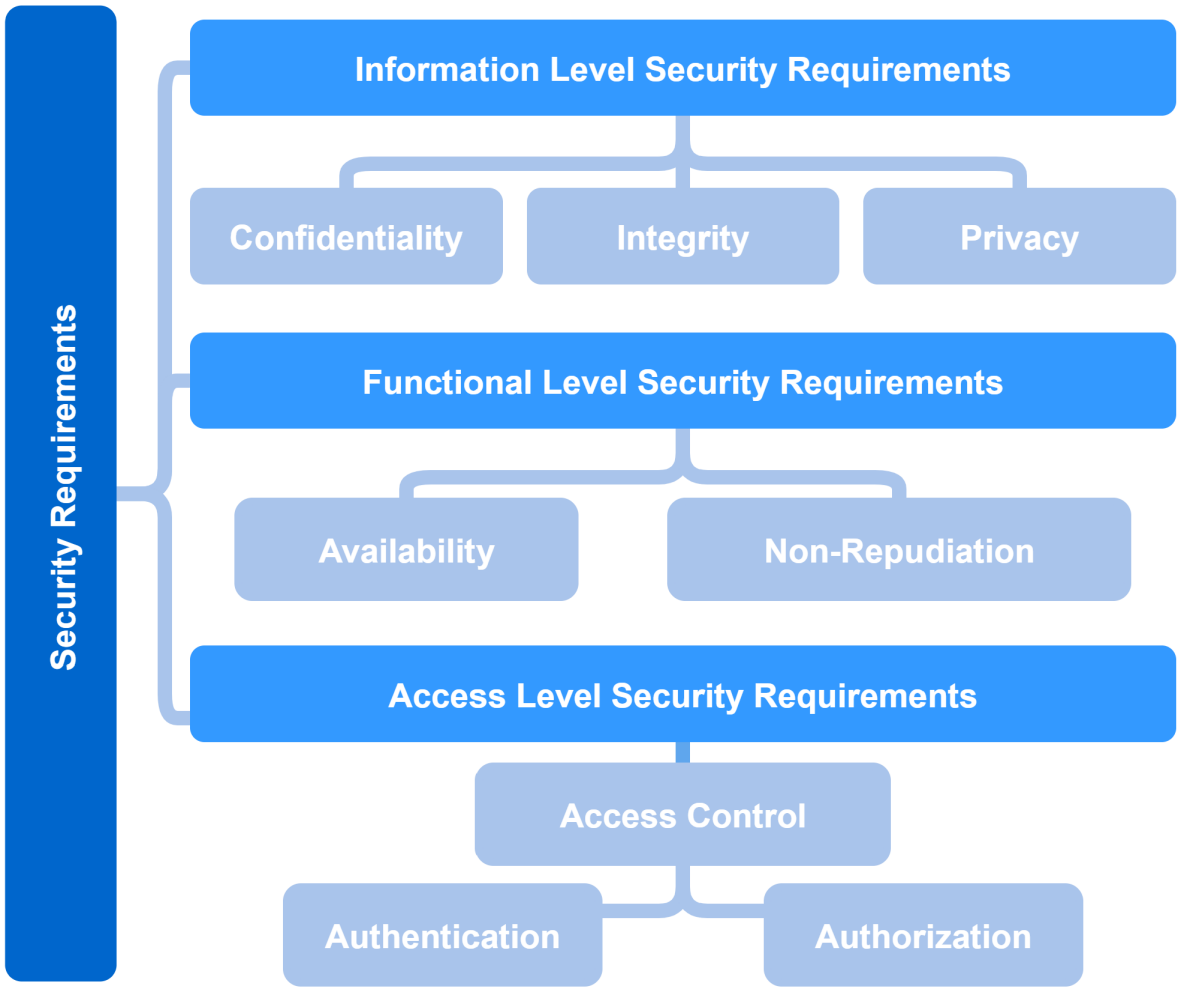

Figure 4. Levels of security requirements.

2. IoMT Authentication Taxonomy

IoMT authentication can be viewed from different perspectives. **Figure 5** illustrates the IoMT authentication taxonomy's perspectives: authentication levels, architectures, credentials, procedures, categories, schemes, and preventing attacks. The perspectives are described in the following sections.

