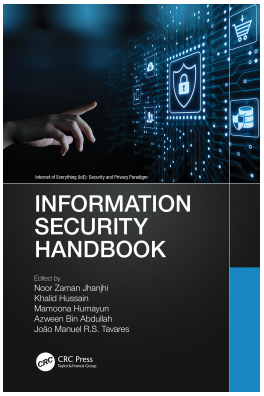

Information Security Handbook

Noor Zaman Jhanjhi, Khalid Hussain, Azween Bin Abdullah, Mamoona Humayun, João Manuel R.S. Tavares

Key Authentication Schemes for Medical Cyber Physical System

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367808228-8
Zia ur Rehman, Saud Altaf, Saleem Iqbal, Khalid Hussain, Kashif Sattar
Published online on: 18 Feb 2022

8 Key Authentication Schemes for Medical Cyber Physical System

Zia ur Rehman, Saud Altaf, Saleem Iqbal, Khalid Hussain, and Kashif Sattar

CONTENTS

8.1 Introduction 141
8.2 Security Objectives for Medical CPS 142
8.2.1 Mutual Authentication 142
8.2.2 Data Freshness 143
8.2.3 Forward Security 143
8.2.4 Data Authenticity 143
8.2.5 Data Integrity 143
8.2.6 Data Confidentiality 143
8.2.7 Unforgeability 144
8.2.8 Scalability 144
8.3 Security Challenges for Medical CPS 144
8.3.1 Resource Constraint (Gupta et al., 2019) 144
8.3.2 Denial of Service Attack (Alguliyev et al., 2018) 144
8.3.3 Impersonation Attack (Xu et al., 2019a,b) 144
8.3.4 Replay Attack (Kompara et al., 2019) 144
8.3.5 Eavesdropping Attack (Shen et al., 2018) 144
8.3.6 Compromised Nodes and Clone Attack (Xu et al., 2019a,b) 145
8.3.7 Anonymous and Unlinkable Sessions (Kompara et al., 2019) 145
8.3.8 Desynchronization/Jamming Attack (Liu & Chung, 2017) 145
8.4 Types of Key Authentication Schemes for Medical CPS 145
8.4.1 Physiological-Based Key Authentication Schemes 145
8.4.2 Cryptographic-Based Authentication Schemes 146
8.4.2.1 Pre-deployed Authentication Schemes 147
8.4.2.2 Asymmetric Authentication Schemes 148
8.4.3 Hybrid Authentication Schemes 150
8.4.4 Channel-Based Authentication Schemes 150
8.5 Conclusion and Future Research Direction 152
References 152

DOI: 10.1201/9780367808228-8

8.1 INTRODUCTION

The rapid development has been enduring in recent years in the various research areas, including hardware, communication technologies, software, etc. The embedded devices have played a pivotal part in various artificially intelligent applications. The extended research has transformed it to become a part of an emerging research direction called cyber physical systems (CPS). The CPS is one of an evolving trend in research that incorporates cyber, physical, and computing components together to unleash an innovative direction in the academic community. The subfields of CPS include smart grids, smart vehicles (unmanned ground vehicles (UGV)), unmanned arial vehicles (UAV), health monitoring, industrial control systems, and water/gas distribution networks. Many of these systems are deployed in critical environments and are playing a vital role in our daily lives.

Before expanding further, the difference between CPS and internet of things (IoT) needs to be elaborated. First, IoT connects sensing devices with the internet by supplementing features like high sensitivity, reliable transmission, and intelligent processing, while CPS utilizes information acquired from IoT with its ability to deeply incorporate the 3Cs (communication, computing and control). In other words, CPS extends the functionality of IoT, firstly by providing more robust control over physical entities with add-on safety, efficiency, and reliability, and secondly, it has far exceeded computational requirements for equipment compared with IoT.

Medical CPS is a special-purpose field devised from the health-monitoring subset of CPS. It requires sensing technologies for reliable data acquisition from remote locations, and for this purpose, it extensively depends on a specialized network called wireless sensors networks (WSN) for data acquisition, transmission, and control. The wearable or implantable devices are used for acquiring data from patients, which is then sent to medical practioner to diagnosis and further treat. The secure data transmission remains the paramount concern due to the openness of the communicational channel, which is wireless most of the time. The aim of the chapter is to address security objectives, numerous security challenges, and various categories of key authentication schemes as a promising solution to achieve those security objectives for the designers of medical CPS applications to enhance the quality of life. The architecture of medical CPS is shown in Figure 8.1.

The chapter is organized as follows: Section 8.2 addresses the security objectives, Section 8.3 highlights the potential security challenges, Section 8.4 describes the various types of key authentication schemes as a possible solution to security problems, and finally, the conclusion and future work is furnished at the end.

