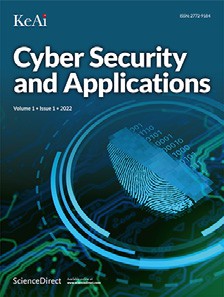
[Cyber Security and Applications 1 (2023) 100013](https://doi.org/10.1016/j.csa.2023.100013)

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/)

Cyber Security and Applications

journal homepage: <http://www.keaipublishing.com/en/journals/cyber-security-and-applications/>

Cryptanalysis of Secure ECC-Based Three Factor Mutual Authentication Protocol for Telecare Medical Information System

C. Madan Kumar [a](#_bookmark0), Ruhul Amin[b](#_bookmark1),[∗](#_bookmark3), M. Brindha[a](#_bookmark0)

a *Department of Computer Science & Engineering, National Institute of Technology, Tiruchirappalli 620015, India*

b *Department of Computer Science & Engineering, National Institute of Technology, Jamshedpur, Jharkhand 831014 India*

a r t i c l e i n f o a b s t r a c t

*Keywords:*

Telecare medical information system Authentication

Elliptic curve cryptography Biohashing

Telecare Medical Information System (TMIS) is gaining importance in the present COVID-19 crisis. TMIS as a technology, offers patients a range of remote medical services, incorporated into Wireless Body Area Network (WBAN). The patient’s medical report is confidentially transmitted over an open channel in TMIS environments. An attacker may attempt to compromise the security, such as forgery, replay, and impersonation attacks. To ensure secure communication, various authentication solutions have been introduced for TMIS. Biometrics and Elliptic Curve Cryptography-based mutual authentication protocol was recommended by Sahoo et al. (2020) and is proved to have some loopholes in the protocol. We discovered, however, Sahoo et al. method is unable to prevent privileged insider attacks and insider attacks along with patient anonymity. Jongseok Ryu et al. recommended a ECC based three-factor mutual authentication protocol and ensures patient’s confidentiality for TMIS with proof of informal analysis. They have also performed formal security studies utilizing the Automated Validation of Internet Security Protocols and Applications (AVISPA), the Burrows–Abadi–Needham (BAN) logic and Real-Or-Random (ROR) model. However, we have reviewed the Jongseok Ryu et al.’s proposal. Based on his attacker model, we have examined that this scheme is unsafe against Message Substitution Attacks, Man-in-the-Middle attacks, Session Key Disclosure attacks, Privileged Insider attacks, and Stolen verifier attacks. we suggest a technique to be safe from the above security threats.

# Introduction

People have developed an interest in utilizing remote services to limit social interaction with others in the recent COVID-19 issue. They avoid going to hospitals and medical centers for fear of spreading the virus to patients who may have the disease. Most of the population found it challenging to go to hospitals and medical centers because of their sensitive health or other circumstances. As a result, there is a growing need for utilizing medical resources online, such as diagnosing patient health online, prescribing medicines, and monitoring patients’ health using wearable devices. Wireless Body Area Network (WBAN) is em- ployed for providing medical benefits with the quick progress of inter- net and wireless communication technology. One of the technologies utilized in WBAN is the Telecare Medical Information System (TMIS), which may deliver various medical services to patients in remote loca- tions through telecare servers [[1,2]](#_bookmark30). TMIS is receiving greater attention in the COVID-19 situation than earlier in-person healthcare services. Pa- tients use wearable sensor devices in the TMIS environment to record their medical data, like heart rate, body temperature and blood pressure. Then, their medical report was sent to the registered mobile devices.