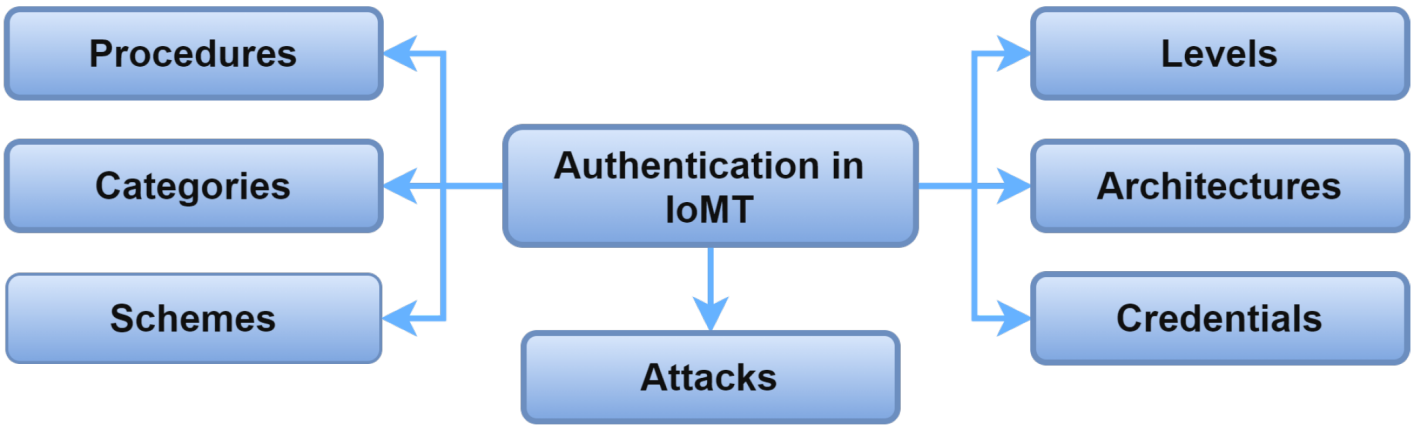

Figure 5. Taxonomy of authentication in IoMT.

2.1. Authentication Levels

Because IoMT systems are complex and distributed, it is challenging to propose generic authentication solutions for various IoMT systems nodes. Therefore, IoMT authentication is primarily considered at three levels: device-level, user-level, and network-level, as shown in **Figure 6**.

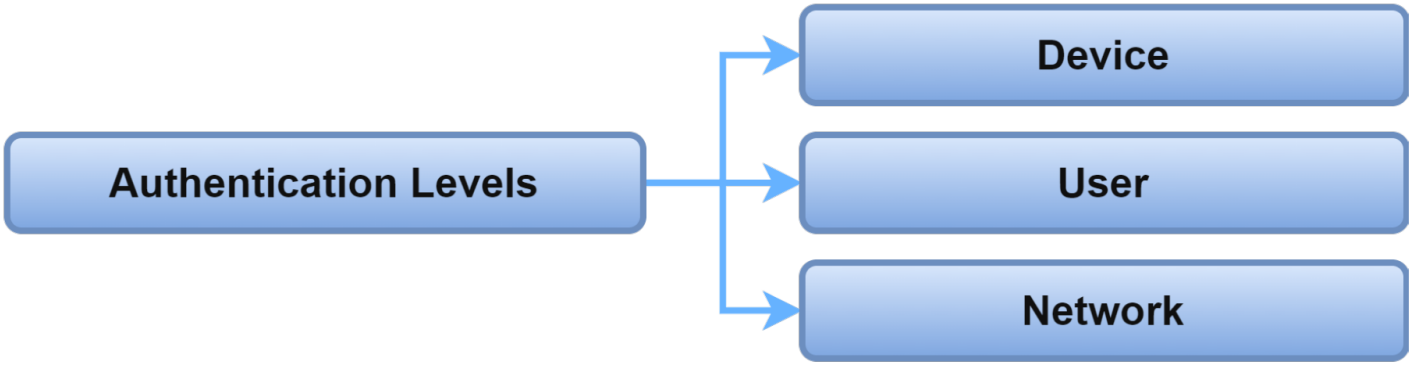

Figure 6. Authentication levels.

2.2. Authentication Architectures

Authentication in IoMT systems depends on either a centralized or decentralized architecture. Centralized authentication requires a centralized server to identify and authenticate the system entities. In contrast, the distributed architecture depends on multiple distributed nodes to accomplish the authentication process. Both the centralized and distributed architecture can be a flat or multi-level architecture. The flat architecture means the nodes are authenticated by authentication servers with the same roles. In a multi-level architecture, the authentication process is performed by authentication servers with different roles, according to their level of communication. That implies that the server at the lower level is used for authenticating nodes at the lower level. **Figure 7** shows the authentication architectures for IoMT systems.

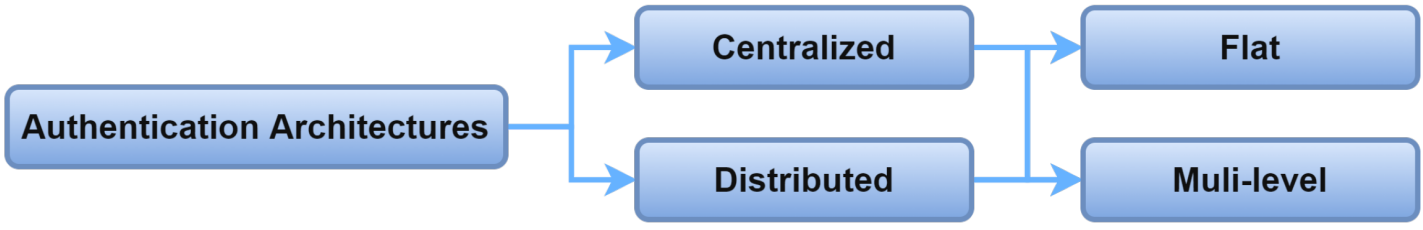

Figure 7. Authentication architectures.

2.3. Authentication Credentials

The authentication process asks for unique credentials from the entities to allow them to access the IoMT systems. This process can be performed through a third, trusted, party or directly between the communicating entities.

Whatever the credentials used, it is necessary to consider their uniqueness, universality, and storability [11]. The credentials required for authentication are classified into four categories [12]. These types are depicted in **Figure 8**.