8.2 SECURITY OBJECTIVES FOR MEDICAL CPS

The following are the security objectives for medical CPS (Rehman et al., 2019):

8.2.1 Mutual Authentication

Mutual authentical ensures that only authentic users can communicate among themselves and data communication is genuine. Therefore, it is vital requirement.

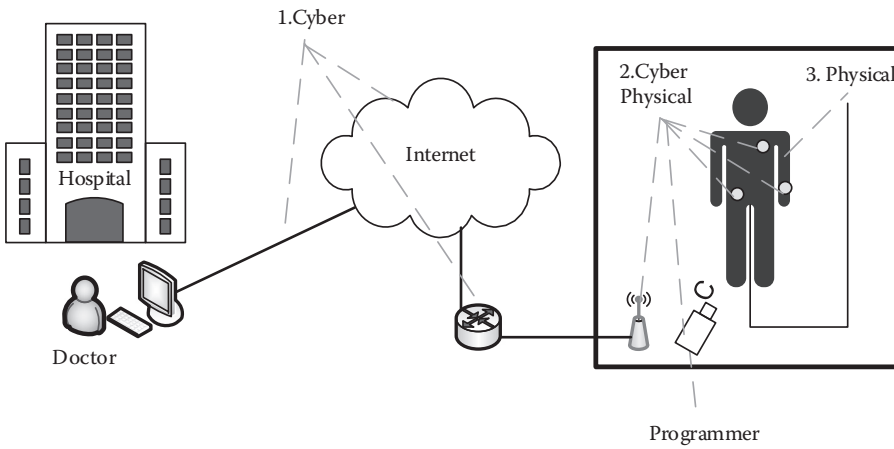

FIGURE 8.1 The architecture of medical CPS.

8.2.2 Data Freshness

This objective ensure that data is new and the system should be vigilant enough to identify older data. This feature helps to make sure that integrity and confidentiality of data is not disturbed.

8.2.3 Forward Security

This security objective is to make sure that an entity cannot access or predict post-departure communication once it leaves the network. An adversary should not be able to predict any future secrets by guessing on the basis of some previous information.

8.2.4 Data Authenticity

This objective makes sure that the valid data is communicated from a legitimate node and it is not from any intruder. Mostly the schemes use message authentication code (MAC) for this purpose.

8.2.5 Data Integrity

This objective ensures that the integrity of data is not disturbed due to any ilegitimate modification during transmission. It makes sure that content of the message is not modified and is accurate.

8.2.6 Data Confidentiality

It refers to the fact data cannot be accessed by unauthorized persons, and it remains confidential. Medical devices have patients' data, which is extremely significant and should not be exposed to impostera.

8.2.7 Unforgeability

It refers to an important feature in which base station should not be compromised by an adversary in order to ensure smooth encumberance-free operation of any authentication scheme.

8.2.8 Scalability

It refers to an important feature in which the authentication scheme should support network growth. In other words, the authentication process should not be disturbed or weakened with the introduction of new nodes.

8.3 SECURITY CHALLENGES FOR MEDICAL CPS

The following security challenges have been commonly found in literature.

8.3.1 Resource Constraint (Gupta et al., 2019)

It is a critical issue when collecting data from wearable or implantable devices to monitor a patient's condition. Therefore, the provision of security is challenging because traditional methods, such as assymetric crypto-solutions, are resource intensive and may not be suitable.

8.3.2 Denial of Service Attack (Alguliyev et al., 2018)

An adversary can overwhelm any device by sending extensive requests to make it unresponsive and thus make the device unavailable.

8.3.3 Impersonation Attack (Xu et al., 2019a,b)

An intruder tries to impersonate the nodes and acts like a genuine member of the network, but actually is not. This happens when an adversary has illegitimately gained access to the user's private credentials allowing them to behave like an actual user.

8.3.4 Replay Attack (Kompara et al., 2019)

An adversary somehow deceitfully captures the valid communication and replays it after some time to gain access to the network. It is a kind of attack that is difficult to detect because communication is normally valid and able to pass all the tests.

8.3.5 Eavesdropping Attack (Shen et al., 2018)

An adversary tries to extract some useful information by listening to the data traffic to extract some secret that can be used to launch any successive attack.

8.3.6 Compromised Nodes and Clone Attack (Xu et al., 2019a,b)

In this attack, an intruder tries to compromise the most important node by gaining access to the particular node and commanding the node to behave as per its will. In a clone attack, it copies all the session keys to create a duplicate node that takes over the legitimate one.

8.3.7 Anonymous and Unlinkable Sessions (Kompara et al., 2019)

In this attack, an adversary tries to link two or more anonymous sessions to the same node to extract some valuable features, which can be used to unveil some secrets, like session keys, etc. Therefore, communication must be kept anonymous.

8.3.8 Desynchronization/Jamming Attack (Liu & Chung, 2017)

When the parties try to update their state in synchronization, after updating the state for the first party, the attacker compromises the communicating link so that the other party cannot update itself. Most of the authentication schemes are found to be vulnerable to this kind of attack.

