Secure Remote User Authentication Scheme on Health Care, IoT and Cloud Applications: A Multilayer Systematic Survey

Vani Rajasekar[1], Premalatha Jayapaul[1], Sathya Krishnamoorthi[1], Muzafer Saračević[2]

[1] Kongu Engineering College, Perundurai Erode, Thoppupalayam, 638060, Tamil Nadu, India; vanikecit.cse@kongu.ac.in, jprem@kongu.ac.in, vanikecit.cse@kongu.edu

[2] Department of Computer Sciences, University of Novi Pazar, Dimitrija Tucovića bb, 36300 Novi Pazar, Serbia; muzafers@uninp.edu.rs

Abstract: Secure remote user authentication is an authentication technique in which the remote server authorizes the identity of the user through an insecure communication network. Since then diverse remote user authentication schemes have been proposed, but each category has its advantages and disadvantages. Besides its strength and weakness, remote user authentication systems have a great impact on real-time applications such as E-health applications, telemedicine applications, Internet of Things (IoT), Cloud, and Multi-server applications. The implementation of the Tele Medicine Information System (TMIS) over public networks continues to disclose confidential information to unauthorized entities. Similarly, remote user authentication techniques have become essential in accelerating IoT as well. Security is a major concern in IoT because it allows secure access to remote services. Cloud computing services and a Multi-server environment share data among different end-users through the internet which also needs security as its paramount concern. Although intensive efforts were made in designing remote user authentication scheme for health care, IoT, Multi-server and cloud applications, the majority of these applications suffers either from security attacks or lagging of critical features. This paper presents an analytical and comprehensive survey of various remote user authentication techniques and categorizes them based on different applications. Furthermore, the state of art recent remote user authentication techniques have been compared, their advantages, key features, computational cost, storage cost, and communication cost are highlighted.

Keywords: remote user authentication; e-health; telemedicine; internet of things; multi-server; security

1 Introduction

The Internet has become an important part of daily life. With the fast growth of Internet technology, we can enable any service from any location and at any time. In Health care, Internet of Things (IoT), Multi-Server environment, Cloud applications, remote user authentication is becoming an essential part to access the precious service or resource. Remote user authentication [1] is a vital component of every security architecture. Authorization provides Identity-Based privileges and without authentication, audit trails will not have transparency. When we can't accurately differentiate an authorized party from an illegal party, secrecy and dignity will be violated. Similarly to avail of the resource located at remote places every user should possess the proper access rights. One of the most basic and convenient protection mechanisms is the use of a password-based authentication scheme. Some of the examples of password-based authentication schemes are Automated Teller Machines (ATM), Database Management Systems, and Personal Digital Assistants (PDA). There are two main problems associated with the password mechanism one is passwords are stored in database systems as a plain not that can be easily accessed by the database administrator. The other problem is an attacker can impersonate a legitimate user by grabbing the user ID and PW from the table of passwords. To overcome these issues in a traditional authentication scheme dynamic id-based authentication scheme has been proposed. In addition to ID bases authentication, smart card-based authentication also seems to be one of the emerging authentication mechanisms. The researcher has presented that most of the smartcard-based authentication scheme overcomes the issues in dynamic ID and password scheme. Telemedicine is an evolving technology that supports a significant part of patient healthcare. This is a medical application that allows patients to have medical appointments outside hospitals using videoconferencing or digital imaging systems. Tier 1 uses the vital signals through wireless sensors, Data are transferred from Tier 2 to Tier 3. Tier 3 processes and generate responses. This enhances secure health monitoring through mobile health. IoT and Big data analytics are not point Information Communication Technology (ICT) paradigms that possess health care services. A smartcard-based efficient three-factor remote user authentication can be used to provide user anonymity and avoids security attacks or threats.

Recent advancement in research shows that IoT is useful in the surveillance of border controls, remote preparation, large scale deployment to enterprise-level, proactive maintenance of facilities, etc. In addition to health care, IoT, remote user authentication plays a major role in cloud computing applications. Remote cloud computing systems are, fundamentally, rather distributed in nature, and heterogeneous. In the mobile cloud computing environment, the mobile user authentication scheme should have a trusted third party, secure mobile user authentication, mutual authentication should exist among mobile users and cloud servers. Various symmetric and asymmetric algorithms can be employed to provide the remote user authentication scheme. The most commonly used algorithm includes RSA, DES, AES, ECC, and Hyperelliptic curve cryptography. Each of these algorithms has its own merits and demerits. In this paper, multi-layer systematic reviews on remote user authentication schemes have been proposed. The first layer intends to survey on the impact of remote user authentication schemes on health care applications, telecare medicines, and wireless body area networks. The second layer aims to make a systematic survey on the impacts of remote user authentication on the Internet of Things applications. The third provides a detailed survey of multi-server and cloud computing applications. The fourth layer provides a detailed analysis of various security threats that those different systems have undergone. In addition to security attacks computational and communication analyses of different schemes were proposed (see Figure 1).

