World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Tele-care medical information systems security techniques: A critical review of the state of the art techniques

Abraham Isiaho *, Kelvin Kabeti Omieno and Hillan Rono

School of Computing & Information Technology, Kaimosi Friends University, Kaimosi, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2022, 07(02), 240–254

Publication history: Received on 13 November 2022; revised on 24 December 2022; accepted on 27 December 2022

Article DOI: https://doi.org/10.30574/wjaets.2022.7.2.0136

Abstract

The advancement in information communication technologies has seen the rise in the deployment of various information exchange devices in the healthcare sector. Among these technologies is the Tele-care Medical Information Systems (TMIS) in which remote users can establish a connection with the hospital medical server and share the necessary information between them. This can potentially offer doctors and patients more reasonable treatment plan, as well as helping address the huge medical expenses and excessive medical treatment duration. There is therefore need to store patient data in the end devices, as well as transmit this data over public channels to facilitate decision making. This paper sought to review the security schemes that have been developed over the recent past to protect the patient data stored or transmitted in TMIS.

Keywords: Attacks; EHR; EMR; TMIS; Security; Privacy

1. Introduction

The conventional clinical data initiatives are typically fragmented among hospital departments or across different health facilities. This presents some difficulties in the effective information flow among these health facilities or departments. Consequently, there is some challenges when the patients want to make reasonable treatment decisions [1]. As such, scalable and secure data sharing is key for the healthcare decision-making process. The recent advancements in network topologies and technologies have given rise to Tele-care Medical Information Systems (TMIS). In this technology, remote users can establish a connection with the hospital medical server and share the necessary information between them [2]. However, this information exchange is normally executed over a public channel [3]. As pointed out in [4], TMIS has revolutionized the traditional medical services in terms of allowing the patients to access hospital information systems via the internet and access doctor's telemedicine services. In so doing, TMIS systems offer doctors and patients more reasonable treatment plan. In addition, they help address the huge medical expenses and excessive medical treatment duration [5].However, TMIS has numerous security issues such as false authentication, information leakage and key loss [6]. As pointed in [7], it is important to uphold privacy [8] during the development of TMIS.

In the current scenario, the patients need to have their health records duplicated in multiple hospitals within a given geographical area [9]. This presents some challenges when one healthcare provider wants to access patient healthcare data held in another provider. This is more so when the patients are in critical conditions. This problem can partly solved by Wireless Medical Sensor Networks (WMSN)-based medical systems. These systems enable the patients and doctors to access various healthcare services over wireless communication technologies without visiting the hospital in person [10]. Other services provided by these systems include medical consultation, emergency treatment and monitoring [11], [12]. This serves to save treatment time and improve the patients' quality of life.

*Corresponding author: Abraham Isiaho

School of Computing & Information Technology, Kaimosi Friends University, Kaimosi, Kenya.

During remote access of healthcare services, security and privacy are two important features that must be preserved [13]-[17]. In addition, authors in [18] discuss the importance of securing user private information during TMIS development and operation. This is due to the ease with which adversaries can disrupt the communication process over public channels. Such disruptions may include message interception, eavesdropping, forgery, replays and side-channel attacks. These threats and attacks can potentially lead to data loss, malicious access and intellectual property infringement. As pointed out in [19], interoperability is another significant challenge in the healthcare industry that can impede exchange of health records among healthcare providers.

It is evident that any successful malicious access or leakage of patient private data can lead to incalculable consequences [20]. This points to the importance of protecting the TMIS systems from attacks. One of the most effective ways of doing this is via the design of intrusion detection technologies as well as secure identity authentication schemes [21], [22]. There is also need for safe storage, integrity protection and secure transmission of patient healthcare data [23], [24].

To this end, many schemes have been put forward based on technologies such as blockchain, Radio Frequency Identification (RFID) and Physical Unclonable Function (PUF). As explained in [25], the blockchain technology plays a crucial role in the provision of a secure and effective means to share information in a variety of domains such as the financial sector, supply chain management, Internet of Things (IoT) and health care systems. The blockchain technology's interoperability, decentralized, transparency and security has rendered it suitable in maintaining the patient Electronic Health Record (EHR) and Electronic Medical Records (EMR) for various medical devices, billing and telemedicine systems. As explained in [26], the blockchain transparency permits the patients and doctors to view and examine the corresponding EHRs stored in the network. In addition, its decentralized nature allows the communication among various nodes devoid of the deployment of the central authority [27] for validation purposes [28]. On the other hand, RFID has been deployed by TMIS to authenticate the identity of the requesting entity. As the authors in [29] discuss, RFID has been heavily utilized in IoT and can therefore offer security for medical information. On its part, PUF technology has been deployed for IP circuit protection, identity authentication, hardware identification, copyright protection and key generation [30]-[32]. This paper makes the following contributions:

- A review of the most prominent technologies for security TMIS is provided.
- The security, performance and privacy challenges of the current schemes for TMIS protection are identified.
- Some general guidelines for the TMIS security enhancement are provided.

The rest of this article is structured as follows: Part 2 presents the related work while Part 3 discusses the results obtained. On the other hand, Part 4 gives the recommendations while Part 5 concludes this article.

2. Related work

The significance of TMIS security has seen the development of numerous schemes for secure information exchange among remote users and hospital medical servers. For example, a secure and efficient protocol for telemedicine services is introduced in [33]. However, this scheme has high communication overheads [34] during the establishment of establish secure and fresh session key, and is therefore inefficient. On the other hand, blockchain-based healthcare systems are developed in [9], [25], [30], [35]-[40]. However, blockchain has high storage and computation overheads [41]. This challenge can potentially be solved by the efficient and secure lightweight authentication protocol in [42]. Unfortunately, the protocol in [42] is vulnerable to traceability, dictionary, password guessing and stolen card attacks [43], [44]. These issues are addressed by the Elliptic Curve Cryptography (ECC) and PUF-based access control and authentication scheme in [6], as well as the RFID and PUF based scheme in [45]. However, PUF based schemes have stability challenges [46]. As such, the authors in [47] have presented an improved lightweight privacy protection access control scheme, while the authors in [48] have developed a new authentication scheme based on RSA. However, the protocol in [48] has high computation complexity due to costly modulo exponentiations.