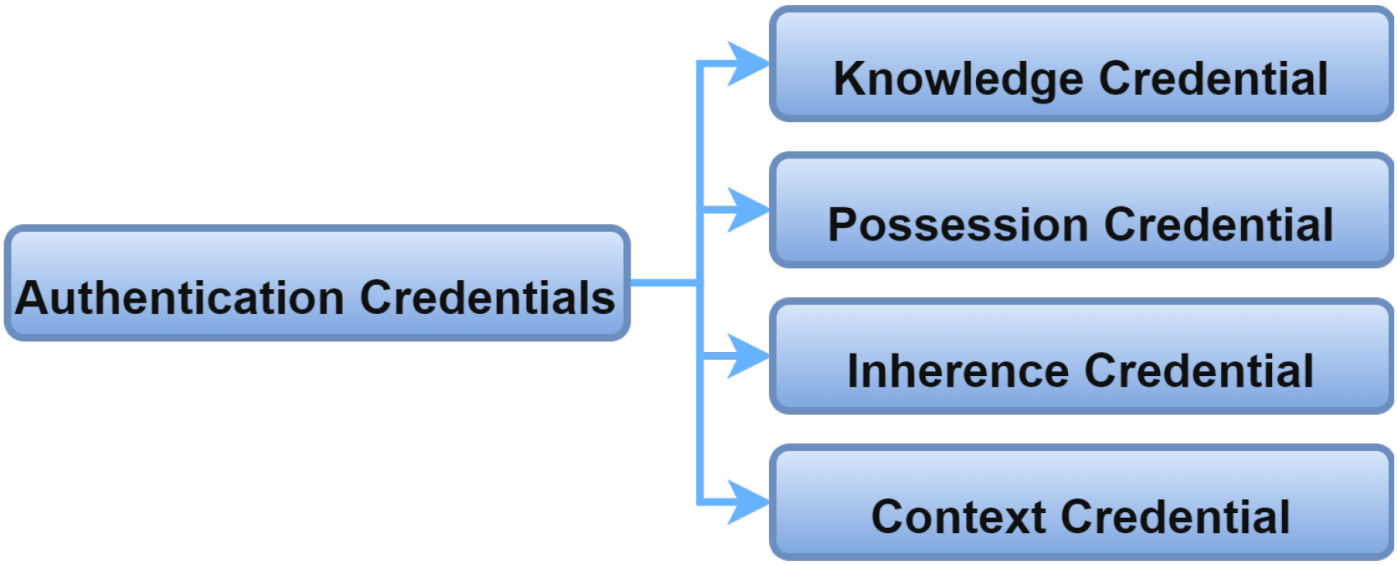

Figure 8. Authentication credentials.

2.4. Authentication Procedures

The authentication in IoMT systems can be classified based on the direction of authenticating entities. The authentication procedure in the IoMT system can be one-way, two-way, and three-way [13]. **Figure 9** shows the authentication procedure in the IoMT system.

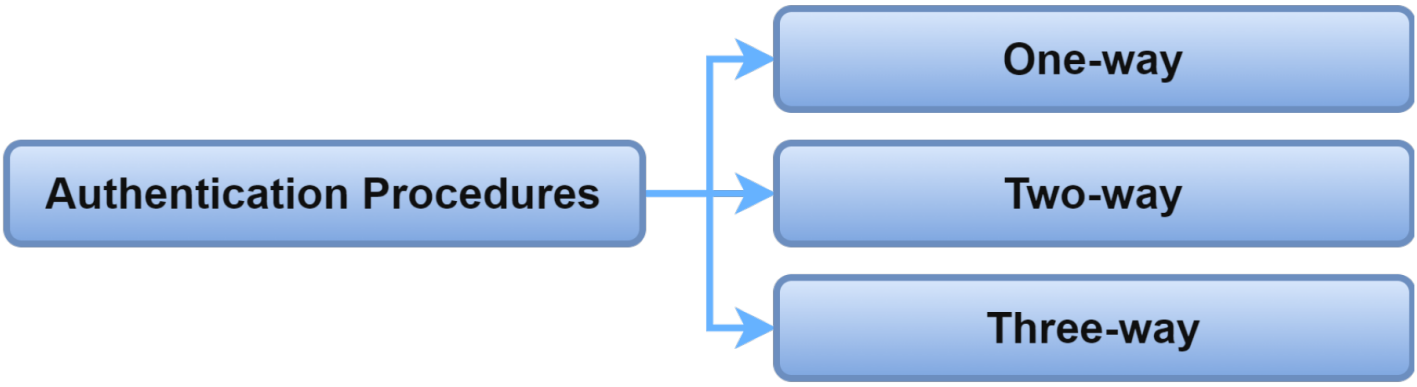

Figure 9. Authentication procedures.

2.5. Authentication Categories

The IoMT systems need a continuous feed of data from IoMT to look after the patient's situation. Accordingly, the IoMT systems need to authenticate those devices for a long period of time. IoMT authentication is classified into continuous and static from that perspective shown in **Figure 10**.