8.4 TYPES OF KEY AUTHENTICATION SCHEMES FOR MEDICAL CPS

After identifying the security threats found in medical CPS, there is a dire need to develop a security mechanism that can adequately protect the communication among sensor nodes (N) and hub nodes (HN). The key authentication schemes are considered as a defense mechanism to secure the communication and are discussed in the remaining section. The researchers have categorized the authentication schemes in different ways; however, the most renowned types are included in the following section and are named as physiological based, cryptographic based, channel based, and hybrid authentication schemes (Rehman et al., 2019; Kompara & Hölbl, 2018).

8.4.1 Physiological-Based Key Authentication Schemes

These key authentication schemes use bodily features of a patient, i.e., heart, pulse rates, blood pressure, electrocardiogram (ECG), etc., to develop and agree on a single shared key, and this key is used to authenticate the communication among devices. Elyazidi et al. (2018) proposed a scheme that collects the physiological features like (ECG, pedometer, blood glucose, body movement, etc.) through body sensor nodes and transmits it to CU (smartphone). The sensor nodes are authenticated on CU if the true (1) correlation exists between the sensor node and CU is otherwise false (0) for the other case. If both sensor nodes and CU are on the same body, then the correlation is 1 else 0 for the opposite case. That's how sensor nodes are authenticated accordingly. The results of accuracy and precision are 84%–94.5% and 88%–91.5%, respectively.

Wu et al. (2018) proposed multitask EEG-based authentication schemes joined with eye blinking. The authors of this scheme have employed 15 imposters for each user to add more information to train classifiers to make the authentication process further stable. Furthermore, they have conducted open-set authentication tests for additional imposters to simulate the practical environment, which adds an extra edge to this scheme over the previous EEG-based authentication schemes. The results of this scheme have shown an increase in accuracy from 92.4% to 97.6%. Moreover, the robust security and reliability of this scheme is shown by a mean false accepted rate (FAR) of 3.9% and a false rejected rate of (FRR) 3.87%, respectively.

Sammoud et al. (2020) proposed an electrocardiogram (ECG) based symmetric key authentication scheme. Their scheme is based on three entities, namely, sensors attached to patients' body, the central node (PDA or cell phone), and the medical server. It also offers better key entropy due time variant property of ECG signal and ensures key retrieval. It is based on two important phases; firstly, the parent-child symmetric key establishment phase is responsible for sharing pre-installed keys with every node except the root node, and lastly, child-child biometric-based key generation phase that allows nodes having common predessor can establish a secure channel to communicate. The comparison results showed that the scheme is energy efficient and robust.

The authors of another study proposed a new scheme, namely CABA that is based on continuous authentication. It utilizes noninvasive biomedical methods for user authentication. The wearable medical sensors (WMSs) were deployed to collect physiological features like blood pressure (arterial systolic blood pressure, arterial average blood pressure, arterial diastolic blood pressure), body temperature, heart rate, oxygen saturation and respiratory rate. CABA engages nine biomedical streams excluding blood glucose (BG), ECG, and EEG to authenticate users continuously. It utilizes a two-phase authentication model, i.e., enrollment phase and authentication phase. The results disclose that it is a lightweight scheme with less cost as compared to peers (Mosenia et al., 2017).

Zouka securely integrated the healthcare system with WMS in his authentication scheme that enabled patients' health monitoring remotely. It utilized physiological features provided by WMS and stored in the healthcare system. The doctor is also intimated about patients' condition via SMS or email, if required. The proposed authentication scheme followed a three-stage model, namely, registration, patient login, and the authentication phase. The results showed it to be a lightweight, efficient, and effective authentication scheme (Zouka, 2017).

8.4.2 Cryptographic-Based Authentication Schemes

The cryptographic-based authentication schemes are further divided into two parts, pre-deployed (symmetric) key authentication schemes and asymmetric authentication schemes. However, pre-deployed key authentication schemes provide the highest performance efficiency compared with asymmetric authentication schemes.

8.4.2.1 Pre-deployed Authentication Schemes

One of the recent studies, Kompara et al. (2019), has proposed an anonymous, authentication, and key agreement scheme, which is an enhancement of an earlier work proposed by Liu and Chung (2017). This study has only two cryptographic operations: hash function and XOR operation are used, which has turned it into a lightweight scheme. The scheme of Liu and Chung (2017) is found vulnerable for the untraceability of communicating nodes. The study of Kompara et al. (2019) has fixed the said problem by retaining the computational complexity of the original scheme and minimizing the communication cost, but on the price of increased cost of storage.

Moreover, on scrutinizing Kompara et al. (2019) further, the authors of another study (Rehman et al., 2020) have identified three vulnerabilities, namely, sensor-node impersonation, base station, and, intermediate node (IN) compromise attacks. Rehman et al. (2020) provided an enhanced scheme by not only providing a solution for these vulnerabilities but also making architectural-level vital changes in the original scheme. Thus reduced the overall communicational cost, which was remarkably lower compared with not only the original scheme but also with peer schemes as well. The network model of Rehman et al.'s scheme is shown in Figure 8.2.