To extend the application scenarios of TMIS and permit users to access services through smart devices, a three factor remote authentication scheme is developed in [49]. However, cloud computing has a number of vulnerabilities that can be exploited by attackers [50]. On the other hand, authors in [51] have presented an ECC based three-party authentication and key agreement scheme, while a lightweight access control protocol based on ECC is developed in [52]. Although the security of the scheme in [52] is verified by the random oracle model, this protocol only offers one-way verification function. To solve this problem, authors in [53] have developed a lightweight two-factor security technique based on hash chains. Although this scheme is resistant to potential security attacks, it cannot prevent sensor physical capture and stolen verifier attacks [54]. This challenge can be addressed by the patient-centric data sharing technique in [55]. In this scheme, machine learning algorithms [56] are deployed to detect the anomaly during the message passing.

To secure the communication in health care services, an efficient chaotic map-based authentication protocol is presented in [57]. However, this approach is vulnerable to impersonations and password guessing attacks [58]. Similarly, the scheme in [59] is susceptible to Man-in-the-Middle (MitM) and session key disclosure attacks. In addition, it cannot guarantee secure mutual authentication among the communicating entities. These challenges can be solved by the digital signature and hash function based scheme in [60]. However, the digital signatures management requires high storage complexities [61]. On the other hand, the schemes in [62], [63], [64], [65] fail to offer anonymous communication. As such, the communicating entities can be traced by the adversaries.

To reduce the cost of TMIS verification, a two-factor ECC based access control and key establishment protocol [66] is presented in [67]. Although this technique has low authentication overheads, it cannot update the password correctly and is vulnerable to replay attacks [68]. This problem is solved by the efficient, secure and robust improved protocol in [58]. However, the protocol in [58] is vulnerable to stolen smart card, identity guess, impersonations and password guessing attacks [69]. On the other hand, the bitcoin-based patient payment portal in [70] has high storage complexities [71]. Therefore, secure and efficient authentication protocols are introduced in [72] and [73]. However, these protocols are susceptible to stolen card, password and identity guessing attacks. Therefore, the authentication and key agreement protocols in [74] and [75] can be deployed to solve these security challenges. On the other hand, a patient verification scheme is developed in [76] based on digital ledger technology. Unfortunately, the patient is unable to select some specific participant for accessing the stored data.

To solve TMIS security risks such as MitM [77] and replay attacks, a three-factor access control protocol is introduced in [78]. Unfortunately, this protocol is susceptible to user simulation and internal attacks [79]. Therefore, improved protocols are presented in [80] and [81]. Although the ECC-based scheme in [80] is resilient against stolen mobile device, de-synchronization, and DoS attacks, it cannot protect against user link and sensor node impersonation attacks [81]. Similarly, although the scheme in [82] is lightweight and hence applicable in heath care telemedicine services, it is susceptible to identity guess, password guess [83] and replay attacks. Similarly, the protocol in [84] is vulnerable to replay attacks [85]. As such, an improved three-factor security technique is introduced in [86]. On the other hand, an efficient access control scheme is developed in [87] to offer strong location confidentiality [88]. Unfortunately, this authentication technique is potentially susceptible to replay attacks. Similarly, the chaotic mapping-based secure remote access control method in [89] cannot withstand side-channel attacks, while the chaotic maps based protocol in [90] cannot offer anonymity and untraceability [91]. Therefore, an improved scheme is presented in [91]. However, this approach is susceptible to stolen smart card attack [92], [93].

To facilitate secure sharing of patient records, a ripple-based scheme is developed in [94]. However, the patient is unable to pay the doctor by using the blockchain wallet. On the other hand, the protocols in [44], [43] and [64] cannot differentiate incorrect inputs within a short time interval due to their flawed input verification procedures. To improve the medication security of patients in TMIS, a privacy protection protocol based on the El-Gamal cryptographic system is introduced in [95]. However, the storage cost [96] of this protocol is too high.Authors in [97] have presented a security authentication protocol based on synchronization secrets to offer privacy in TMIS. However, this scheme has serious security risks in that attacker can access the user's private information by stealing the server [98]. Therefore, an enhanced scheme is presented in [98] in which an authentication mechanism is incorporated between the database and the reader so as to resist server loss attacks. Unfortunately, this technique cannot resist asynchronous and replay attacks [99]. In addition, it fails to offer anonymity [100] of tags and readers. Although the scheme in [101] provides effective verification of a single tag, it is susceptible to secret disclosure and de-synchronization attacks [102]. Therefore, an enhanced secure and efficient chaotic map based authentication protocol is developed in [2] to secure tele-care medicine information system. Similarly, the scheme in [103] can protect physical layer threats. Based on secondary residue and timestamps, a security scheme for protecting private data is presented in [99]. However, this protocol fails to resist asynchronous attacks [84]. In addition, its implementation costs are too high for the resource-constrained [104] TMIS systems. To address this problem, a lightweight and privacy-preserving protocol is presented in [105]. However, this approach is vulnerable to user impersonation, offline password guessing and privileged insider attacks [106]. In addition, it cannot offer user anonymity.

The authors in [107] and [108] have introduced security solutions to boost reliability in the provision of healthcare services. However, these techniques are based on centralized infrastructure and hence prone to issues such as a single point of failure [109]. In addition, this centralized entity becomes the network bottleneck. This issue can be solved by the robust key negotiation protocol developed in [110]. Unfortunately, an in-depth analysis of this approach reveals that it is vulnerable to traceability, server impersonation, packet replay and privileged insider attacks [111]. On the other hand, a Diffie-Hellman key exchange scheme is introduced in [112]. However, this scheme is susceptible to offline password guessing and stolen-verifier attacks [113]. In addition, its huge computation overheads imply that it is inapplicable in resource constrained medical devices [114]. Although this problem is effectively handled by the ECC-based anonymous protocol in [115], it is prone to guessing, impersonation and session key hijacking attacks [116]. Based on the PUF and blockchain technologies, a reliable scheme that is demonstrated to offer mutual authentication and perfect forward secrecy is developed in [14]. Although this approach prevents impersonation, physical sensor device capture and tracing attacks, it is still vulnerable to man in-the-middle (MITM), and session key disclosure attacks [10].The schemes in [117] and [118] can potentially solve these problems. Unfortunately, these schemes are insecure against stolen verifier and cloning attacks [119].