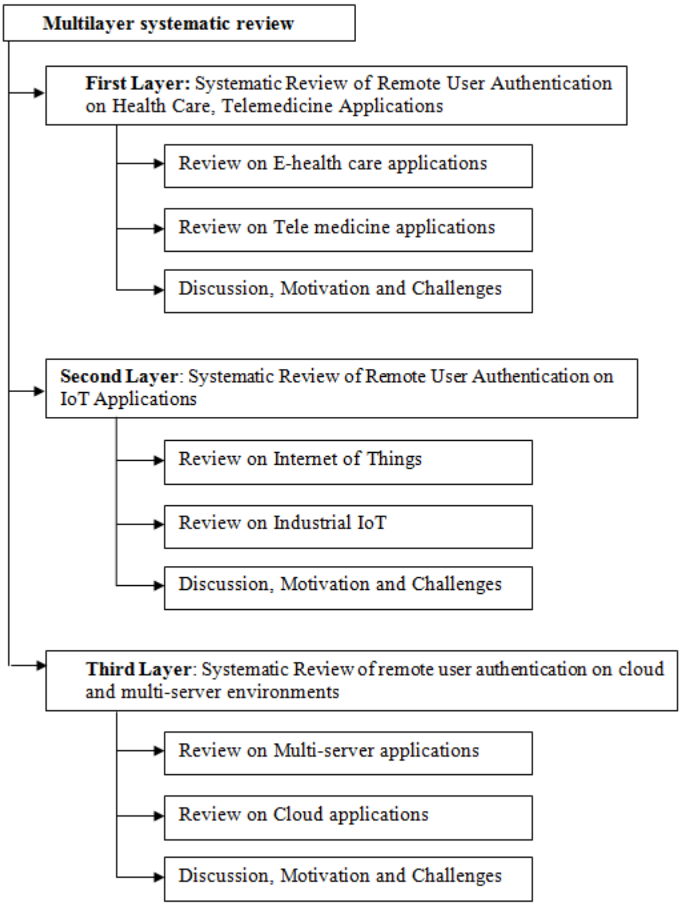
Multilayer systematic review
First Layer: Systematic Review of Remote User Authentication on Health Care, Telemedicine Applications
Review on E-health care applications
Review on Tele medicine applications
Discussion, Motivation and Challenges
Second Layer: Systematic Review of Remote User Authentication on IoT Applications
Review on Internet of Things
Review on Industrial IoT
Discussion, Motivation and Challenges
Third Layer: Systematic Review of remote user authentication on cloud and multi-server environments
Review on Multi-server applications
Review on Cloud applications
Discussion, Motivation and Challenges

Figure 1

A framework of multi-layer remote authentication schemes

2 First Layer Systematic Review of Remote User Authentication on Health Care and Telemedicine Applications

Telemedicine technologies are commonly featured in scientific literature and have gained significant prominence recently. The keywords used for this survey are telemedicine, sensor, health care, security, authentication schemes. From the literature of varied databases such as science direct, IEEE explores, Web of Science the source of this layer was carefully screened. The study of this layer includes recent research in the field of telemedicine, healthcare for the last five years from 2015-2020.

2.1 Review of Authentication on Health Care Applications

Zhang et al. [2] design a dynamic privacy-protective measure that offers server-side biometric authentication. In their process, user confidentiality during authentication and key negotiation processes can be completely conserved. They have shown that their scheme is lightweight, as only hash and BioHash functions are taken into consideration. The advantage of their scheme:

- A dynamic verification table is provided to enhance the security
- Meet the demands of energy use and the protection needs of e-health systems.

The security tools used for their scheme are the Real-or-Random model. The communicational cost and computational costs are 164bytes and 0.0989 seconds respectively. Jiang et al. [3] proposed an efficient security protocol for wearable health monitoring services. Their methodology enables secure communication established between the medical professional and wearable sensors. This is an efficient end-end authentication protocol mainly developed based on quadratic residues. Their scheme enhances the security of Amin et al. protocol as their scheme prone to desynchronization attacks, mobile device attacks, sensor key exposure.

Xiong et al. [4] developed an enhanced 1-round authentication scheme for wireless body area networks. The communication cost of their scheme is 11.15 ms. Fatma et al. [5] developed an authentication protocol IoT-based health care application. They have added two important improvements in the recent M2C mutual authentication protocol that is based on health care RFID systems. The M2M authentication protocol they have developed is based on Elliptic Curve Cryptography RFID systems. The M2M authentication protocol they have developed based on Elliptic Curve Cryptography (ECC) and security was measured based on two well-known protocol verifier tools AVISPA and Proverif.

Their application is mainly used for resource-constrained devices. Yessad et al. [6] proposed a reliable authentication scheme for medical body area networks. It is proposed as a security solution. The routine activities of the patient such as walking, running, routine activities are periodically analyzed using sensors. They build an empirical model for assessing the physical and logical effect of attacks using the learning phase and the authentication phase.

2.2 Review of Authentication on the Telemedicine Information System (TMIS)

Telemedicine is an emerging concept in the field of health yet some challenges remain particularly in securing communication over the internet in remote monitoring systems. To improve protection, biometric features are used as a third factor in the design of a strong authentication scheme. Chaudry et al. [7] developed a multi-server biometric authentication scheme for establishing secure communication between the medical practitioner and patient. Chaudry et al. proposed that their scheme can change the password used in the authentication system without the intervention of the Central Management System (CMS). Proverif tool was used to ensure the security of their proposed scheme. The major advantage of their scheme is it is secure over an insecure channel and it assures perfect secrecy, light weightlessness. The security-related problems in the telemedicine world can be solved by improving the procedure of patient enrolment, which is a normal identity-proofing process.