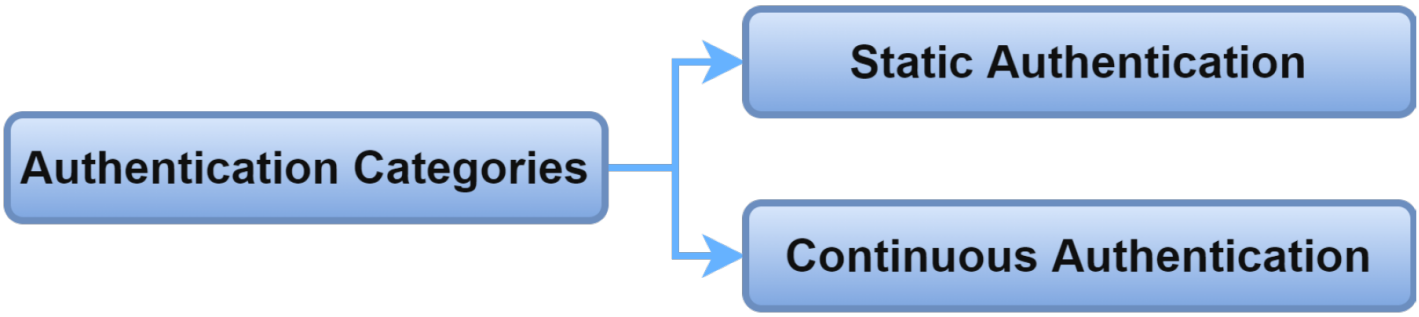

Figure 10. Authentication categories.

2.6. Authentication Schemes

Authentication in IoMT systems can depend on a basic, key-based, certificate-based, or cryptography-based scheme. Researchers have recently adopted hybrid schemes to improve system performance and security. **Figure 11** shows a classification of authentication schemes.

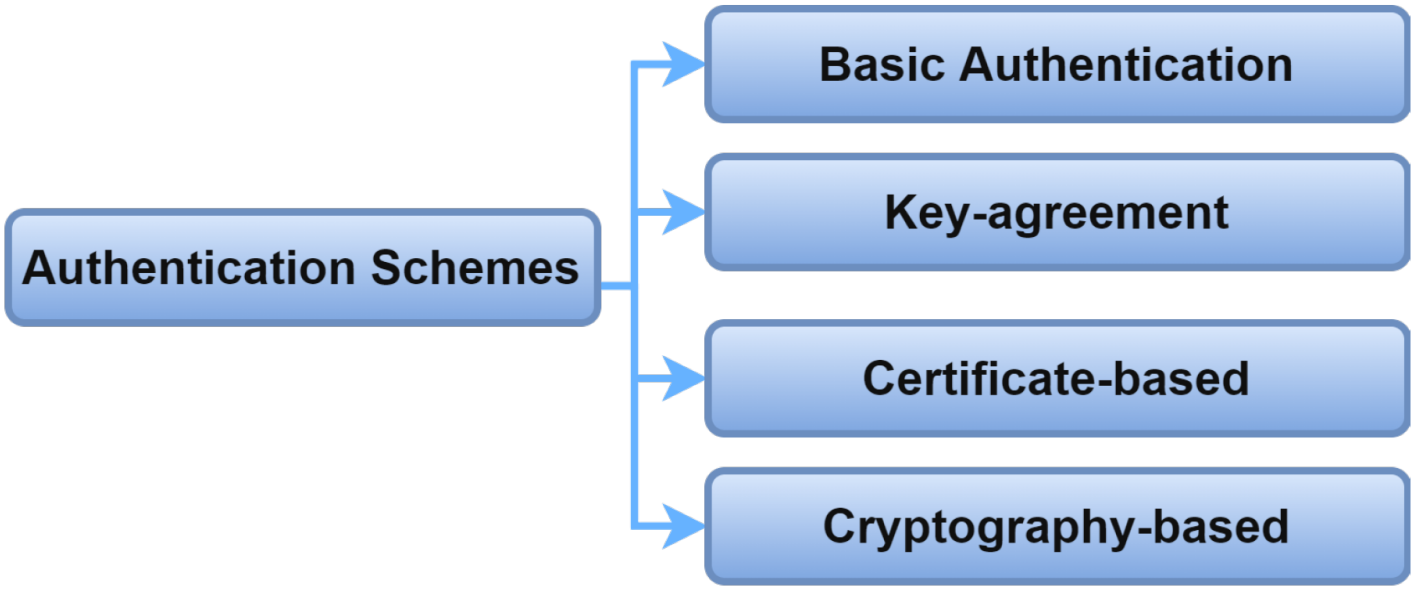

Figure 11. Authentication schemes.

2.6.1. Basic Authentication

In basic authentication, the credentials used to authenticate an entity are the factors used to identify that entity. The accuracy and efficiency of the authentication schemes will rely on how many factors are required to perform the authentication process. **Figure 12** shows a classification of authentication schemes according to the number of factors involved in identifying entities for the IoMT systems. Usually, two factors are used for basic authentication; entities need to provide identification data and biometric information to access the IoMT system [14][15]. To enhance the security and make the problem of authentication harder for adversaries to compromise, many schemes depend on three factors by combining knowledge, inheritance, and possession credentials [16][17][18][19][20][21].