Similarly, another improvement of Liu and Chung (2017) has been proposed by (Chen et al., 2018). They have highlighted that the Li et al.'s scheme is vulnerable

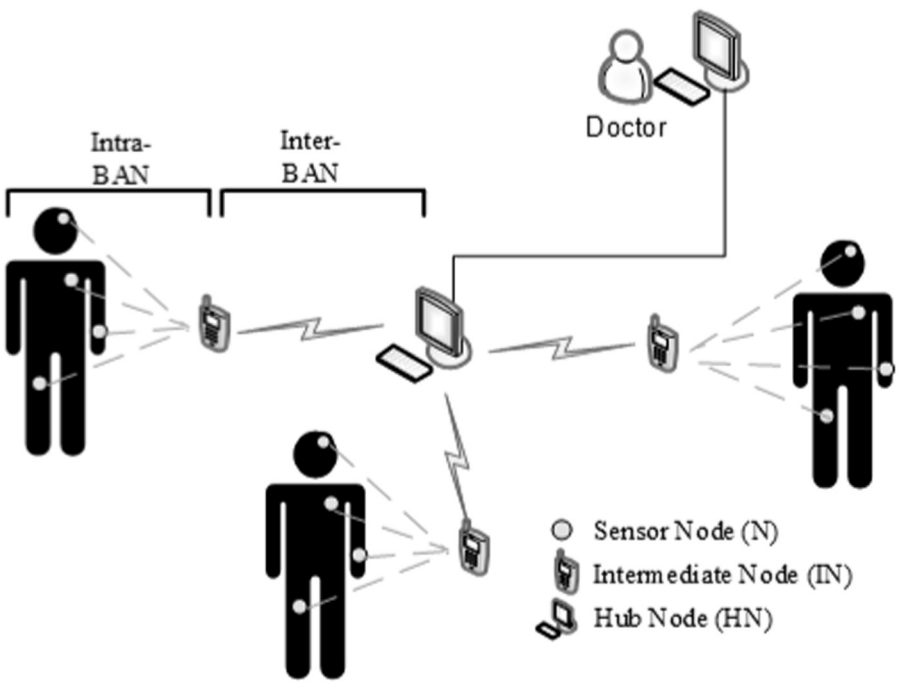

FIGURE 8.2 The network model of Rehman et al.'s scheme (2020).

to offline identity guessing, sensor-node impersonation, and hub node spoofing attacks. They have presented their own scheme by rectifying the highlighted flaws. Thus, they are providing more security and efficiency for the proposed scheme. They have modified the conventional way of communication between sensor node (SN), first node (FN), and hub node (HN) by limiting the role of FN as a relaying node because it is only forwarding data to HN without taking an active role in authenticating the nodes. This change has positively impacted the overall scheme by lowering the communication and storage cost over other peer schemes. Moreover, another enhancement of Li et al.'s (2017) scheme is also proposed by (Ostad-Sharif et al., 2019). They have pointed out that Li et al.'s scheme is vulnerable to wrong session key agreement and dsynchronization attacks. They have provided the solution to these problems, along with security against some other known attacks like impersonation, man-in-the-middle, modification, replay, hub-node stolen database, etc. The experimental results have shown better efficiency, security, and practicabillity.

In another study, (Xu et al., 2019b) has presented a lightweight, anonymous, authentication, and key agreement, which also relies on XOR operations and hash function. This study ensures forward secrecy without utilizing asymmetric encryption; even if an adversary some how compromises the master key. The experimental results of this study indicate low computational cost and also incur low security risk as compared with other peer lightweight schemes. Moreover, the lightweight scheme proposed by (Xu et al., 2019a) also uses XOR operations and hash function. The scheme provides security against a number of known attacks, e.g., eavesdropping, man-in-the-middle, replay, jamming/desynchronization, sensor-node anonymity and untraceability, forward/backward security, hub-node spoofing, and sensor-node impersonation attacks. The comparison results of this study depict that it has lower communication cost and security risk.

Shuai et al. (2020a) have recently presented a lightweight, privacy-perserving authentication scheme using one-way hash funchtion and pseudonym identity technique. The scheme provided resilience against forward secrecy, smart card loss, wrong password login and desynchronization attacks, respectively. The comparison results with peer work showed that it is efficient in terms of computational cost but slightly expensive in terms of communicational cost. Moreover, another enhancement of Kompara et al.'s work is proposed by (Almuhaideb & Alqudaihi, 2020). The authors proposed two protocols, namely P-I and P-II for authentication and re-authentication, respectively to protect anonymity of nodes. Although the scheme has high communication complexity, it achieved improved trade-off between performance and security. The performance analysis of the scheme showed that it has reduced computational cost and time if we consider P-I and P-II separately, but communication overhead is high on the hub node as compared with peer work.