Narwal et al. [8] proposed a mutual authentication and key agreement scheme for the telemedicine system which addresses the mobility and openness raising issues like complicated requirements and privacy leakage. It is analyzed with an ns2 simulator along with a counterpart scheme for end-end delay and throughput. SEEMAKA achieves superior performance with regard to overhead production, energy dissipation, and safety features. Zhang et al. [9] proposed a three-factor authentication scheme for telecare medicine systems based on chaotic map-based cryptography. Amin et al. [10] developed anonymity preserving mutual authentication scheme for wireless medical sensor networks. Their scheme offers robust mutual authentication and user-friendly password change phases included. It protects against mobile stolen attacks, offline password guessing attacks, and replay attacks. AVISPA and BAN Logic structures were used to verify the security of the proposed scheme. The main advantage includes cost-effectiveness and robustness compared to other existing approaches. Saracevic et al. [11, 12] proposed a novel iris recognition approach based on stylometric features. In the first stage, filtering and scanning to weed out duplicates and irrelevant studies of remote health monitoring systems focused on security concerns on health care and telemedicine. In the second stage of this layer, the authors performed a screening of papers collected from the first stage based on the security and privacy of telemedicine applications.

The comparison of remote user authentication schemes on health care and telemedicine application is specified in Table 1 (Legend: AS = Authentication Schemes; Y= Year; R = Reviewed on; K= Key feature; ST = Security tool used; CS1 = Computational cost; CS2= Communication cost).

Table 1

Comparison of remote user scheme on health care and telemedicine applications

AS	Y	R	K	ST	Performance parameters	
					CS1	CS2
Mohammed et al. [13]	2018	Existing authentication schemes	1.Secure and lightweight 2.Converts Patient biometric into key	AVISPA	200 ms	200 bytes
Sowjanya et al. [14]	2020	Li et al. [4] scheme	1.End-end authentication 2.Enhance medical data security	1.BAN logic 2.AVISPA	130 ms	2272 bits
Alzahrani et al. [15]	2020	Xu et al. [16] scheme	1. The Novel and robust patient monitoring scheme	1.BAN logic 2. Proverif	-	2624 bits
Jiang et al. [17]	2017	Lu et al. scheme [18]	1.Fulfills session key secrecy	Proverif	8.95 ms	1120 bits
Zhang et al. [2]	2017	-	1. Dynamic privacy protection scheme 2. Preserves user anonymity	Real-or-Random	0.09 seconds	164 bytes
Zhang et al. [9]	2017	Mishra’s et al. [19] scheme	1.Chaotic map-based cryptography	-	4TC +3Ts+20 Th	1312 bits
Dhillon et al. [20]	2018	-	1. IoT based health care 2. Maintains key freshness	AVISPA	1TEXP + 14TH	-
Ravanbakhsh et al. [21]	2018	Amin et al. scheme [22]	1. Uses ECC and Fuzzy 2. Robust against privileged-insider	1.AVISPA 2.Random oracle	-	-
Chaudry et al. [7]	2016	Amin et al. [22]	1. Secure communication 2. Facility to change password	Proverif	15.63 ms	1664 bits

Merabat et al. [5]	2020	-	1. Efficient and scalable 2.Uses ECC for M2M	1.AVISPA 2.Proverif	485 ms	7N bits
Amin et al. [10]	2016	-	1. Anonymity preserving mutual authentication	1.BAN logic 2.AVISPA	0.0136 ms	2112 bits
Yessad et al. [6]	2017	-	1.Developed analytical model to mitigate attacks	BAN Logic	TAR-91.6%	Detection rate=97%

3 Second Layer Systematic Review of Remote User Authentication on IoT Applications

Internet of Things (IoT) is any internet substructure entity associated with an advanced global dynamic network. The IoT is composed of three elements: things, communication networks, and Informatics. Before this, researchers focused on new strategies and successful approaches to properly integrating WSNs into the IoT situation.

3.1 Review of Authentication Schemes for IoT Applications

Li et al. [23] proposed a two-factor authentication scheme suitable for the Industrial Internet of Things (IIoT). They utilized improved requirements set for the commercial Internet of Things. They evaluate 42 specific schemes to prove their requirements are successful. Through implementing the "honeywords" strategy, how Xde capture attacks are detected and thwarted. Ostad et al. [24] identified a data transmission technique in IoT networks in which it is protected by three parties through the design of a lightweight authenticated key agreement. Their scheme offers perfect forward secrecy, best storage cost when compared to other related schemes. Their scheme resists id guessing, password guessing, replay, and impersonation attack. Result analysis concluded that their scheme is efficient and appropriate for real-time IoT-based wireless sensor applications.

Xuelei et al. [25] proposed an improved biometric authentication scheme using ECC. The security of the proposed scheme is analyzed with Random oracle and BAN logic [26]. Nikravan et al. [27] proposed an advanced multi-factor scheme based on the bilinear pairing of IoT. The protocol uses ECC, establishes a fresh session key, several security requirements are satisfied. Their result analysis has shown that their scheme is resistant to well-known IoT related attacks and more suitable for well-known resource-constrained environments such as WSN.