Patients can then send the medical data to telecare medical servers any- time. After receiving patient medical data, the telecare servers provide appropriate healthcare services with doctor’s suggestions available in remote access, such as medical monitoring, therapy, prescriptions, etc. Patients can use intelligent healthcare services, saving time and money. These advantages make TMIS more suitable for providing competent medical services than instead of the physical presence of patients in the recent COVID-19 circumstances. Despite having many benefits, as mentioned, TMIS has several security-related issues. The telecare server in TMIS is responsible for protecting patient privacy and medical data, including identities, passwords, and medical records available electron- ically. Only authorized patients should be given access to safeguard the privacy and confidentiality of the patient data. Additionally, private pa- tients’ information is sent to the telecare medical server over a open channel, giving a chance for an attacker to carry out various attacks like man-in-the-middle (MITM) attacks and impersonation attacks. There- fore, key agreement techniques and secure mutual authentication are crucial challenges in TMIS contexts. To address TMIS security issues, numerous studies have recently been proposed [[3,4]](#_bookmark34). An IoT-enabled device with mutual verification protocol for TMIS was designed by

∗ Corresponding author.

*E-mail addresses:* [amin\_ruhul@live.com](mailto:amin_ruhul@live.com) (R. Amin), [brindham@nitt.edu](mailto:brindham@nitt.edu) (M. Brindha).

<https://doi.org/10.1016/j.csa.2023.100013>

Received 26 July 2022; Received in revised form 25 September 2022; Accepted 25 January 2023

Available online 5 February 2023

2772-9184/© 2023 The Authors. Published by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>)

Sahoo et al. [[3]](#_bookmark34). Sahoo et al.’s technique uses biometric data, Ellip- tic Curve Cryptography, and symmetric key cryptosystem to secure the patient’s confidential data. They asserted that their proposed protocol could survive various security attacks such as oﬄine password guessing attacks, replay attacks, and smartcard Stolen attacks. We scrutinized that their proposed protocol is compromised with privileged insider attacks and insider attacks. In line, we investigated that their scheme is defenseless for patient anonymity and a password updating process. This research recommends a robust mutual authentication protocol with three-factor authentication for TMIS that uses a patient’s mobile com- munication device.

* 1. *Research contribution*

In this article, we have reviewed Jongseok Ryu’s authentication scheme for Telecare Medical Information System. We then demonstrated that Ryu’s proposal is vulnerable to Message substitution attacks, Man- in-the-middle attacks, Session Key Disclosure attacks, and privileged in- sider attacks described in [Section 5](#_bookmark9) by performing the cryptanalysis on Ryu’s authentication scheme. We also proposed suggestions for improv- ing the protocol, which prevents the attacks mentioned above.

# Related works

In the recent trend, numerous authentication methods were pro- posed for TMIS environments [[2,5–9]](#_bookmark31). Using a smartcard for two-factor- based authentication and TMIS was proposed by Khan and Kumari

[[10]](#_bookmark11) in 2013. They claimed their system is safe from oﬄine password prediction attacks, replay attacks, and stolen verifier attacks. Their plan is defenseless to an oﬄine password guessing attack. To enhance Khan and Kumari’s system, Giri et al. [[11]](#_bookmark13) recommended a user authentica- tion scheme appertaining to RSA in 2014. Giri et al. asserted that their proposal defends numerous threats like guessing oﬄine password at- tacks, insider attacks, and replay attacks by performing informal secu- rity. Giri et al.’s technique is suffering from privileged insider attacks and guessing oﬄine passwords found by Amin and Biswas [[12]](#_bookmark14) in 2015. Later, they offered an enhanced RSA-based authentication method and AVISPA to have high security. However, Sutrala et al. [[13]](#_bookmark15) found that Amin and Biswas’s proposal failed to control oﬄine password guessing attacks, impersonation attacks and replay attacks. Later, they suggested an RSA-based verification scheme and key agreement scheme.