To offer user anonymity, two-factor authentication scheme are presented in [120] and [121]. However, the approach in [121] is susceptible to privileged insider, sensor node capture and user tracking attacks [122]. Owing to the smaller key sizes of ECC, numerous authentication schemes have been developed based on this technology [123-150]. However, many security flaws have also been noticed among these schemes for the TMIS [151]. On the other hand, an enhanced and anonymous two-factor security solution has been developed in [152]. However, this protocol cannot withstand denial of service (DoS), user impersonation and offline identity as well as password guessing attacks [153], [154].

Another ECC-based anonymous scheme is presented in [155] for efficient and secure key agreement and authentication. Unfortunately, this technique cannot withstand replay and stolen or lost smart card attacks. In addition, it fails to offer mutual authentication and its password modification phase is incorrect. Therefore, the authors in [156] have presented an improved scheme to address these issues. Although this approach offers anonymity and provable security, it cannot resist user and server impersonation [157]. As such, an identity-based remote user authentication is developed in [158] to solve this problem. However, this protocol is vulnerable to stolen verifier, secret key leakage and masquerading attacks [159].Similarly, the improved protocol in [157] can solve the issues in [156]. Unfortunately, this scheme cannot protect against man-in-middle [160], offline password-guessing, offline identity guessing as well as server and user masquerade [161]. Therefore, the authors in [161] have presented an enhanced protocol based on fuzzy verifier techniques. Unfortunately, this scheme has an incorrect notion of perfect anonymity and is vulnerable to user masquerade attacks [151].

The security solution in [162] can address some of these issues using only hash and XOR functions. Unfortunately, it is vulnerable to sensor key leakage, de-synchronization and stolen mobile device attacks [163]. To address this issue, a Radio-Frequency Identification (RFID) based protocol is presented in [164], while an end-to-end security solution is developed in [163]. However, the approach in [164] is still susceptible to synchronization, DoS and replay attacks [165]. As such, an enhanced authentication protocol is developed in [166] to improve the challenges in [164]. However, this technique cannot protect against session-specific temporary information attack [167]. On the other hand, the scheme in [163] is vulnerable to DoS, known session temporary information and privileged insider attacks [168], [169].

3. Results

It is evident that numerous schemes have been put forward for the security of TMIS systems. However, the attainment of perfect security still remains challenging due to the many setbacks that have been discovered in majority of these schemes. For instance, although chaotic maps possess dynamic structures that play very vital roles in the construction of secure and efficient authentication protocols, they are generally found vulnerable to numerous threats such as password guessing, impersonation [170], identity guessing and stolen smart-card attacks. On the other hand, RFID-based authentication schemes are susceptible to side-channel attacks [171]. TMIS systemswith such security vulnerabilities will not only leak private information, but also cause significant economic losses [172]. Table 1 gives a summary of the security, performance and privacy challenges of the conventional TMIS protection schemes.

Based on Table 1, majority of the current schemes for securing TMIS have several security, performance and privacy issues. The security issues [173] revolve around susceptibility to traceability, dictionary, password guessing, stolen card, sensor physical capture, stolen verifier, replay, privileged insider, identity guess, impersonations, MitM, asynchronous, secret disclosure, de-synchronization, session key disclosure, user simulation, side-channel and internal attacks. In terms of privacy,failure to offer user anonymity, anonymity of tags and readers, attacker access to the user's private information, as well as traceability. On the other hand, performance challenges are manifested in terms of stability challenges, high communication [174], storage [175], and computation overheads [176].

Table 1 Summary of TMIS Challenges

S. No.	Scheme	Setbacks
1	Jiang et al. [33]	High communication overheads
2	Toshniwal et al. [35], Omar et al. [36], Khatoon [37], Jamil et al. [38], Li et al. [30], Chelladurai et al. [9] Zhouet al. [39], Panigrahi et al. [25], Azaria et al. [40]	High storage and computation overheads
3	Chen et al. [42]	Vulnerable to traceability, dictionary, password guessing and stolen card attacks
4	Xiao, et al. [6], Akgün and Çaˇglayan [45]	Have stability challenges
5	Dharminder et al. [48]	High computation complexity due to costly modulo exponentiations
6	Siddiqui et al. [49]	Has a number of vulnerabilities that can be exploited by attackers
7	Farash et al. [52]	Offers only one-way verification function
8	Fotouhi et al. [53]	Cannot prevent sensor physical capture and stolen verifier attacks
9	Li et al. [57]	Vulnerable to impersonations and password guessing attacks
10	Wang et al. [59]	Susceptible to MitM and session key disclosure attacks; cannot guarantee secure mutual authentication among the communicating entities
11	Angraal et al. [60]	Requires high storage complexities
12	Wei et al. [62], Wu et al. [63], Zhu et al. [64], Lee et al. [65]	Fail to offer anonymous communication
13	Xu et al. [67]	Cannot update the password correctly and is vulnerable to replay attacks
14	Madhusudhan et al. [110]	Vulnerable to stolen smart card, identity guess, impersonations and password guessing attacks
15	Dagher et al. [70]	High storage complexities
16	Wu et al. [72], Radhakrishnan et al. [73]	Susceptible to stolen card, password and identity guessing attacks
17	Dhagarraet al. [76]	The patient is unable to select some specific participant for accessing the stored data
18	Amin and Biswas [78]	Susceptible to user simulation and internal attacks
19	Zhang et al. [82]	Vulnerable to identity guess, password guess and replay attacks
20	Safkhani & Vasilakos [84]	Vulnerable to replay attacks
21	Tewari and Gupta [87]	Susceptible to replay attacks
22	Li et al. [89]	Cannot withstand side-channel attacks