Roy et al. [28] proposed an anonymous user authentication scheme that is based on an enotended chaotic map. Their scheme overcomes the higher computational cost of elliptic curve point multiplication and modular operation. Biometric fuzzy enotractors are utilized to enhance the performance metrics and this scheme is well suited for real-time e-healthcare systems. Dharminder et al. [29] analyzed flaws and construct a remote user authentication scheme based on smart cards. Their scheme uses lightweight cryptographic operations such as XOR operations and hash functions. The random oracle method was used to analyze the security of the proposed protocol [30]. Rajaram et al. [31] analyzed the security pitfalls of Awasthi’s scheme and proposed eUASBP based mutual authentication scheme. It resists all possible attacks with smart card-based applications, enhances session key agreement, it detects the wrong password at the earliest possible.

Smart IoT architecture is composed of diverse microdevices and gathers different types of real-time information. It is not effective for realistic IoT systems, however, since the cost of computation and communication could be raised when the scale of the IoT networks and the distance between users is raised (see Table 2, Legend: AS = Authentication Schemes; Y= Year; R = Reviewed on; K= Key feature; ST = Security tool used; CS1 = Computational cost; CS2= Communication cost).

Table 2
Comparison of remote user scheme on IoT applications

AS	Y	R	K	ST	Performance parameters	
					CS1	CS2
Li et al. [23]	2019	Amin et al. scheme [10]	1. Evaluate 42 representative scheme to show the effectiveness	AVISPA	-	-
Ostad et al. [24]	2019	Amin et al. scheme [10]	1.Provides perfect forward secrecy 2. Best storage cost	AVISPA	0.0132 ms	5376 bits
Xuelei et al. [25]	2018	Lu et al. scheme [18]	1. Bio hash function and Elliptic curve authentication scheme using ECC.	1. Random oracle 2. BAN Logic	Communication cost=3TM + 11Th + 2Tsym	
Amintoosi et al. [26]	2019	-	1. Uses sparse representation 2. K singular value decomposition (K-SVD)	1.K-SVD 2. OMP suit	Accuracy=0.97 , sensitivity=0.983, specificity=0.978, prevalence=0.072	

Nikravan et al. [27]	2020	-	1. Uses the concept of bilinear pairing and identity-based cryptography	1.BAN Logic 2.AVISPA	1.2 sec	16th + 7tmul + 2tp + 8tex
Roy et al. [28]	2018	-	1. Enotended chaotic map-based user authentication 2. Uses biometric fuzzy enotractor	1.Real-or-random 2.Proverif 3.BAN Logic	23.52 ms	992 bits
Dharminder et al. [29]	2020	Limbasiya et al. scheme [30]	1.Uses lightweight cryptographic operations	1.Random oracle	-	-
Rajaram et al. [31]	2020	Awasthi et al. scheme [32]	1. eUASBP ensures strong security and mutual authentication	BAN Logic	Storage cost= 1152 bits	1216 bits

4 Third Layer Systematic Review of Remote User Authentication on Cloud and Multi-Server Environments

Cloud computing is a cutting-edge technology that provides services without direct user control based on resource demand It is highly scalable, stable, and allows anywhere access to the data in indeed time.

4.1 Review of Authentication Schemes for Cloud Applications and Multi-Server Applications

Karuppiah et al. [33] proposed a generic authentication framework based on ID which provides roaming service. In GLOMONET, the construction of secure anonymous user authentication is difficult because the wireless networks are generally subjected to the vulnerability of attacks. Moreover, mobile devices are generally resource-constrained in terms of processing, storage, and communication [34, 35].

Feng et al. [36] proposed an anonymous key agreement scheme for a multi-server environment. They believed that biometrics is a preferred alternative for secure and reliable authentication and uses the elliptic curve cryptosystem.

The information can be analyzed in various cloud services where the user can access it remotely, whenever needed. Yet, the key concerns to safeguard data because the data has been in a remote server it is prone to malicious attacks and can be disrupted at times. So the advancement of a secure communications mechanism for data through authentication and access control is indispensable (see Table 3, Legend: AS = Authentication Schemes; Y= Year; R = Reviewed on; K= Key feature; ST = Security tool used; CS1 = Computational cost; CS2= Communication cost).

Table 3

Comparison of remote user scheme on Multi-server applications

AS	Y	R	K	ST	Performance parameters	
					CS1	CS2
Karuppiah et al. [33]	2017	Miyoung et al. scheme [34]	1.An ID-based generic framework for GLOMONET	Proverif	1.62 ms	2272 bits
Challa et al. [35]	2020	-	1. ECC based anonymous authentication scheme	1.AVISPA 2.BAN Logic	0.32 sec	1536 bits
Feng et al. [36]	2017	Kumari et al. scheme [37]	1. Elliptic curve cryptosystem and biometrics are combined	BAN Logic	0.708 seconds	3531 bits
Liu et al. [38]	2018	Lu et al. scheme [18]	1. Three handshake mechanism with privacy protection	BAN Logic	1.148 ms	Energy dissipation= 6.924 mJ
Joseph et al. [39]	2020	-	1. Multimodal biometric authentication (Finger + Palm print) 2. Uses AES, DES, and Blowfish algorithms	-	1. FAR=0.15 2. FRR=94.5	
Nunes et al. [40]	2019	-	1. Biometric authentication combining multi-party and fuzzy vault 2. Enrolls 1000 users within a second	-	GAR of ≈90% FAR of ≈3%.	