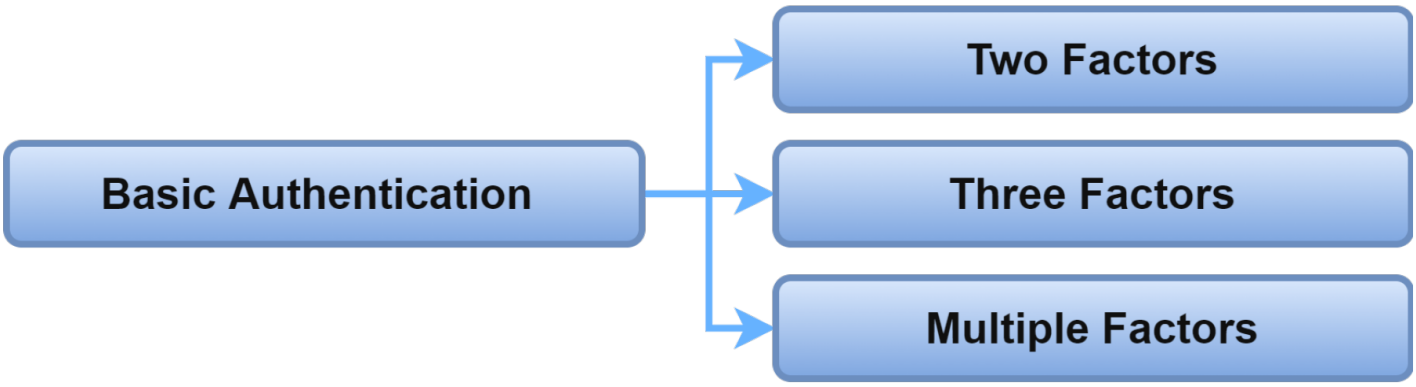

Figure 12. Basic Authentication.

2.6.2. Authentication and Key Agreement

IoMT authentication can be achieved by creating a key shared between the communicating entities to ensure secure communication. Authentication protocols can adopt a simple key agreement where two entities negotiate upon a key to secure their communication [22][23]. G. Mwitende et al. [24] proposed a key agreement between two entities with a blind signing mechanism based on blockchain technology. On the other hand, authentication protocols can adopt a group key agreement [25][26]. Group-key agreement protocols require more than two entities to generate a group-key such that anyone of these entities can use it for communication [24]. **Figure 13**a shows the key agreement classification.

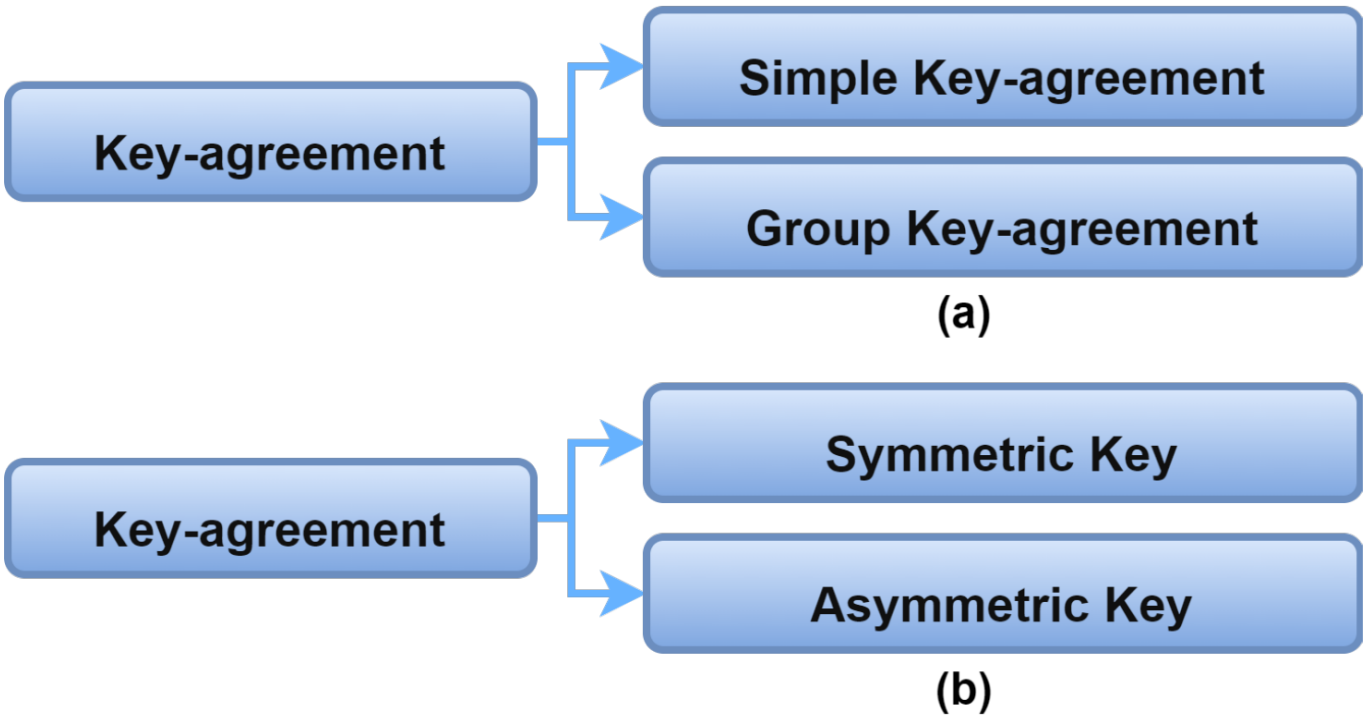

Figure 13. (**a**,**b**) Key agreement scheme.