Authenticated key agreement approach in TMIS, utilizing ECC, was suggested by Zhang and Zhu [[14]](#_bookmark16) in 2015 and offers greater security having a minor key size compared to Asymmetric key cryptography like RSA. Zhang and Zhu claimed their safety against oﬄine and MITM pass- word guessing assault. According to Liu et al. [[15]](#_bookmark17), Zhang and Zhu’s pro- tocol cannot resist guessing oﬄine password attacks, including attacks using smartcards thefts. An ECC-based authentication technique was also presented in 2018 by Ostad-Sharif et al. [[16]](#_bookmark18). Their system contains security weaknesses like key compromise impersonation and password guessing attacks, although being more effective than RSA [[17]](#_bookmark19). These techniques [[10–12,18–21]](#_bookmark11) depend on the following factors like pass- word and smartcard, by which it is challenging to perform attacks using stolen smartcards or oﬄine password guessing attacks. Researchers rec- ommended a three-factor authentication technique to address the issues in the TMIS environment with two-factor authentication [[3,22,23]](#_bookmark34). Lu et al. [[22]](#_bookmark20) in 2015, recommended an authentication protocol with a biometric technique for the TMIS architecture. They claimed their pro- posal is safe against multiple security assaults, like replay attacks and oﬄine password guessing attacks. Their proposal, however, is prone to impersonation attacks and oﬄine password guessing attacks [[24]](#_bookmark21). In 2016, Ravanbakhsh and Nazari [[25]](#_bookmark22) proposed a session key agreement technique with an enhanced mutual authentication for TMIS. Unfortu- nately, Ostad-Sharif et al. [[26]](#_bookmark23) shows that Ravanbakhsh and Nazari’s method cannot guarantee forward secrecy and cannot defend against known session-specific temporary information attacks. Then, in 2018,

Qi and Chen [[27]](#_bookmark24) recommended mutual authentication technique adopt- ing biometrics features and Elliptic Curve Cryptography for TMIS. They proved that their proposal offers mutual authentication by employing BAN logic. However, there are security weaknesses in the Qi and Chen approach, like key compromise impersonation attacks along with oﬄine password guessing attacks [[28]](#_bookmark25). Consequently, Lu et al. [[22]](#_bookmark20), Ravan- bakhsh and Nazari [[25]](#_bookmark22), Qi and Chen [[27]](#_bookmark24) continue to be unsuitable for TMIS situations. In 2019, Zeng et al. [[29]](#_bookmark26) exhibited an anonymous user authentication (E-AUA) proposal for both users and servers in a multiserver environment. In 2020, Shoban Mandal et al. [[30]](#_bookmark28) scruti- nized that Zeng et al.’s proposal is suffering from lost/stolen smart gate- way, oﬄine Password guessing assault involving a privileged insider at- tack and has proposed Certificateless-Signcryption-Based Three-Factor User Access Control Scheme, resistant to assaults mentioned above. In 2019, Shuai et al.’s protocol [[31]](#_bookmark29) presented a protected three-factor authentication protocol for online patient monitoring. In 2020 Jiaqing Mo et al. [[32]](#_bookmark32) scrutinized that Shuai et al.’s proposal is prone to of- fline dictionary guessing attacks and privileged insider attacks by per- forming the cryptanalysis. In addition, they also pointed out a flaw in their design, part of their proposal results password update phase and proposed countermeasures for the enhancement of Two verifica- tion Schemes for Healthcare Systems. Using Wireless Medical Sensor Networks, we can prevent all possible attacks. Fotouhi et al. [[33]](#_bookmark33) in 2020, proposed a secured scheme having perfect forward security, un- traceability, and resilience against numerous attacks, is secure against a variety of known attacks required for WBANs. The suggested tech- nique is resistant to known session-specific temporary information at- tacks as well as key compromise impersonation attempts. Taleb et al.