Sharma et al. [41]	2018	-	1. Authentication based on quantum key distribution 2.Entanglement based QKD	AVISPA	1.Key Rate=4.11 bit/s 2.Error rate=9.21%	
Shashidhara et al. [42]	2020	Xu et al. scheme [43]	1. Provable security established through mobile user	AVISPA	0.0187 seconds	2560 bits
Jangirala et al. [44]	2017	Shunmuganathan et al. scheme [45]	1. Dynamic identity-based authentication	1. BAN logic 2.AVISPA	(25 Th & 12Tx)	1120 bits
Zhang et al. [46]	2017	Odelu et al. scheme [47]	1.Uses secure sketch and Chebyshev chaotic map 2.Secure sketch to solve fuzzy in biometrics	1.BAN logic 2.Proverif	1.55 seconds	1952 bits
Nguyen et al. [48]	2018	-	1. Uses fuzzy commitment and random orthonormal projection scheme	-	1.FAR=7% 2.FRR=7%	
Ying et al. [49]	2019	-	1. Self-certified public-key cryptography based on ECC	-	3.54 ms	368 bytes
Chandrakar et al. [50]	2017	Wen et al. scheme [51]	1.Secure three-factor authentication scheme	1.BAN Logic 2.AVISPA	-	3232 bits

Liu et al. [38] proposed a lightweight and efficient multi-server authentication based on dynamic biometrics. They used three handshakes to establish mutual authentication and all the remote services are offered with privacy protection. The protocol is more robust and fault-tolerant.

Nunes et al. [40] proposed a biometric authentication scheme based on multi-party computation techniques and Fuzzy enotractors or vaults. Their scheme involves the development of a modular, scalable, and safe framework allowing non-interactive re-enrollment of users.

The main advantages of this scheme are around 1000 users are able to enroll within a second. Shashidhara et al. [42] developed an authentication protocol that achieves provable security. Jangirala et al. [44] proposed an identity-based authentication scheme for a multi-server environment. The major application of their scheme is resource-constrained wireless sensor networks.

Zhang et al. [46] proposed a secure three-factor authentication scheme based on a sketch algorithm and Chebyshev chaotic map. The purpose of including a sketch algorithm is to solve the problems involved in fuzzy characters of biometrics.

Nguyen et al. [48] modeled a biometric-based authentication scheme that helps to mitigate malicious attacks. Their scheme specifically attacks against sensitive information threat and also protect against insider attacks.

Ying et al. [49] modeled a remote user authentication protocol that is lightweight and self-certified public-key cryptography. They developed this scheme for 5G multi-server networks and uses ECC for self-certified public-key cryptography.

The advantage of their scheme includes:

- Able to provide protection of privacy required in 5 G applications
- It has greater efficiency in terms of communication and computational cost.

Chandrakar et al. [50] identified a secure safe three-factor authentication scheme for a multi-server environment. Yao et al. [52] proposed an RLWE based remote user authentication that is privacy-preserving and developed mainly for single and multi-server environments. They have included user biometric in their authentication scheme to enhance security, which is termed as RLWE based Remote Biometric Authentication Scheme (RRBAS). Their scheme satisfies the authenticated key agreement scheme (AKA). which resists all types of security attacks and provides post-quantum secure features.

5 Motivation towards Security Requirements and Attacks

This section list out and describes the various security attacks that an optimal remote user authentication scheme should tolerate. The comparison of various security attacks on remote user authentication schemes is specified in Table 4.

Table 4

Comparison of security attacks on remote user authentication schemes

Authentication scheme	1	2	3	4	5	6	7	8	9	10	11	12	13
Mohammed et al. [13]	×	×	√	×	×	×	×	×	×	×	√	×	√
Sowjanya et al. [14]	√	×	×	√	×	×	×	×	×	√	√	×	√
Alzahrani et al. [15]	×	×	√	×	×	×	×	×	×	×	√	×	√

Jiang et al. [17]	×	×	√	×	×	×	×	×	×	×	√	×	√
Zhang et al. [2]	×	√	√	×	×	√	×	√	×	×	×	×	×
Zhang et al. [9]	×	×	×	×	×	×	×	×	×	×	×	×	×
Dhilon et al. [20]	×	√	×	×	×	×	×	×	×	×	√	√	×
Ravanbakhsh et al. [21]	×	×	×	×	×	×	×	×	×	×	×	×	×
Chaudry et al. [7]	√	√	×	×	×	×	×	×	√	×	×	×	×
Merabat et al. [5]	×	√	√	×	×	√	×	×	×	√	×	×	×
Amin et al. [10]	×	×	×	×	×	√	×	√	×	×	√	×	√
Yessad et al. [6]	×	×	√	×	×	×	×	×	×	×	√	×	√
Jiang et al. [3]	×	×	√	×	×	×	×	×	×	×	√	×	√
Li et al. [4]	×	√	×	×	√	×	√	√	×	×	×	×	×
Xrwal et al. [8]	×	×	×	√	×	×	×	×	√	×	×	×	×
Sasikaladevi et al. [53]	×	×	×	×	√	×	×	×	×	×	×	×	×
Li et al. [23]	×	×	√	×	×	×	×	×	×	×	√	×	√
Ostad et al. [24]	×	√	×	√	×	×	√	×	×	×	√	×	√
Xuelei et al. [25]	×	×	×	×	×	×	×	×	×	×	√	×	√
Nikravan et al. [27]	×	√	×	×	×	×	√	×	×	√	×	×	×
Roy et al. [28]	×	×	×	×	×	×	×	×	×	√	×	√	×
Dharminder et al. [29]	×	×	×	×	×	×	×	×	×	×	×	×	×
Rajaram et al. [31]	√	×	×	√	×	×	×	×	×	×	×	×	×
Punithavathi et al. [54]	×	×	×	×	×	√	×	×	×	×	×	×	√
Xiong et al. [55]	×	×	×	×	×	×	×	×	×	√	×	√	×

1) Password guessing attack: Many of the password authentication schemes possess less entropy that is susceptible to password guessing attack, in which an attacker accesses and stores authorization messages locally and then tries to use the guessed password to test for correctness.