8.4.2.2 Asymmetric Authentication Schemes

Shen et al. (2018) have proposedauthentication schemes for securing communication between personal digital assistance (PDA) and sensors, and the process used for key generation is kept lightweight. Another novel nonpairing, certificateless

approach based one elliptic curve cryptography (ECC) is used for securing communication between PDA and the application provider (AP). The architectural design of this protocol is shown in Figure 8.1. The experimental results have shown the scheme is lightweight as compared to other RSA-based schemes; it is also efficient in a practical sense.

Xie et al. (2019b) presentated a certificateless authentication scheme, which is an improvement of an earlier work of (Ji et al., 2018) with conditional privacy-preserving (called CasCP). In this study, signature and authentication procedures are developed using elliptic curve cryptography (ECC), which eliminated complex bilinear pairing operation used previously. CasCP provides security against known attacks along with forgery and batch authentication attacks. The comparative results of this scheme have proved its advantage over the same schemes in computation and communication cost. Similarly, Xie et al. (2019a) proposed an improved certificateless aggregation signature scheme (iCLAS) based on a prior study of (Kumar et al., 2018). The iCLAS utilizes ECC, which makes use of an efficient message-signing algorithm, signature verification algorithm, and aggregation algorithm. The proposed scheme is also found resistant against known attacks and upon comparative analysis with other schemes; it is found better in terms of computational and communicational costs.

Truong et al. (2020) presented a chebyshev polynomial based authentication scheme in a multiserver environment. The scheme added a parallel session feature, which was not addressed in the peer work discussed in the article; it gave an extra edge over the peer work. However, storage authentication costs of the said scheme are comparatively higher than the related work. In another work proposed by Chaudhry et al. (2020) an improved and secure authentication scheme is presented. The scheme provided key agreement between cloud server through trusted authority and user. Although the said scheme is verified through a real or random (ROR) model, and informal security features analysis showed added advantage over peer work; but upon comparison of computation and communication costs, it resulted in a slight increase.

Moreover, Shuai et al. (2020b) proposed recently an authentication scheme using elliptic curve cryptography (ECC). The authors adoped identity-based certificateless authentication due to the proposed scheme becoming appropriate for multiserver architecture without participation of a third party. The comparative results showed that computational cost is slightly lower than the peer work, but it has high communicational cost, same as the storage cost. However, the scheme is better in terms of computational cost, and it is also privacy preserving.

In another research work proposed by (Shu et al., 2020), a certificateless aggregation scheme is used in conjunction with blockchain for secure storage of medical data. Although blockchain has limited capacity, it is used only for data-sharing purposes. The multi-trapdoor or chameleon function is used based on ECC to build a certificateless aggregation scheme. The experimental results showed that it is more computationally efficient than pairing-based schemes. The length of aggregate signature is constant, which means with increase of transactions, storage capacity remains same. This feature gave extra credit to it as compared to its peer work.

8.4.3 Hybrid Authentication Schemes

The authors of a paper (Wazid et al., 2018) proposed a scheme that uses mobile password and biometric information to generate a key that is further utilized to authenticate the user. The proposed scheme is lightweight, and semantic security of the said scheme is proved by real-or-random (ROR) model, which showed that the scheme resists against the well-known attacks. It is also simulated through a NS2 simulation tool to measure the performance, and, upon comparison with other peer schemes, it showed low computational and communicational overhead.

Koya & P.P. (2018) proposed a hybrid scheme that improved an earlier work of (Liu & Chung, 2017) by combining it with electrocordiography (ECG) of the subject. The proposed scheme is designed in such way to improve the previous scheme by strengthening the vital security parameters. The biokey is generated from ECG signal by first calculating inter-pulse-interval (IPI); second by removing the most significant bits (MSB) and least significant bits (LSB), thirdly by gray coding, and lastly by applying concatenation operation. Hence, 128 bits biokey is generated through this process, which is used in authentication process. The performance and security analysis show that it provides more functionality and better security.

Challa et al. (2018) proposed a three-factor key agreement protocol and authentication to improve the limitations found in (Liu & Chung, 2017). The three-factors used in this study comprise user password, smart card, and user biometrics to improve the security, and this is the reason it is treated as a hybrid scheme. It is worth mentioning that three factors are combined with an ECC algorithm to make it low communication and low computation costs. This enhancement makes it feasible for wide applicability in the healthcare sector.

Chen (2020) presented biometric-based fuzzy authentication and key negotiation (BFAKN) scheme that provides overall authentication solution for all the entities involved in the communication process, including sensors, terminal, and the server. It deviced mutually agreed keys to ensure the validity of whole system, i.e., starting from local communication to terminal processing and then to server. The exprimental results showed that it provides high security, reliability, and effectiveness.