[[34]](#_bookmark35) in 2021, presented a analysis between leading wireless technologies

with proposed wireless technologies oriented for medical applications. Jiliang Li et al. [[35]](#_bookmark36) in 2021, to avail complete public channels in IoMT, introduced the provably secure and lightweight MAAKA (PSL-MAAKA) protocol. The hash operation and XOR operation are the main oper- ations in the verification stage and key agreement. This article uses the random oracle model to demonstrate the security of the protocol that is being given. In 2020, Xiong Li et al. [[35]](#_bookmark36) have proposed a strat- egy that offers user privacy and guards against sensor node imperson- ation attacks. Later, Muhammad Asad Saleem et al. [[36]](#_bookmark37) claimed that their scheme fails to prevent sensor node impersonation attacks and fails to provide user anonymity. Muhammad proposed a suitable so- lution for the problem mentioned above. In 2021, authors [[37,38]](#_bookmark39) pro- posed a robust anonymous verification and key agreement proposal with privacy-preserving for smart cities. In 2022, Tanveer et al. [[5]](#_bookmark38), proposed REAS-TMIS claiming that this protocol is resistant to all possible attacks. Madan et al. [[39]](#_bookmark43) has scrutinized the Tanveer et al.’s protocol and found that it is suffering from session key disclosure attacks, privileged insider attacks, and medical server impersonation attacks. Madan et al. has rec- ommended a mechanism to overcome the above mentioned attacks. In 2022, Many Authors, including Prateek et al. [[40–45]](#_bookmark44) recommended V2I authentication in vehicular ad-hoc networks, suggested implement- ing the Privacy-Preserving verification Protocol for Quantum Comput- ing. Using message authentication codes, several message authentica- tion proposals are also created in VANETs. The quantum cryptosystem [[46,47]](#_bookmark47), which combines quantum ciphering and conventional encryp- tion, utilizing laws of physics and quantum mechanics for safe trans- mission of data between the involved entities. A quantum key exchange or distribution technique [[48,49]](#_bookmark48) does not rely on the computationally diﬃcult behaviour of some mathematical problem. A subset of the enor- mously popular developing concept of IoT is called the Internet of Ve- hicles (IoV). In order to transform a vehicle into a smart vehicle, an extended vehicular adhoc network (VANET) is used, by giving them a on board unit (OBU), enabling them to communicate with other vehi- cles, Humans (customers or pedestrians), technology (internet, cloud, parking lots, traﬃc signals, etc.). Through messages or beacons, the ve- hicles can directly or indirectly communicate with each other over wire- less open channels. Open channels during communication allow for a

**Table 1**

Summary of the existing work in user authentication schemes.

|  |  |  |  |
| --- | --- | --- | --- |
| Scheme | Year | Cryptographic Features | Limitations |
| Zhang et al. [[52]](#_bookmark51) | 2017 | Exclusive-OR, chaotic map and SHA | diﬃcult to prevent PGU and SIM attacks. |
| Qui et al. [[53]](#_bookmark52) | 2018 | ECC, Exclusive-OR, and SHA | diﬃcult to prevent URIM attacks. Unable to provide URA feature. |
| Chaudhry et al. [[54]](#_bookmark53) | 2018 | ECC, Exclusive-OR, and SHA | diﬃcult to prevent EPLE attacks and impersonation and can not provide anonymity feature. |
| Renuka et al. [[9]](#_bookmark12) | 2019 | ECC, Exclusive-OR, and SHA | cannot prevent PIN and provide URA feature. |
| Madhusudhan et al. [[8]](#_bookmark42) | 2019 | Exclusive-OR, chaotic map and SHA | cannot prevent replay, MATM, PIN, and SIM. Does not provide MA and URA feature. |
| Son et al. [[2]](#_bookmark31) | 2020 | BP, Exclusive-OR, and SHA | cannot prevent replay, MATM, PIN, and SIM. Does not provide MA and URA feature. |
| Nayak et al. [[7]](#_bookmark41) | 2020 | Exclusive-OR, and SHA | diﬃcult to prevent D-SYN and cannot provide URA feature. |
| Chaudhry et al. [[55]](#_bookmark54) | 2021 | ECC, Exclusive-OR, and SHA | cannot prevent impersonation attacks and EPLE attacks and cannot provide anonymity feature. |
| Ryu et al. [[6]](#_bookmark40) | 2022 | ECC, Biohashing | cannot restrain impersonation, forgery and MITM attack. |
| Tanveer et al. [[5]](#_bookmark38) | 2022 | SHA and AEAD scheme | cannot restrain impersonation, smartcard stolen attack, insider attack |