2) Parallel session attack: An attacker may masquerade as the authorized user, despite knowing a user's password by generating a legitimate login message off any eavesdropped conversation between user and server. The attacker could also initiate a simultaneous attack by recreating the response message from the server at such a later stage as the login message from the user.

3) Forgery attack: An intruder attempts to alter captured messages to masquerade as the legitimate user for wireless system access to the resources. An Intruder could even masquerade as a legitimate server for the manipulation of confidential legal user data.

4) Denial of service attack: This attack prohibits the use or maintenance of communicating messages. This attack can impact a specific user. For example: an adversary can cause the server to refuse a particular user's login before it is re-registered. The DoS attack excludes all or individual users by aggressive behavior on the server or through a forgery of the password validation of the user.

5) Reflection attack: A reflection attack is a form of targeting an authentication device for the response to challenges that utilize a certain protocol through both directions. That is, both sides have used the same challenge-response protocol to validate the users. The attack's basic concept is to trap the target into offering the answer to its question.

6) Stolen verifier attack: The server stores hashed passwords in several applications, rather than plain tenot passwords. The stolen verifier assault implies an attacker who stoles the password verifier that is hashed password. And during the user authentication process, the server may use it explicitly to masquerade as just an authorized user.

7) Smart card loss attack: Unauthorized users can easily modify the smart card's password when the smart card is stolen or lost. Or can formulate a user's password by password guessing attacks, or can obtain by user signing into the program.

8) Replay attack: An intruder who has obtained previous communications can impersonate the authorized user to sign in to the system. The intruder will playback the messages that were intercepted. An attempt in which a legitimate transmission of information is maliciously or fraudulently replicated either by the originator or an attacker who intercepts the information and forward, probably as part of a masquerade assault.

9) Insider attack: An insider attack is a deliberate misuse of people allowed to use computers and networks. To get a password, the server insider will perform an off-line guessing attack. If it works, the server's attacker will try using a password to spoof users to log into other servers using standard password authentication methods

10) Man-in-the-middle attack: Man-in-the-middle (MITM) attack is a form of threat where attackers intervene in an existing two computer communication and then track, capture, and monitor the interaction. In Man-in-the-Middle Attack, an attacker assumes the identity of legitimate users to gain control of network traffic.

11) Lack of session key attack: Often session keys are called symmetric keys because the same key is used both for encryption and decryption. The key is transmitted along with every message during each session and is encrypted with the public key of the recipient. The key is transmitted along with every message during each session and is encrypted with the public key of the recipient. An attacker who attempts to gain this session key of a particular communication is called a session key attack.

12) Impersonation attack: An impersonation attack is an attack in which an attacker effectively assumes the identity of one of the legitimate parties in a contact protocol or program. The purpose of a strong identity or entity

authentication protocol is to make the possibility negligible to make impersonation in secure communication.

13) Biometric recognition error: Two types of biometric recognition errors have happened in any biometric device. A) False accept rate: The rate at which the device accepts an unauthorized person B) False reject rate: The rate at which the device falsely rejects an authorized person.

Conclusion

In this paper, a systematic review of recent advances in remote user authentication scheme has been proposed. Security attacks that every authentication should mitigate and security requirements that each authentication scheme should satisfy have been outlined. The remote user authentication scheme is categorized into three systematic layers in which the first layer depicts the remote user authentication scheme for health care applications, the second layer depicts the remote user authentication scheme on IoT applications and the third layer elaborates on the remote user authentication scheme on cloud and multi-server applications. E-healthcare is the active area of research in TMIS which gives mobility to its users.

Having considered the privacy of patients, medical information, authenticated, and secure access to medical data are needed. The comparative evaluation of the recent remote user authentication scheme has been pointed out. Given the growing speed and complexity of IoT devices in our society, the need for such devices to be authenticated would be much needed. Before actually supplying mobile users with any connection to the cloud service, mutual authentication of the cloud service provider and the mobile user is required. In this paper, around 100 recent remote user authentication schemes have been analyzed and compared concerning key features, security tool used, performance parameters such as computation cost, communication cost, storage cost, accuracy, FAR, FRR. Moreover, it is believed that the ongoing direction in a survey of remote user authentication scheme helps the researchers to easily point out the ideal properties, possible factors, and helps to outline the various security attacks. In future research, in addition to IoT, health care, cloud, and multi-server applications, remote user authentication will find its major concern in emerging real-time applications such as agriculture, E-governance, smart cities, E-passport, etc.