23	Guo et al. [90]	Cannot offer anonymity and untraceability
24	Hao et al. [91]	Susceptible to stolen smart card attack
25	Dimitrov et al. [94]	The patient is unable to pay the doctor by using the blockchain wallet
26	Cao et al. [44], Lin et al. [43],Zhu [64]	Cannot differentiate incorrect inputs within a short time interval due to their flawed input verification procedures
27	Salem and Amin [95]	High storage overheads
28	Srivastava et al. [97]	Attacker can access the user's private information by stealing the server
29	Li et al. [98]	Cannot resist asynchronous and replay attacks; it fails to offer anonymity of tags and readers
30	Xu et al. [101]	Susceptible to secret disclosure and de-synchronization attacks
31	Zhou et al. [99]	Fails to resist asynchronous attacks; its implementation costs are too high
32	Masud et al. [105]	Vulnerable to user impersonation, offline password guessing and privileged insider attacks; cannot offer user anonymity

4. Recommendations

Based on the shortcomings noted in majority of the TMIS systems security schemes, the following are the general guidelines that are critical for secure communication:

- All data should be sufficiently enciphered [177] before being coupled into the communication channel. This is to protect against attacks such as eavesdropping, tampering and malicious modifications.
- The data residing in communicating entities should be in encrypted format. This is in an effort to protect against attacks such as side-channeling and stolen verifier attacks.
- The encryption algorithms deployed should be lightweight so that the computation overheads are kept at minimum.
- The number of messages exchanged during the authentication and key agreement phase should be minimal so as to reduce bandwidth consumption.
- The number of security parameters stored in the communicating entities should be kept low. This is to ensure that the storage overheads are not excessive for the resource-limited devices.

5. Conclusion

The Tele-care Medical Information Systems have revolutionized the traditional medical services by making it possible for the patients to access hospital information systems through the internet and access doctor's telemedicine services. However, since this communication takes place over the public wireless channels, many vulnerabilities lurk in these healthcare systems. Any successful exploitation of these vulnerabilities can result in untold consequences, which may impede the adoption of these healthcare technologies. In this paper, the most current security solutions in this domain have been reviewed. Based on the findings, the attainment of ideal security at low complexities has been noted to be quite challenging. Therefore, numerous recommendations have been offered which can potentially improve the security posture of TMIS.

Compliance with ethical standards

Acknowledgments

We would like to extend our appreciation to all our colleagues and mentors whose kind advice and guidance facilitated the successful completion of this article.

Disclosure of conflict of interest

The authors hereby declare that they do not have any conflict of interest.

References

[1] Siyal AA, Junejo AZ, Zawish M, Ahmed K, Khalil A, Soursou G. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography. 2019 Jan 2, 3(1):3.

[2] Dharminder D, Kumar U, Gupta P. A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services. Complex & Intelligent Systems. 2021 Oct, 7(5):2531-42.

[3] Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[4] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telematics and Informatics. 2019 May 1, 38:100-17.

[5] Li CT, Shih DH, Wang CC. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Computer methods and programs in biomedicine. 2018 Apr 1, 157:191-203.

[6] Xiao L, Xie S, Han D, Liang W, Guo J, Chou WK. A lightweight authentication scheme for telecare medical information system. Connection science. 2021 Jul 3, 33(3):769-85.

[7] Justinia T. Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. ActaInformaticaMedica. 2019 Dec, 27(4):284.

[8] Nyangaresi VO. Lightweight Anonymous Authentication Protocol for Resource-Constrained Smart Home Devices Based on Elliptic Curve Cryptography. Journal of Systems Architecture. 2022 Oct 18:102763.

[9] Chelladurai U, Pandian S. A novel blockchain based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing. 2022 Jan, 13(1):693-703.

[10] Yu S, Park Y. A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions. IEEE Internet of Things Journal. 2022 May 2, 1-15.

[11] Qi J, Yang P, Min G, Amft O, Dong F, Xu L. Advanced internet of things for personalised healthcare systems: A survey. Pervasive and Mobile Computing. 2017 Oct 1, 41:132-49.

[12] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[13] Song J, Zhong Q, Wang W, Su C, Tan Z, Liu Y. FPDP: flexible privacy-preserving data publishing scheme for smart agriculture. IEEE Sensors Journal. 2020 Aug 18, 21(16):17430-8.

[14] Wang W, Chen Q, Yin Z, Srivastava G, Gadekallu TR, Alsolami F, Su C. Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. IEEE Internet of Things Journal. 2021 Oct 5, 9(11):8883-91.

[15] Javed AR, Beg MO, Asim M, Baker T, Al-Bayatti AH. Alphalogger: Detecting motion-based side-channel attack using smartphone keystrokes. Journal of Ambient Intelligence and Humanized Computing. 2020 Feb 15:1-4.

[16] Zhang L, Zou Y, Wang W, Jin Z, Su Y, Chen H. Resource allocation and trust computing for blockchain-enabled edge computing system. Computers & Security. 2021 Jun 1, 105:102249

[17] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In 2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[18] Zhang S, Yao T, Arthur Sandor VK, Weng TH, Liang W, Su J. A novel blockchain-based privacy-preserving framework for online social networks. Connection Science. 2021 Jul 3, 33(3):555-75.

[19] Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of big data. 2018 Dec, 5(1):1-8.

[20] Amin R, Islam SH, Gope P, Choo KK, Tapas N. Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. IEEE journal of biomedical and health informatics. 2018 Sep 14, 23(4):1749-59.

[21] Liang W, Xiao L, Zhang K, Tang M, He D, Li KC. Data fusion approach for collaborative anomaly intrusion detection in blockchain-based systems. IEEE Internet of Things Journal. 2021 Jan 22, 9(16): 14741-14751.

[22] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014, 16(5):137-44.

[23] Kui X, Feng J, Zhou X, Du H, Deng X, Zhong P, Ma X. Securing top-k query processing in two-tiered sensor networks. Connection Science. 2021 Jan 2, 33(1):62-80.

[24] Liang W, Fan Y, Li KC, Zhang D, Gaudiot JL. Secure data storage and recovery in industrial blockchain network environments. IEEE Transactions on Industrial Informatics. 2020 Jan 13, 16(10):6543-52.

[25] Panigrahi A, Nayak AK, Paul R. HealthCare EHR: A Blockchain-Based Decentralized Application. International Journal of Information Systems and Supply Chain Management (IJISSCM). 2022 Jul 1, 15(3):1-5.