variety of attacks, including replay, man-in-the-middle, impersonation, fabrication, etc. To overcome these attacks, Bagga et al. [[50]](#_bookmark49) developed a novel remote access management system to address security concerns in smart transportation. Later, keeping in view the needs of smart de- vices in terms of storage cost, Yan et al. [[51]](#_bookmark50) designed a update protocol to optimize the storage cost to constant. Sahoo et al. [[3]](#_bookmark34) developed a three-factor authentication scheme for the TMIS environment in 2020 to solve security issues comparable to existing techniques. Their tech- nique proved resistant to insider attacks, oﬄine password guessing, and attacks using stolen smart cards. We scrutinized Sahoo et al.’s solution and found it defenseless against privileged insider attacks and insider attacks. Additionally, we discovered a weakness in the password update stage and cannot guarantee patient privacy. So, utilizing biometrics and ECC, we suggest a robust mutual authentication system for TMIS secu- rity. In [Table 1](#_bookmark5), we exhibit the analysis of existing works to highlight the features and Limitations.

# Paper organization

The paper is organized using the following sections: [Section 1](#_bookmark2) presents the requirement for Telecare Medical Informa- tion System. The Related works are discussed in [Section 2](#_bookmark4). The paper organization is defined in [Section 3](#_bookmark7). The review of Jongseok Ryu et al. protocol is presented in [Section 4](#_bookmark8). Security limitations of Jongseok Ryu et al. protocol are discussed in [Section 5](#_bookmark9). Suggestions to overcome these limitations by improving the protocol are given in [Section 6](#_bookmark10). Concluding comments and the scope of this paper are presented in [Section 7](#_bookmark27).

# Brief review of Jongseok Ryu et al. scheme

We exhibit a review of Jongseok Ryu et al.’s [[6]](#_bookmark40) proposal. This pro- tocol executes different phases like the initialization phase, patient reg- istration phase, telecare server registration phase, login phase, authen- tication phase, and password update phase. The notations used in this article are summarized in [Table 2](#_bookmark6).

* 1. *Initialization section*

In the initialization section, *𝑅𝐶* chooses an elliptic curve *𝐸𝑝*(*𝑟, 𝑠*), a plane curve over a finite field *𝐹𝑝*. Following that, a base point P is considered on *𝐸𝑝*(*𝑟, 𝑠*) and also a private key *𝑘𝑟𝑐* is selected by RC. The following *𝐸𝑝*(*𝑟, 𝑠*), *𝑃* , *ℎ*(∙), *ℎ𝑏*(∙) are the parameters which are then pub- lished by *𝑅𝐶*.

**Table 2**

List of notations in this paper.

|  |  |
| --- | --- |
| Terms | Expansion |
| *𝑈𝑖* | User |
| *𝑇 𝑆𝑗* | Telecare Medical Server |
| *𝑆𝐶* | Smart card |
| *𝑅𝐶𝐼* | Identity of RC |
| *𝑆𝐼𝐷𝑗* | *𝑇 𝑆𝑗* ’s Identity |
| *𝑃𝑆𝐼𝐷𝑖* | *𝑇 𝑆𝑗* ’s Pseudo Identity |
| *𝑅𝐶* | Registration Center |
| *𝐼𝐷𝑖* | Identity of *𝑈𝑖* |
| *𝑃𝐼𝐷𝑖* | Pseudo Identity of *𝑈𝑖* |
| *𝑃𝑊𝑖* | Password of *𝑈𝑖* |
| *𝐵𝐼𝑖* | Biometric information of *𝑈𝑖* |
| *𝑀𝐷𝑖* | Mobile device of *𝑈𝑖* |
| *𝑛*1 *, 𝑛*2 *, 𝑅𝑗 , 𝑅𝑁𝑢 , 𝑅𝑁𝑠𝑗* | Random Numbers |
| *𝑥, 𝑦, 𝑘𝑟𝑐* | *𝑅𝐶*’s Private key |
| *𝑇𝑢 , 𝑇𝑟 , 𝑇*1 *, 𝑇*2 | Timestamps |
| *𝑆𝐾* | *𝑅𝐶*’s Session key |
| *𝑘𝑠𝑗* | *𝑇 𝑆𝑗* ’s Private key |
| *𝑝𝑘𝑠𝑗* | *𝑇 𝑆𝑗* ’s Public key |
| *𝑚𝑘* | Master key of *𝑅𝐶* |
| *ℎ𝑏* (*.*) | Biohash function |
| *ℎ*(*.*) | Hash operation |
| *𝐸𝑘* ∕*𝐷𝑘* | Symmetric Cipher/decipher |
| *⊕* | XOR operations |
| ∥ | concatenation operations |