8.4.4 Channel-Based Authentication Schemes

Zhang and Ma (2018) have proposed a key authentication scheme on the basis of similarity of received signal strength (RSS). The key is extracted from RSS values of sensor nodes and coordinator nodes. The inconsistency in the key is reduced using n-dimension quantification, and fuzzy extraction is used to transform the output of n-dimension quantifiers into a secret key. This study has high key entropy, which makes it more robust and difficult for an eavesdropper to guess the key. It also ensures low bit inconsistency rate and high key generation rate. The experimental results of scheme demonstrate it as a more feasible solution for resource constraint environment.

In paper (Zhang et al., 2018), the authors presented a variant of password authentication protocol without depending on preshared password assumption. The scheme extracts the password from fading channel and then usee it for devising a

secret key for communication. Authors believed that their protocol would have better performance in terms of computation and communication, as compared to other password authenticated key exchange (PAKE) protocols.

Sciancalepore et al. (2019) presented EXCHANge protocol, which establishes crypto-less over-the-air key based on anonymity of sender/receiver. It is implemented in OpenWSN protocol and tested on OpenMote-CC2538 architecture. Another important aspect of this shceme is that it is the first real-world implementation of establishing a key protocol, which is based on the anonymity of the channel. It works on a physical layer and can set up the new key of 128 bits in an average of 10 seconds, although it requires only single hash function calculation. The experimental results have proved it secure against active and passive attacks and found it feasible for indoor scenarios and wearable applications.

Umar et al. (2020) recently presented authentication scheme based channel characteristics and an enhanced butterfly algorithm. The experimental results proved it an efficient scheme in terms of storage and computation costs. However, communication cost is slightly higher than one of the peer work. The scheme is also experimentally evaluated not only in different environments and scenarios but also in its performance, which is analyzed on different volunteers. The experimental results showed that the said scheme provided effective mutual authentication and resilience against various security attacks.

An authentication scheme name BANA was introduced by (Shi et al., 2013) that utilized variations of RSS to distinguish between legitimate and nonlegitimate nodes. The limitation of BANA was that the sensors need to maintain the line of sight (LOS), and it did not generate any secret key. This drawback was rectified in successive schemes, namely MASK-BAN (Shi et al., 2015) that extracted secret keys based on channel characteristics. The false positive rates are controlled using a multi-hop authentication mechanism. The experimental results showed it to be an efficient and effective authentication scheme.

In another research, authors utilized the ratio of RSS among '*wearable proxy devices (WPDs)*' and '*implantable medical devices (IMDs)*' to differentiate between a genuine user and an intruder. Furthermore, in order to improve IMD accessibility in emergency mode and to safeguard against forced authentication attack, they designed two '*authentication request filter (ARF)*' based protocols. The experimental results illustrated that the said scheme achieved a great authentication response rate of 99.2% for a genuine user and low authentication response rate for an intruder (Zhang et al., 2020).

Aman et al. (2020) proposed a lightweight protocol that used channel characteristics to excerpt wireless fingerprints and '*physical unclonable functions*' to achieve mutual authentication, anonymity, and data provenance. The scheme actually used a link-quality indicator (LQI) to distinguish among adversarial and nonadversarial wireless links. The experimental results showed that fingerprints accurately identify cyber-attacks, and it is energy efficient as compared to peer work.

Similarly, in another investigation, an authentication scheme was presented that utilized the user's behavioral fingerprints along with channel characteristics. The RSS is monitored for user actions like teeth brushing, water drinking,

medicine taking, and breakfast eating in this experimental study. These behavioral data were collected and stored in a monitoring station that generated fingerprints for the user. This data is further utilized for the authentication process. The experimental results demonstrated that the scheme successfully recognized identity, even in worst case scenarios as well, and showed adequate resistance against intruders (Zhao et al., 2016).

8.5 CONCLUSION AND FUTURE RESEARCH DIRECTION

Medical CPS is a promising field that paves the way for additional research activities. It is a research arena with a lot of potential to improve quality of life in remote health-monitoring scenarios. However, the ease is accompanied by the cost, i.e., security of patient's data, which is of utmost importance. The new security challenges have been arising with the advent of new technology and interconnection of devices. Therefore, the severe concerns regarding security will be continuing. This chapter figured out the security objectives along with the challenges regarding security, which is found commonly. A summary of various types of key authentication schemes have been discussed briefly as a possible solution to these problem. By scrutinizing these schemes, it has been found that pre-deployed key authentication schemes are highly efficient, lightweight, and recommended choice for this field as compared with other authentication schemes. However, other authentication schemes are equally important and are potential candidates for deploying them in resource and energy constraint environments; still more research trends can be found in symmetric key crypto-solution and especially in pre-deployed key authentication schemes.