2.6.3. Certificate-Based Authentication

The authentication schema in IoMT can depend on using a certificate to identify legitimate entities. Accordingly, authentication schemes may require a hard certificate, soft certificate, implicit certificate, or no certificate for identifying entities, see **Figure 14**. Most of the authentication literature in the IoMT environment suggests a hard certificate to accomplish the authentication process. A smart card is a hard certificate used to authenticate users in the IoMT system [27][28]. Similarly, an RFID chip is used to authenticate IoMT devices uniquely by providing it as a device identifier [29][30][31][32]. A hard certificate also requires to be validated and signed by a reliable party. The second type of certificate is a soft certificate, or a digital certificate that refers to a token that requires to be validated by a reliable party [33][34]. The reliable party is called a certificate authority (CA) or a delegated entity.

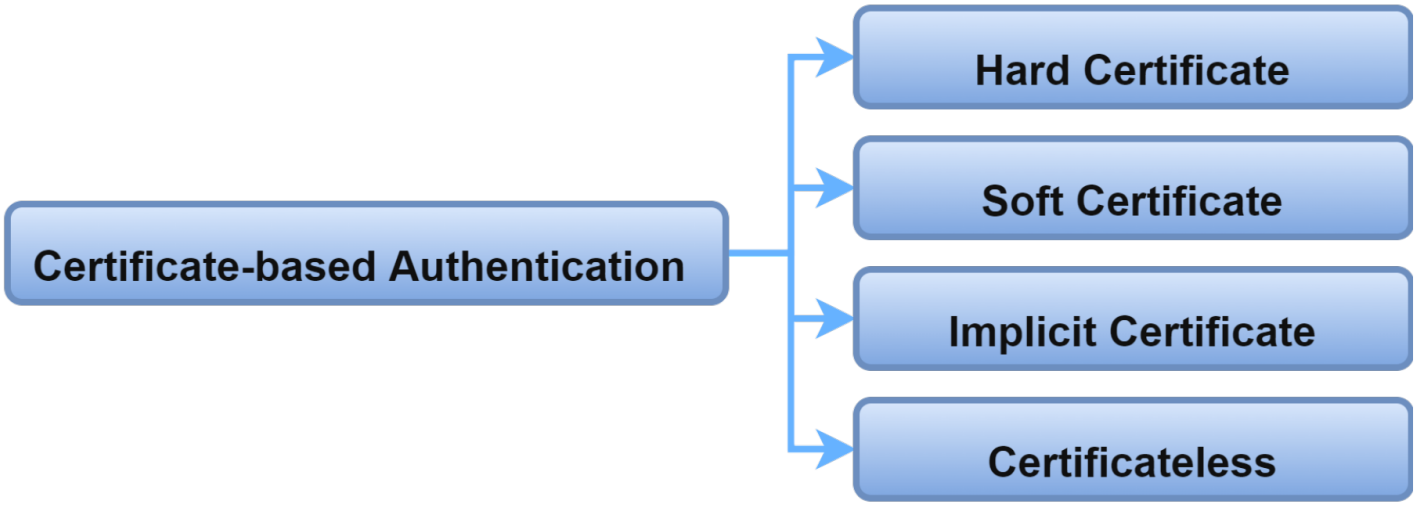

Figure 14. Certificate-based authentication.

2.6.4. Cryptography-Based Authentication

Currently, cryptography is an essential part of authentication, and various cryptography techniques offer a good opportunity to empower IoMT security. **Figure 15** illustrates different cryptographic-based authentication schemes. Cryptographic-based authentication commonly uses a hash function, which is efficient for resource-constrained IoMT devices [35]. H. Khemissa et al. [36] adopted a keyed-hash authentication message code (HMAC) calculated by an iterative hash function such as SHA-1 or MD5.