References

[1] Y. Park, K. Park, K. Lee, H. Song, and Y. Park: Security analysis and enhancements of an improved multi-factor biometric authentication scheme, International Journal of Distributed Sensor Networks, Vol. 13, p. 1550147717724308, 2017

[2] L. Zhang, Y. Zhang, S. Tang, and H. Luo: Privacy protection for e-health systems using dynamic authentication and three-factor key agreement, IEEE Transactions on Industrial Electronics, Vol. 65, pp. 2795-2805, 2017

[3] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry: Efficient end-to-end authentication protocol for wearable health monitoring systems, Computers & Electrical Engineering, Vol. 63, pp. 182-195, 2017

[4] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K.-K. R. Choo: An enhanced 1-round authentication protocol for wireless body area networks with user anonymity, Computers & Electrical Engineering, Vol. 61, pp. 238-249, 2017

[5] F. Merabet, A. Cherif, M. Belkadi, O. Blazy, E. Conchon, and D. Sauveron: New efficient M2C and M2M mutual authentication protocols for IoT-based healthcare applications, Peer-to-Peer Networking and Applications, Vol. 13, pp. 439-474, 2020

[6] N. Yessad, S. Bouchelaghem, F.-S. Ouada, and M. Omar: Secure and reliable patient body motion based authentication approach for medical body area networks, Pervasive and Mobile Computing, Vol. 42, pp. 351-370, 2017

[7] S. A. Chaudhry, M. T. Khan, M. K. Khan, and T. Shon: A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography, Journal of medical systems, Vol. 40, p. 230, 2016

[8] B. Narwal and A. K. Mohapatra: SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks, Wireless Personal Communications, pp. 1-24, 2020

[9] L. Zhang, S. Zhu, and S. Tang: 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, Vol. 21, pp. 465-475, 2016

[10] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar: A robust and anonymous patient monitoring system using wireless medical sensor networks, Future Generation Computer Systems, Vol. 80, pp. 483-495, 2018

[11] S. Adamović, V. Miškovic, N. Maček, M. Milosavljević, M. Šarac, M. Saračević, et al.: An efficient novel approach for iris recognition based on stylometric features and machine learning techniques, Future Generation Computer Systems, Vol. 107, pp. 144-157, 2020

[12] M. Saračević, S. Adamović, and E. Biševac: Application of Catalan Numbers and the Lattice Path Combinatorial Problem in Cryptography, Acta Polytechnica Hungarica, Vol. 15, 2018

[13] M. Mohammedi, M. Omar, and A. Bouabdallah: Secure and lightweight remote patient authentication scheme with biometric inputs for mobile healthcare environments, Journal of Ambient Intelligence and Humanized Computing, Vol. 9, pp. 1527-1539, 2018

[14] K. Sowjanya, M. Dasgupta, and S. Ray: An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems, International Journal of Information Security, Vol. 19, pp. 129-146, 2020

[15] B. A. Alzahrani, A. Irshad, A. Albeshri, and K. Alsubhi: A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks, Wireless Personal Communications, pp. 1-23, 2020

[16] Z. Xu, C. Xu, H. Chen, and F. Yang: A lightweight anonymous mutual authentication and key agreement scheme for WBAN, Concurrency and Computation: Practice and Experience, Vol. 31, p. e5295, 2019

[17] Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, and J. Ma: Security analysis and improvement of bio-hashing based three-factor authentication scheme for telecare medical information systems, Journal of Ambient Intelligence and Humanized Computing, Vol. 9, pp. 1061-1073, 2018

[18] Y. Lu, L. Li, H. Peng, D. Xie, and Y. Yang: Robust and efficient biometrics based password authentication scheme for telecare medicine information systems using extended chaotic maps, Journal of medical systems, Vol. 39, p. 65, 2015

[19] D. Mishra: On the security flaws in id-based password authentication schemes for telecare medical information systems, Journal of medical systems, Vol. 39, p. 154, 2015

[20] P. K. Dhillon and S. Kalra: Multi-factor user authentication scheme for IoT-based healthcare services, Journal of Reliable Intelligent Environments, Vol. 4, pp. 141-160, 2018

[21] N. Ravanbakhsh and M. Nazari: An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems, Multimedia Tools and Applications, Vol. 77, pp. 55-88, 2018

[22] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, and N. Kumar: An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography, Journal of medical systems, Vol. 39, p. 180, 2015

[23] W. Li and P. Wang: Two-factor authentication in industrial Internet-of-Things: Attacks, evaluation and new construction, Future Generation Computer Systems, Vol. 101, pp. 694-708, 2019

[24] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood: Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme, Future Generation Computer Systems, Vol. 100, pp. 882-892, 2019

[25] X. Li, Q. Wen, and W. Li: A three-factor based remote user authentication scheme: Strengthening systematic security and personal privacy for

wireless communications, Wireless Personal Communications, Vol. 86, pp. 1593-1610, 2016

[26] H. Amintoosi and A. J. Taresh: Sparse coding-based feature extraction for biometric remote authentication in Internet of Things, SN Applied Sciences, Vol. 1, p. 1098, 2019

[27] M. Nikravan and A. Reza: A multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of Things, Wireless Personal Communications, Vol. 111, pp. 463-494, 2020

[28] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and M. Jo: Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of Things, IEEE Internet of Things Journal, Vol. 5, pp. 2884-2895, 2017

[29] D. Dharminder, S. Rana, N. Kundu, and D. Mishra: Construction of lightweight authentication scheme for network applicants using smart cards, Sādhanā, Vol. 45, pp. 1-14, 2020

[30] T. Limbasiya, M. Soni, and S. K. Mishra: Advanced formal authentication protocol using smart cards for network applicants, Computers & Electrical Engineering, Vol. 66, pp. 50-63, 2018