[26] Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Computational and structural biotechnology journal. 2018 Jan 1, 16:267-78.

[27] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Aug 23:e13126.

[28] Udokwu C, Anyanka H, Norta A. Evaluation of approaches for designing and developing decentralized applications on blockchain. InProceedings of the 2020 4th international conference on algorithms, computing and systems 2020 Jan 6 (pp. 55-62).

[29] Chen YC, Chen RS, Sun HM, Wu SF. Using RFID technology to develop an intelligent equipment lock management system. International Journal of Computational Science and Engineering. 2019, 20(2):157-65.

[30] Li D, Zhu Q, Wang H, Liu W, Feng Z, Zhang J. A novel computational model for SRAM PUF min-entropy estimation. International Journal of Computational Science and Engineering. 2019, 19(2):215-22.

[31] Liang W, Xie S, Long J, Li KC, Zhang D, Li K. A double PUF-based RFID identity authentication protocol in service-centric internet of things environments. Information Sciences. 2019 Nov 1, 503:129-47.

[32] Gao Y, Ma H, Abbott D, Al-Sarawi SF. PUF sensor: Exploiting PUF unreliability for secure wireless sensing. IEEE Transactions on Circuits and Systems I: Regular Papers. 2017 May 13, 64(9):2532-43.

[33] Jiang Q, Chen Z, Li B, Shen J, Yang L, Ma J. Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug, 9(4):1061-73.

[34] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Verifiable Security and Privacy Provisioning Protocol for High Reliability in Smart Healthcare Communication Environment. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 569-574). IEEE.

[35] Toshniwal B, Podili P, Reddy RJ, Kataoka K. PACEX: PAtient-centric EMR eXchange in healthcare systems using blockchain. In2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) 2019 Oct 17 (pp. 0954-0960). IEEE.

[36] Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. InInternational conference on security, privacy and anonymity in computation, communication and storage 2017 Dec 12 (pp. 534-543). Springer, Cham.

[37] Khatoon A. A blockchain-based smart contract system for healthcare management. Electronics. 2020 Jan 3, 9(1):94.

[38] Jamil F, Hang L, Kim K, Kim D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics. 2019 May 7, 8(5):505.

[39] Zhou L, Wang L, Sun Y. MIStore: a blockchain-based medical insurance storage system. Journal of medical systems. 2018 Aug, 42(8):1-7.

[40] Azaria A, Ekblaw A, Vieira T, Lippman A. Medrec: Using blockchain for medical data access and permission management. In2016 2nd international conference on open and big data (OBD) 2016 Aug 22 (pp. 25-30). IEEE.

[41] Nyangaresi VO. Provably Secure Protocol for 5G HetNets. In 2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[42] Chen HM, Lo JW, Yeh CK. An efficient and secure dynamic id-based authentication scheme for telecare medical information systems. Journal of medical systems. 2012 Dec, 36(6):3907-15.

[43] Lin HY. On the security of a dynamic id-based authentication scheme for telecare medical information systems. Journal of medical systems. 2013 Jan, 37(2):1–5

[44] Cao T, Zhai J. Improved dynamic id-based authentication scheme for telecare medical information systems. Journal of medical systems. 2013 June, 37(2):1–7

[45] Akgün M, Çağlayan MU. Providing destructive privacy and scalability in RFID systems using PUFs. Ad Hoc Networks. 2015 Sep 1, 32:32-42.

[46] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[47] Gope P, Lee J, Quek TQ. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Transactions on Information Forensics and Security. 2018 May 3, 13(11):2831-43.

[48] Dharminder D, Mishra D, Li X. Construction of RSA-based authentication scheme in authorized access to healthcare services. Journal of medical systems. 2020 Jan, 44(1):1-9.

[49] Siddiqui Z, Abdullah AH, Khan MK, Alghamdi AS. Smart environment as a service: three factor cloud based user authentication for telecare medical information system. Journal of medical systems. 2014 Jan, 38(1):1-4.

[50] Nyangaresi VO, Ma J, Al Sibahee MA, Abduljabbar ZA. Packet Replays Prevention Protocol for Secure B5G Networks. In Proceedings of Seventh International Congress on Information and Communication Technology 2023 (pp. 507-522). Springer, Singapore.

[51] Xie Q, Hu B, Dong N, Wong DS. Anonymous three-party password-authenticated key exchange scheme for telecare medical information systems. PloS one. 2014 Jul 21, 9(7):e102747.

[52] Farash MS, Nawaz O, Mahmood K, Chaudhry SA, Khan MK. A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. Journal of medical systems. 2016 Jul, 40(7):1-7.

[53] Fotouhi M, Bayat M, Das AK, Far HA, Pournaghi SM, Doostari MA. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. Computer Networks. 2020 Aug 4, 177:107333.

[54] Li J, Su Z, Guo D, Choo KK, 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 of Things Journal. 2021 Feb 1, 8(17):13183-95.

[55] Angelis J, Da Silva ER. Blockchain adoption: A value driver perspective. Business Horizons. 2019 May 1, 62(3):307-14.

[56] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan, 4(1): 10-19.

[57] Li CT, Lee CC, Weng CY, Chen SJ. A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems. Journal of medical systems. 2016 Nov, 40(11):1-0.

[58] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. In International Conference on Internet of Things as a Service 2022 (pp. 3-18). Springer, Cham.

[59] Wang W, Huang H, Zhang L, Su C. Secure and efficient mutual authentication protocol for smart grid under blockchain. Peer-to-Peer Networking and Applications. 2021 Sep, 14(5):2681-93.

[60] Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes. 2017 Sep, 10(9):e003800.

[61] Nyangaresi VO, Al Sibahee MA, Abduljabbar ZA, Ma J, Khalefa MS. Biometric-Based Packet Validation Scheme for Body Area Network Smart Healthcare Devices. In 2022 IEEE 21st Mediterranean Electrotechnical Conference (MELECON) 2022 Jun 14 (pp. 726-731). IEEE.

[62] Wei J, Hu X, Liu W. An improved authentication scheme for telecare medicine information systems. Journal of medical systems. 2012 Dec, 36(6):3597-604.