We perceive that the research regarding security of medical CPS will remain enduring in the future, as with the advancement in technology and security challenges. Channel-based schemes are found more robust and have extra edge in terms of key entropy, but they are computation intensive like asymmetric crypto-solutions. As discussed earlier, pre-deployed key authentication schemes are the potential candidate for future work due to lightweightness and low computation demands. Hybrid authentication schemes are another potential candidate for future work due to the robustness it offers.

REFERENCES

[1] Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*(April), 212–223. 10.1016/j.compind.2018.04.017.

[2] Aman, M. N., Basheer, M. H., & Sikdar, B. (2020). A lightweight protocol for secure data provenance in the internet of things using wireless fingerprints. *IEEE Systems Journal*, 1–11. 10.1109/jsyst.2020.3000269.

[3] Almuhaideb, Abdullah M., & Alqudaihi, Kawther S. (2020). A Lightweight and Secure Anonymity Preserving Protocol for WBAN. *IEEE Access*, 8, 178183–178194. 10.1109/access.2020.3025733.

[4] Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., & Vasilakos, A. V. (2018). An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks.

Computers and Electrical Engineering, *69*, 534–554. 10.1016/j.compeleceng.2017.08.003.

[5] Chaudhry, Shehzad Ashraf, Shon, Taeshik, Al-Turjman, Fadi, & Alsharif, Mohammed H. (2020). Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. *Computer Communications*, 153, 527–537. 10.1016/j.comcom.2020.02.025.

[6] Chen, C., Xiang, B., Wu, T., & Wang, K. (2018). An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks. *MDPI*, *8*(1074), 1–15. 10.3390/app8071074.

[7] Chen, Hanlin, Ding, Ding, Su, Shuchun, & Yin, Jingyi (2020). Biometrics-based cryptography scheme for E-Health systems. *Journal of Physics: Conference Series*, 1550, 022039. 10.1088/1742-6596/1550/2/022039.

[8] Elyazidi, Saâd, Escamilla-Ambrosio, Ponciano Jorge, Gallegos-Garcia, Gina, & Rodríguez-Mota, Abraham (2018). Accelerometer Based Body Area Network Sensor Authentication, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering,Smart Technology* (pp. 151–16410.1007/978-3-319-73323-4_15.

[9] Gupta, A., Tripathi, M., Shaikh, T. J., & Sharma, A. (2019). A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Computer Networks*, *149*, 29–42. 10.1016/j.comnet.2018.11.021.

[10] Ji, S., Gui, Z., Zhou, T., Yan, H., & Shen, J. (2018). An efficient and certificateless conditional privacy-preserving authentication scheme for wireless body area networks big data services. *IEEE Access*, *6*, 69603–69611. 10.1109/ACCESS.2018.2880898.

[11] Kompara, M., & Hölbl, M. (2018). Survey on security in intra-body area network communication. *Ad Hoc Networks*, *70*, 23–43. 10.1016/j.adhoc.2017.11.006.

[12] Kompara, M., Islam, S. H., & Hölbl, M. (2019). A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Computer Networks*, *148*, 196–213. 10.1016/j.comnet.2018.11.016.

[13] Kumar, P., Kumari, S., Sharma, V., & Kumar, A. (2018). Sustainable computing: Informatics and systems A certificateless aggregate signature scheme for healthcare wireless sensor network. *Sustainable Computing: Informatics and Systems*, *18*, 80–89. 10.1016/j.suscom.2017.09.002.

[14] Koya, Aneesh M., & P. P., Deepthi (2018). An Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. Computer Networks, 140, 138–151. 10.1016/j.comnet.2018.05.006.

[15] Liu, C. H., & Chung, Y. F. (2017). Secure user authentication scheme for wireless healthcare sensor networks. *Computers and Electrical Engineering*, *59*, 250–261. 10.1016/j.compeleceng.2016.01.002.

[16] Li, Xiong, Ibrahim, Maged Hamada, Kumari, Saru, Sangaiah, Arun Kumar, Gupta, Vidushi, & Choo, Kim-Kwang Raymond (2017). An Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, 129, 429–443. 10.1016/j.comnet.2017.03.013.

[17] Mosenia, A., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2017). CABA: Continuous authentication based on BioAura. *IEEE Transactions on Computers*, *66*(5), 759–772. 10.1109/TC.2016.2622262.

[18] Rehman, Z. U., Altaf, S., & Iqbal, S. (2019). Survey of authentication schemes for health monitoring: A subset of cyber physical system. In 2019 16th International Bhurban Conference on Applied Sciences and Technology, IBCAST 2019, pp. 653–660. IEEE. 10.1109/IBCAST.2019.8667166.

[19] Shuai, Mengxia, Xiong, Ling, Wang, Changhui, & Yu, Nenghai (2020). Lightweight and privacy-preserving authentication scheme with the resilience of

desynchronisation attacks for WBANs. *IET Information Security*, 14, 380–390. 10.1049/iet-ifs.2019.0491.