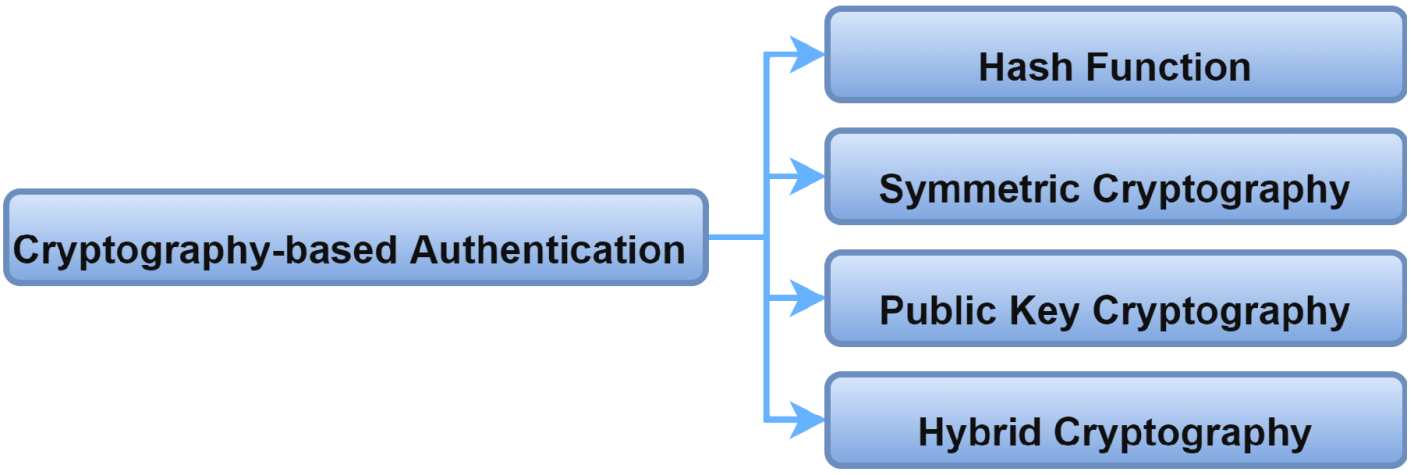

Figure 15. Cryptography-based authentication.

2.7. Authentication Attacks

The main purpose of adopting authentication schemes in IoMT is to ensure that only authorized users and devices are enabled to use system resources and services. Therefore, it is necessary to test the authentication schemes against attacks that succeed in getting unauthorized access to IoMT systems. **Figure 16** shows the widespread attacks used in IoMT authentication. Those attacks are shown as being prevented in different ways in the literature, according to the proposed authentication scheme.

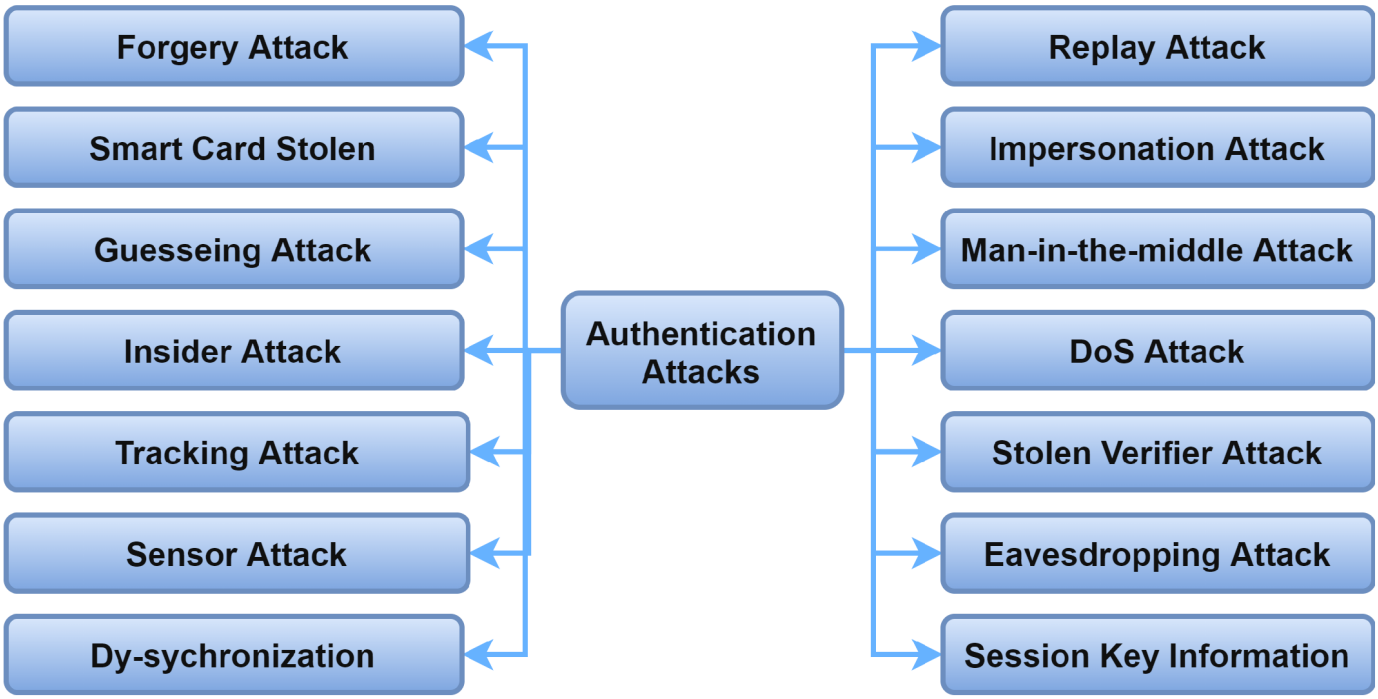

Figure 16. Authentication attacks.

References

1. Mamdouh, M.; Awad, A.I.; Khalaf, A.A.; Hamed, H.F. Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Comput. Secur. 2021, 111, 102491.
2. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. Internet Things 2019, 8, 100123.
3. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th

International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 457–464.

4. Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. IoT Security: Advances in Authentication; John Wiley and Sons: Hoboken, NJ, USA, 2020.
5. Sundaravadivel, P.; Kougianos, E.; Mohanty, S.P.; Ganapathiraju, M.K. Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health. IEEE Consum. Electron. Mag. 2017, 7, 18–28.
6. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. Sensors 2020, 20, 4828.
7. Hemanth, J.A.D.J.; George, A. Internet of Medical Things: Remote Healthcare Systems and Applications; Springer: Berlin/Heidelberg, Germany, 2021.
8. Kumar, T.; Braeken, A.; Jurcut, A.D.; Liyanage, M.; Ylianttila, M. AGE: Authentication in gadget-free healthcare environments. Inf. Technol. Manag. 2019, 21, 95–114.
9. Pradhan, B.; Bhattacharyya, S.; Pal, K. IoT-Based Applications in Healthcare Devices. J. Health Eng. 2021, 2021, 6632599.
10. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9 October 2017; pp. 112–120.
11. Dasgupta, D.; Roy, A.; Nag, A. Advances in User Authentication; Springer: Berlin/Heidelberg, Germany, 2017.
12. Ducray, B. Authentication by Gesture Recognition: A Dynamic Biometric Application Submitted by Royal Holloway; University of London: London, UK, 2017.
13. Science, C. A Survey on the Authentication Techniques in Internet of Things. In Proceedings of the 2020 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 22–23 February 2020.
14. Li, X.; Niu, J.; Karuppiah, M.; Kumari, S.; Wu, F. Secure and Efficient Two-Factor User Authentication Scheme with User Anonymity for Network Based E-Health Care Applications. J. Med. Syst. 2016, 40, 1–12.
15. Karthigaiveni, M.; Indrani, B. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. J. Ambient Intell. Humaniz. Comput. 2019, 1–12.
16. Renuka, K.; Kumari, S.; Li, X. Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare. J. Med. Syst. 2019, 43, 133.

17. Soni, P.; Pal, A.K.; Islam, S.H. An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput. Methods Programs Biomed. 2019, 182, 105054.
18. Das, A.K. A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. Peer-to-Peer Netw. Appl. 2014, 9, 223–244.
19. Shuai, M.; Liu, B.; Yu, N.; Xiong, L. Lightweight and Secure Three-Factor Authentication Scheme for Remote Patient Monitoring Using On-Body Wireless Networks. Secur. Commun. Netw. 2019, 2019, 8145087.
20. Shuai, M.; Yu, N.; Wang, H.; Xiong, L.; Li, Y. A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications. J. Organ. End User Comput. 2021, 33, 1–18.
21. Ali, R.; Pal, A.K.; Kumari, S.; Sangaiah, A.K.; Li, X.; Wu, F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. J. Ambient Intell. Humaniz. Comput. 2018, 1–22.
22. Al-Naji, F.H.; Zagrouba, R. CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things. J. King Saud Univ. -Comput. Inf. Sci. 2020, 34, 2497–2514.
23. Al-Naji, F.H.; Zagrouba, R. A survey on continuous authentication methods in Internet of Things environment. Comput. Commun. 2020, 163, 109–133.
24. Chen, C.-M.; Deng, X.; Gan, W.; Chen, J.; Islam, S.K.H. A secure blockchain-based group key agreement protocol for IoT. J. Supercomput. 2021, 77, 9046–9068.
25. Le, T.-V.; Hsu, C.-L. An Anonymous Key Distribution Scheme for Group Healthcare Services in 5G-Enabled Multi-Server Environments. IEEE Access 2021, 9, 53408–53422.
26. Chen, M.; Lee, T.-F. Anonymous Group-Oriented Time-Bound Key Agreement for Internet of Medical Things in Telemonitoring Using Chaotic Maps. IEEE Internet Things J. 2021, 8, 13939–13949.
27. Deebak, B.D.; Al-Turjman, F. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE J. Sel. Areas Commun. 2020, 39, 346–360.
28. Li, J.; Su, Z.; Guo, D.; Choo, K.-K.R.; Ji, Y. PSL-MAAKA: Provably Secure and Lightweight Mutual Authentication and Key Agreement Protocol for Fully Public Channels in Internet of Medical Things. IEEE Internet Things J. 2021, 8, 13183–13195.
29. Aghili, S.F.; Mala, H.; Kaliyar, P.; Conti, M. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. Futur. Gener. Comput. Syst. 2019, 101, 621–634.

30. Kang, J.; Fan, K.; Zhang, K.; Cheng, X.; Li, H.; Yang, Y. An ultra light weight and secure RFID batch authentication scheme for IoMT. Comput. Commun. 2020, 167, 48–54.
31. He, D.; Zeadally, S. An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography. IEEE Internet Things J. 2014, 2, 72–83.
32. Kumar, N.; Kaur, K.; Misra, S.C.; Iqbal, R. An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud. Peer-to-Peer Netw. Appl. 2015, 9, 824–840.
33. Cheng, X.; Zhang, Z.; Chen, F.; Zhao, C.; Wang, T.; Sun, H.; Huang, C. Secure Identity Authentication of Community Medical Internet of Things. IEEE Access 2019, 7, 115966–115977.
34. Abou-Nassar, E.M.; Iliyasu, A.M.; El-Kafrawy, P.M.; Song, O.Y.; Bashir, A.K.; Abd El-Latif, A.A. DITrust chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access 2020, 8, 111223–111238.
35. Nandy, T.; Bin Idris, M.Y.I.; Noor, R.M.; Kiah, M.L.M.; Lun, L.S.; Juma'At, N.B.A.; Ahmedy, I.; Ghani, N.A.; Bhattacharyya, S. Review on Security of Internet of Things Authentication Mechanism. IEEE Access 2019, 7, 151054–151089.
36. Khemissa, H.; Tandjaoui, D. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. In Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, 9–11 September 2015; pp. 90–95.