[63] Wu ZY, Lee YC, Lai F, Lee HC, Chung Y. A secure authentication scheme for telecare medicine information systems. Journal of medical systems. 2012 Jun, 36(3):1529-35.

[64] Zhu Z. An efficient authentication scheme for telecare medicine information systems. Journal of medical systems. 2012 Dec, 36(6):3833-8.

[65] Lee TF, Chang IP, Lin TH, Wang CC. A secure and efficient password-based user authentication scheme using smart cards for the integrated epr information system. Journal of medical systems. 2013 Jun, 37(3):1-7.

[66] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In 2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[67] Xu X, Zhu P, Wen Q, Jin Z, Zhang H, He L. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems. Journal of medical systems. 2014 Jan, 38(1):1-7.

[68] Abduljabbar ZA, OmolloNyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, QaysAbduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19, 11(3):55.

[69] Dharminder D, Gupta P. (2019) Pratik security analysis and application of Chebyshev Chaotic map in the authentication protocols. Int J Comput Appl. 2019 Nov, 0(0):1–9.

[70] Dagher GG, Mohler J, Milojkovic M, Marella PB. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable cities and society. 2018 May 1, 39:283-97.

[71] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In 2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[72] Wu F, Xu L, Kumari S, Li X, Das AK, Shen J. A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications. Journal of Ambient Intelligence and Humanized Computing. 2018 Aug, 9(4):919-30.

[73] Radhakrishnan N, Karuppiah M. An efficient and secure remote user mutual authentication scheme using smart cards for Telecare medical information systems. Informatics in Medicine Unlocked. 2019 Jan 1, 16:100092.

[74] He D, Zeadally S, Kumar N, Lee JH. Anonymous authentication for wireless body area networks with provable security. IEEE Systems Journal. 2017 Apr 22, 11(4):2590-601.

[75] Mandal S, Bera B, Sutrala AK, Das AK, Choo KK, Park Y. Certificateless-signcryption-based three-factor user access control scheme for IoT environment. IEEE Internet of Things Journal. 2020 Jan 13, 7(4):3184-97.

[76] Dhagarra D, Goswami M, Sarma PR, Choudhury A. Big Data and blockchain supported conceptual model for enhanced healthcare coverage: The Indian context. Business Process Management Journal. 2019 Mar, 25(7): 1-21.

[77] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In 2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[78] Amin R, Biswas GP. A secure three-factor user authentication and key agreement protocol for tmis with user anonymity. Journal of medical systems. 2015 Aug, 39(8):1-9.

[79] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. In EAI International Conference on Applied Cryptography in Computer and Communications 2022 (pp. 46-64). Springer, Cham.

[80] Li X, Peng J, Obaidat MS, Wu F, Khan MK, Chen C. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Systems Journal. 2019 Mar 19, 14(1):39-50.

[81] Saleem MA, Shamshad S, Ahmed S, Ghaffar Z, Mahmood K. Security analysis on "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems". IEEE Systems Journal. 2021 May 5, 15(4):5557-9.

[82] Zhang L, Zhu S, Tang S. Privacy protection for telecare medicine information systems using a chaotic map-based three-factor authenticated key agreement scheme. IEEE Journal of Biomedical and health informatics. 2017 Jan 12, 21(2):465-75.

[83] Nyangaresi VO, Abduljabbar ZA, Ma J, Al Sibahee MA. Temporary Symmetric Key Based Message Verification Protocol for Smart Energy Networks. In 2022 IEEE 7th International Energy Conference (ENERGYCON) 2022 May 9 (pp. 1-6). IEEE.

[84] Safkhani M, Vasilakos A. A new secure authentication protocol for telecare medicine information system and smart campus. IEEE Access. 2019 Feb 7, 7:23514-26.

[85] Zheng L, Song C, Cao N, Li Z, Zhou W, Chen J, Meng L. A new mutual authentication protocol in mobile RFID for smart campus. IEEE Access. 2018 Oct 15, 6:60996-1005.

[86] Challa S, Das AK, Odelu V, Kumar N, Kumari S, Khan MK, Vasilakos AV. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. Computers & Electrical Engineering. 2018 Jul 1, 69:534-54.

[87] Tewari A, Gupta BB. An internet-of-things-based security scheme for healthcare environment for robust location privacy. International Journal of Computational Science and Engineering. 2020, 21(2):298-303.

[88] Nyangaresi VO, Morsy MA. Towards Privacy Preservation in Internet of Drones. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[89] Li X, Wu F, Khan MK, Xu L, Shen J, Jo M. A secure chaotic map-based remote authentication scheme for telecare medicine information systems. Future Generation Computer Systems. 2018 Jul 1, 84:149-59.

[90] Guo C, Chang CC. Chaotic maps-based password-authenticated key agreement using smart cards. Communications in Nonlinear Science and Numerical Simulation. 2013 Jun 1, 18(6):1433-40.

[91] Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Khalefa MS, Honi DG. MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. In International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures 2022 (pp. 16-36). Springer, Cham.

[92] Jiang Q, Ma J, Lu X, Tian Y. Robust chaotic map-based authentication and key agreement scheme with strong anonymity for telecare medicine information systems. Journal of medical systems. 2014 Feb, 38(2):1-8.

[93] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. In International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference 2022 (pp. 325-340). Springer, Cham.

[94] Dimitrov DV. Blockchain applications for healthcare data management. Healthcare informatics research. 2019 Jan 31, 25(1):51-6.

[95] Salem FM, Amin R. A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. Information sciences. 2020 Jul 1, 527:382-93.

[96] Nyangaresi VO, Abduljabbar ZA, Abduljabbar ZA. Authentication and Key Agreement Protocol for Secure Traffic Signaling in 5G Networks. In 2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC) 2021 Dec 20 (pp. 188-193). IEEE.

[97] Srivastava K, Awasthi AK, Kaul SD, Mittal RC. A hash based mutual RFID tag authentication protocol in telecare medicine information system. Journal of medical systems. 2015 Jan, 39(1):1-5.

[98] Li CT, Weng CY, Lee CC. A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system. Journal of medical systems. 2015 Aug, 39(8):1-8.