[20] Rehman, Zia Ur, Altaf, Saud, & Iqbal, Saleem (2020). An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN. *IEEE Access*, 8, 175385–175397. 10.1109/access.2020.3026630.

[21] Ostad-Sharif, Arezou, Nikooghadam, Morteza, & Abbasinezhad-Mood, Dariush (2019). Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks. *International Journal of Communication Systems*, 32, e3974. 10.1002/dac.3974.

[22] Sammoud, Amal, Chalouf, Mohamed Aymen, Hamdi, Omessaad, Montavont, Nicolas, & Bouallegue, Ammar (2020). A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis. *Computers & Security*, 96, 101838. 10.1016/j.cose.2020.101838.

[23] Sciancalepore, S., Oligeri, G., Piro, G., Boggia, G., & Di, R. (2019). EXCHANge: Securing IoT via channel anonymity. *Computer Communications*, *134*(February 2018), 14–29. 10.1016/j.comcom.2018.11.003.

[24] Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems*, *78*, 956–963. 10.1016/j.future.2016.11.033.

[25] Shi, L., Li, M., Yu, S., & Yuan, J. (2013). BANA: Body area network authentication exploiting channel characteristics. *IEEE Journal on Selected Areas in Communications*, *31*(9), 1803–1816. 10.1109/JSAC.2013.130913.

[26] Shi, L., Yuan, J., Yu, S., & Li, M. (2015). MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *IEEE Internet of Things Journal*, *2*(1), 52–62. 10.1109/JIOT.2015.2391113.

[27] Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D., & Sun, L. (2020). An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems. *Sensors (Switzerland)*, *5*(2020), 1521.

[28] Truong, T., Tran, M., & Duong, A. (2020). Chebyshev polynomial-based authentication scheme in multiserver environment polynomial-based authentication scheme. *Security and Communication Networks, 2020*.

[30] Wazid, M., Das, A. K., & Vasilakos, A. V. (2018). Authenticated key management protocol for cloud-assisted body area sensor networks. *Journal of Network and Computer Applications*, *123*(September), 112–126. 10.1016/j.jnca.2018.09.008.

[31] Umar, Mubarak, Wu, Zhenqiang, & Liao, Xuening (2020). Mutual Authentication in Body Area Networks Using Signal Propagation Characteristics. *IEEE Access*, 8, 66411–6642210.1109/access.2020.2985261.

[32] Wu, Q., Zeng, Y., Zhang, C., Tong, L., & Yan, B. (2018). An EEG-based person authentication system with open-set capability combining eye blinking signals. *Sensors (Switzerland)*, *18*(2), 1–18. 10.3390/s18020335.

[33] Xie, Y., Li, X., Zhang, S., & Li, Y. (2019a). ICLAS: An improved certificateless aggregate signature scheme for healthcare wireless sensor networks. *IEEE Access*, *7*, 15170–15182. 10.1109/ACCESS.2019.2894895.

[34] Xie, Y., Zhang, S., Li, X., Li, Y., Chai, Y., & Zhang, M. (2019b). CasCP: Efficient and secure certificateless authentication scheme for wireless body area networks with conditional privacy-preserving. *Security and Communication Networks, 13*. 10.1155/2019/5860286.

[35] Xu, Z., Xu, C., Chen, H., & Yang, F. (2019a). A lightweight anonymous mutual authentication and key agreement scheme for WBAN. *Concurrency Computation*, *31*(14), 1–12. 10.1002/cpe.5295.

[36] Xu, Z., Xu, C., Liang, W., Xu, J., & Chen, H. (2019b). A lightweight mutual authentication and key agreement scheme for medical internet of things. *IEEE Access*, *7*(c), 53922–53931. 10.1109/ACCESS.2019.2912870.

[37] Zhang, P., & Ma, J. (2018). Channel characteristic aware privacy protection mechanism in WBAN. *Sensors*, *18*(8), 2403. 10.3390/s18082403.

[38] Zhang, Y., Xiang, Y., Wu, W., & Alelaiwi, A. (2018). A variant of password authenticated key exchange protocol. *Future Generation Computer Systems*, *78*, 699–711. 10.1016/j.future.2017.02.016.

[39] Zhang, Z., Xu, X., Han, S., Liang, Y., & Liu, C. (2020). Wearable proxy device-assisted authentication request filtering for implantable medical devices. In IEEE Wireless Communications and Networking Conference, WCNC, 2020 May. 10.1109/WCNC45663.2020.9120856.

[40] Zhao, N., Ren, A., Hu, F., Zhang, Z., Rehman, M. U., Zhu, T., … Alomainy, A. (2016). Double threshold authentication using body area radio channel characteristics. *IEEE Communications Letters*, *20*(10), 2099–2102. 10.1109/LCOMM.2016.2597831.

[41] Zouka, H. A. El. (2017). An authentication scheme for wireless healthcare monitoring sensor network. In 2017 14th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), pp. 68–73. 10.1109/HONET.2017.8102205.