[31] S. Rajaram, T. Maitra, S. Vollala, N. Ramasubramanian, and R. Amin: eUASBP: enhanced user authentication scheme based on bilinear pairing, Journal of Ambient Intelligence and Humanized Computing, pp. 1-14, 2019

[32] A. K. Awasthi: An improved remote user authentication scheme with smart cards using bilinear pairings, International Journal of Applied Mathematics and Computation, Vol. 4, pp. 382-389, 2012

[33] M. Karuppiah, S. Kumari, X. Li, F. Wu, A. K. Das, M. K. Khan, et al.: A dynamic id-based generic framework for anonymous authentication scheme for roaming service in global mobility networks, Wireless Personal Communications, Vol. 93, pp. 383-407, 2017

[34] M. Kang, H. S. Rhee, and J.-Y. Choi: Improved user authentication scheme with user anonymity for wireless communications, IEICE transactions on fundamentals of electronics, communications and computer sciences, Vol. 94, pp. 860-864, 2011

[35] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos: Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems, Future Generation Computer Systems, Vol. 108, pp. 1267-1286, 2020

[36] Q. Feng, D. He, S. Zeadally, and H. Wang: Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment, Future Generation Computer Systems, Vol. 84, pp. 239-251, 2018

[37] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K. R. Choo, and J. Shen: Design of a provably secure biometrics-based multi-cloud-server authentication scheme, Future Generation Computer Systems, Vol. 68, pp. 320-330, 2017

[38] X. Liu, Y. Li, J. Qu, and L. Lu: ELAKA: energy-efficient and lightweight multi-server authentication and key agreement protocol based on dynamic biometrics, Wireless Personal Communications, Vol. 100, pp. 767-785, 2018

[39] T. Joseph, S. Kalaiselvan, S. Aswathy, R. Radhakrishnan, and A. Shamna: A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment, Journal of Ambient Intelligence and Humanized Computing, pp. 1-9, 2020

[40] I. D. O. Nunes, K. Eldefrawy, and T. Lepoint: SNUSE: A secure computation approach for large-scale user re-enrollment in biometric authentication systems, Future Generation Computer Systems, Vol. 98, pp. 259-273, 2019

[41] G. Sharma and S. Kalra: Identity based secure authentication scheme based on quantum key distribution for cloud computing, Peer-to-Peer Networking and applications, Vol. 11, pp. 220-234, 2018

[42] R. Shashidhara, S. Bojjagani, A. K. Maurya, S. Kumari, and H. Xiong: A Robust user authentication protocol with privacy-preserving for roaming service in mobility environments, Peer-to-Peer Networking and Applications, pp. 1-24, 2020

[43] G. Xu, J. Liu, Y. Lu, X. Zeng, Y. Zhang, and X. Li: A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility networks, Journal of Network and Computer Applications, Vol. 107, pp. 83-92, 2018

[44] S. Jangirala, S. Mukhopadhyay, and A. K. Das: A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards, Wireless Personal Communications, Vol. 95, pp. 2735-2767, 2017

[45] S. Shunmuganathan, R. D. Saravanan, and Y. Palanichamy: Secure and efficient smart-card-based remote user authentication scheme for multiserver environment, Canadian Journal of Electrical and Computer Engineering, Vol. 38, pp. 20-30, 2015

[46] M. Zhang, J. Zhang, and W. Tan: Remote three-factor authentication protocol with strong robustness for multi-server environment, China Communications, Vol. 14, pp. 126-136, 2017

[47] V. Odelu, A. K. Das, and A. Goswami: A secure biometrics-based multi-server authentication protocol using smart cards, IEEE Transactions on Information Forensics and Security, Vol. 10, pp. 1953-1966, 2015

[48] T. A. T. Nguyen and T. K. Dang: Privacy preserving biometric-based remote authentication with secure processing unit on untrusted server, IET Biometrics, Vol. 8, pp. 79-91, 2018

[49] B. Ying and A. Nayak: Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography, Journal of Network and Computer Applications, Vol. 131, pp. 66-74, 2019

[50] P. Chandrakar and H. Om: Cryptanalysis and extended three-factor remote user authentication scheme in multi-server environment, Arabian Journal for Science and Engineering, Vol. 42, pp. 765-786, 2017

[51] F. Wen, W. Susilo, and G. Yang: Analysis and improvement on a biometric-based remote user authentication scheme using smart cards, Wireless Personal Communications, Vol. 80, pp. 1747-1760, 2015

[52] H. Yao, C. Wang, X. Fu, C. Liu, B. Wu, and F. Li: A privacy-preserving RLWE-based remote biometric authentication scheme for single and multi-server environments, IEEE Access, Vol. 7, pp. 109597-109611, 2019

[53] N. Sasikaladevi and D. Malathi: Energy Efficient Lightweight Mutual Authentication Protocol (REAP) for MBAN Based on Genus-2 Hyper-Elliptic Curve, Wireless Personal Communications, Vol. 109, pp. 2471-2488, 2019

[54] P. Punithavathi, S. Geetha, M. Karuppiah, S. H. Islam, M. M. Hassan, and K.-K. R. Choo: A lightweight machine learning-based authentication framework for smart IoT devices, Information Sciences, Vol. 484, pp. 255-268, 2019

[55] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo: A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, Journal of Network and Computer Applications, Vol. 103, pp. 194-204, 2018