[99] Zhou Z, Wang P, Li Z. A quadratic residue-based RFID authentication protocol with enhanced security for TMIS. Journal of ambient intelligence and humanized computing. 2019 Sep, 10(9):3603-15.

[100] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

[101] Xu H, Ding J, Li P, Zhu F, Wang R. A lightweight RFID mutual authentication protocol based on physical unclonable function. Sensors. 2018 Mar 2, 18(3):760.

[102] Bendavid Y, Bagheri N, Safkhani M, Rostampour S. Iot device security: Challenging "a lightweight rfid mutual authentication protocol based on physical unclonable function". Sensors. 2018 Dec 15, 18(12):4444.

[103] Alladi T, Chamola V. HARCI: A two-way authentication protocol for three entity healthcare IoT networks. IEEE Journal on Selected Areas in Communications. 2020 Sep 1, 39(2):361-9.

[104] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[105] Masud M, Gaba GS, Choudhary K, Hossain MS, Alhamid MF, Muhammad G. Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. IEEE Internet of Things Journal. 2021 May 14, 9(4):2649-56.

[106] Kwon D, Park Y, Park Y. Provably secure three-factor-based mutual authentication scheme with PUF for wireless medical sensor networks. Sensors. 2021 Sep 9, 21(18):6039.

[107] Albahri OS, Zaidan AA, Zaidan BB, Hashim M, Albahri AS, Alsalem MA. Real-time remote health-monitoring Systems in a Medical Centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects. Journal of medical systems. 2018 Sep, 42(9):1-47.

[108] Taleb H, Nasser A, Andrieux G, Charara N, Motta Cruz E. Wireless technologies, medical applications and future challenges in WBAN: A survey. Wireless Networks. 2021 Nov, 27(8):5271-95.

[109] Nyangaresi VO, Abduljabbar ZA, Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. In Ad Hoc Networks and Tools for IT 2021 Dec 6 (pp. 188-204). Springer, Cham.

[110] Madhusudhan R, Nayak CS. A robust authentication scheme for telecare medical information systems. Multimedia Tools and Applications. 2019 Jun, 78(11):15255-73.

[111] Sureshkumar V, Amin R, Obaidat MS, Karthikeyan I. An enhanced mutual authentication and key establishment protocol for TMIS using chaotic map. Journal of Information Security and Applications. 2020 Aug 1, 53:102539.

[112] Yang CC, Wang RC, Liu WT. Secure authentication scheme for session initiation protocol. Computers & Security. 2005 Aug 1, 24(5):381-6.

[113] Huang HF. A new efficient authentication scheme for session initiation protocol. In9th Joint International Conference on Information Sciences (JCIS-06) 2006 Oct (pp. 402-404). Atlantis Press.

[114] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Dec 17, 11(24):12040.

[115] Ostad-Sharif A, Abbasinezhad-Mood D, Nikooghadam M. An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. International journal of communication systems. 2019 Mar 25, 32(5):e3913.

[116] Nikooghadam M, Amintoosi H. An improved secure authentication and key agreement scheme for healthcare applications. In2020 25th International Computer Conference, Computer Society of Iran (CSICC) 2020 Jan 1 (pp. 1-7). IEEE.

[117] Limbasiya T, Sahay SK, Sridharan B. Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system. Information Systems Frontiers. 2021 Aug, 23(4):835-48.

[118] Gaikwad VP, Tembhurne JV, Meshram C, Lee CC. Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. The Journal of Supercomputing. 2021 Aug, 77(8):8281-304.

[119] Nyangaresi VO, Abood EW, Abduljabbar ZA, Al Sibahe MA. Energy Efficient WSN Sink-Cloud Server Authentication Protocol. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 Oct 22 (pp. 1-6). IEEE.

[120] Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems. 2018 May 1, 82:727-37.

[121] Li X, Niu J, Kumari S, Liao J, Liang W, Khan MK. A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. Security and Communication Networks. 2016 Oct, 9(15):2643-55.

[122] Das AK, Sutrala AK, Odelu V, Goswami A. A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks. Wireless Personal Communications. 2017 Jun, 94(3):1899-933.

[123] Arshad R, Ikram N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimedia tools and applications. 2013 Sep, 66(2):165-78.

[124] Farash MS, Attari MA. An enhanced authenticated key agreement for session initiation protocol. Information Technology and Control. 2013 Dec 12, 42(4):333-42.

[125] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In 2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[126] Tang H, Liu X. Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol. Multimedia tools and applications. 2013 Aug, 65(3):321-33.

[127] Kumari S, Li X, Wu F, Das AK, Choo KK, Shen J. Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems. 2017 Mar 1, 68:320-30.

[128] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[129] Kumari S, Khan MK, Atiquzzaman M. User authentication schemes for wireless sensor networks: A review. Ad Hoc Networks. 2015 Apr 1, 27:159-94.

[130] Mahmood K, Naqvi H, Alzahrani BA, Mehmood Z, Irshad A, Chaudhry SA. An ameliorated two-factor anonymous key exchange authentication protocol for mobile client-server environment. International Journal of Communication Systems. 2018 Dec, 31(18):e3814.

[131] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Sep, 3(5):1-6.

[132] Kumari S, Li X, Wu F, Das AK, Arshad H, Khan MK. A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps. Future Generation Computer Systems. 2016 Oct 1, 63:56-75.

[133] Yoon EJ, Yoo KY. Cryptanalysis of DS-SIP authentication scheme using ECDH. In2009 international conference on new trends in information and service science 2009 Jun 30 (pp. 642-647). IEEE.

[134] Nyangaresi VO. ECC based authentication scheme for smart homes. In 2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[135] Kumari S, Chaudhary P, Chen CM, Khan MK. Questioning key compromise attack on Ostad-Sharif et al.'s authentication and session key generation scheme for healthcare applications. IEEE Access. 2019 Mar 19, 7:39717-20.

[136] Yoon EJ, Shin YN, Jeon IS, Yoo KY. Robust mutual authentication with a key agreement scheme for the session initiation protocol. IETE Technical Review. 2010 May 1, 27(3):203-13.

[137] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[138] Kumari S. Design flaws of "an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography". Multimedia tools and applications. 2017 Jun, 76(11):13581-3.

[139] Khatoon S, Rahman SM, Alrubaian M, Alamri A. Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment. IEEE access. 2019 Apr 9, 7:47962-71.

[140] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. In International Conference for Emerging Technologies in Computing 2021 Aug 18 (pp. 3-20). Springer, Cham.

[141] Qiao H, Dong X, Shen Y. Authenticated key agreement scheme with strong anonymity for multi-server environment in TMIS. Journal of medical systems. 2019 Nov, 43(11):1-3.

[142] Liu X, Ma W, Cao H. MBPA: A medibchain-based privacy-preserving mutual authentication in TMIS for mobile medical cloud architecture. IEEE Access. 2019 Oct 14, 7:149282-98.

[143] Nyangaresi VO, Moundounga AR. Secure Data Exchange Scheme for Smart Grids. In 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[144] Liu X, Ma W, Cao H. NPMA: A novel privacy-preserving mutual authentication in TMIS for mobile edge-cloud architecture. Journal of Medical Systems. 2019 Oct, 43(10):1-6.

[145] Naqvi H, Chaudhry S, Mahmood K. An improved authentication protocol for SIP-based VoIP. InInternational Conference on Recent Advances in Computer Systems 2015 Nov (pp. 7-12). Atlantis Press.

[146] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[147] Heydari M, SajadSadough SM, Chaudhry SA, Farash MS, Mahmood K. An improved one-to-many authentication scheme based on bilinear pairings with provable security for mobile pay-TV systems. Multimedia Tools and Applications. 2017 Jun, 76(12):14225-45.

[148] Chaudhry SA, Shon T, Al-Turjman F, Alsharif MH. Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems. Computer Communications. 2020 Mar 1, 153:527-37.

[149] Nyangaresi VO, Abd-Elnaby M, Eid MM, NabihZakiRashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 May 6:e4528.

[150] Alzahrani BA, Chaudhry SA, Barnawi A, Al-Barakati A, Alsharif MH. A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks. Symmetry. 2020 Feb 15, 12(2):287.

[151] Shamshad S, Ayub MF, Mahmood K, Kumari S, Chaudhry SA, Chen CM. An enhanced scheme for mutual authentication for healthcare services. Digital Communications and Networks. 2022 Apr 1, 8(2):150-61.

[152] Wu F, Xu L, Kumari S, Li X. An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. Multimedia Systems. 2017 Mar, 23(2):195-205.

[153] Srinivas J, Mishra D, Mukhopadhyay S. A mutual authentication framework for wireless medical sensor networks. Journal of medical systems. 2017 May, 41(5):1-9.

[154] Nyangaresi VO, Ibrahim A, Abduljabbar ZA, Hussain MA, Al Sibahee MA, Hussien ZA, Ghrabat MJ. Provably Secure Session Key Agreement Protocol for Unmanned Aerial Vehicles Packet Exchanges. In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2021 Dec 9 (pp. 1-6). IEEE.

[155] Xu X, Jin ZP, Zhang H, Zhu P. A dynamic ID-based authentication scheme based on ECC for telecare medicine information systems. InApplied Mechanics And Materials 2014 (Vol. 457, pp. 861-866). Trans Tech Publications Ltd.

[156] Islam SK, Khan MK. Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. Journal of medical systems. 2014 Oct, 38(10):1-6.

[157] Shehzad Ashraf Chaudhry, Husnain Naqvi, Taeshik Shon, Muhammad Sher, and Mohammad SabzinejadFarash. Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. Journal of Medical Systems. 2016 Apr, 39(6):66.

[158] Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. IEEE Access. 2019 Jan 21, 7:12557-74.

[159] Ali Z, Hussain S, Rehman RH, Munshi A, Liaqat M, Kumar N, Chaudhry SA. ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments. IEEE Access. 2020 Jun 10, 8:107993-8003.

[160] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abduljaleel IQ, Abood EW. Towards Security and Privacy Preservation in 5G Networks. In 2021 29th Telecommunications Forum (TELFOR) 2021 Nov 23 (pp. 1-4). IEEE.

[161] Qiu S, Xu G, Ahmad H, Wang L. A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems. IEEE access. 2017 Dec 8, 6:7452-63.

[162] Amin R, Islam SH, Biswas GP, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems. 2018 Mar 1, 80:483-95.

[163] Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. Computers & Electrical Engineering. 2017 Oct 1, 63:182-95.

[164] Fan K, Jiang W, Li H, Yang Y. Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics. 2018 Jan 18, 14(4):1656-65.

[165] Chen X, Geng D, Zhai J, Liu W, Zhang H, Zhu T. Security analysis and enhancement of the most recent RFID protocol for telecare medicine information system. Wireless Personal Communications. 2020 Sep, 114(2):1371-87.

[166] Ravanbakhsh N, Nazari M. An efficient improvement remote user mutual authentication and session key agreement scheme for e-health care systems. Multimedia Tools and Applications. 2018 Jan, 77(1):55-88.

[167] Nyangaresi VO, Khalefa MS, Abduljabbar ZA, Al Sibahee MA. Low Bandwidth and Side-Channeling Resilient Algorithm for Pervasive Computing Systems. In Proceedings of International Conference on Communication and Computational Technologies 2023 (pp. 193-208). Springer, Singapore.

[168] Mo J, Hu Z, Lin Y. Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks. Security and Communication Networks. 2020 Feb 19, 2020.

[169] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. In Artificial Intelligence and Sustainable Computing 2022 (pp. 91-111). Springer, Singapore.

[170] Majzoobi M, Rostami M, Koushanfar F, Wallach DS, Devadas S. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching. In2012 IEEE Symposium on Security and Privacy Workshops 2012 May 24 (pp. 33-44). IEEE.

[171] Malialis K, Devlin S, Kudenko D. Distributed reinforcement learning for adaptive and robust network intrusion response. Connection Science. 2015 Jul 3, 27(3):234-52.

[172] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. In the 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[173] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map. IEEE Access. 2022 Feb 11, 10:26257-70.

[174] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[175] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy SA. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical and Computer Engineering (IJECE). 2023 Feb, 13(1):335-46.

[176] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Oct 17, 11(4):66.

[177] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Nov 16.