* + 1. *Patient registration*

To utilize the medical facilities from *𝑇 𝑆𝑗* , all the users *𝑈𝑖* need

(*𝑈𝑖*) creates an identity (*𝐼𝐷𝑖*), a password (*𝑃 𝑊𝑖*), the biometrics *𝐵𝐼𝑖* to register in RC safely. The details are presented as follows: User and creates *𝑅𝑁𝑢* a random no. Later, User *𝑈𝑖* calculates *𝐻𝐼𝐷𝑖* = *ℎ*(*𝐼𝐷𝑖* ∥ *𝑅𝑁𝑢*), *𝐻𝑃 𝑊𝑖* = *ℎ*(*𝑃 𝑊𝑖* ∥ *ℎ𝑏*(*𝐵𝐼𝑖*)), and *𝐺𝑃 𝑊𝑖* = (*𝐻𝑃𝑊𝑖 ⊕ 𝑅𝑁𝑢*) and transfers the (*𝐻𝐼𝐷𝑖, 𝐺𝑃 𝑊𝑖*) message to Registration Center through a secured communication path. Registration Center calculates *𝑈𝑅𝑖* = *ℎ*(*𝐻𝐼𝐷𝑖* ∥ *𝑘𝑟𝑐* ) and *𝐵𝑖* = *𝑈𝑅𝑖 ⊕ 𝐺𝑃 𝑊𝑖*. Afterwards, Registration Center safely keeps *𝐻𝐼𝐷𝑖* in the RC server and transfers *𝐵𝑖* to User *𝑈𝑖*. User

*𝑈𝑖* calculates *𝑅𝑃 𝑊𝑖* = *ℎ*(*𝐼𝐷𝑖* ∥ *𝑃 𝑊𝑖* ∥ *ℎ𝑏*(*𝐵𝐼𝑖*)), *𝐴*1 = *𝑅𝑁𝑢 ⊕ 𝑅𝑃 𝑊𝑖*, *𝐴*2 =

*ℎ*(*𝐻𝐼𝐷𝑖* ∥ *𝐻𝑃 𝑊𝑖* ∥ *𝑅𝑃 𝑊𝑖* ∥ *𝑅𝑁𝑢*), and *𝐴*3 = *𝐵𝑖 ⊕ 𝑅𝑁𝑢* = *𝑈𝑅𝑖 ⊕ 𝐻𝑃𝑊𝑖*. Later, these computed entities (*𝐴*1, *𝐴*2, *𝐴*3) are stored by *𝑈𝑖* into the memory of mobile device *𝑀𝐷𝑖*.

* + 1. *Telecare medical server registration*

To provide medical facilities to the users *𝑈𝑖*, *𝑇 𝑆𝑗* should get reg- istered in RC. As part of registration, *𝑇 𝑆𝑗* chooses *𝑆𝐼𝐷𝑗* , an identity and *𝑅𝑁𝑠𝑗* , a random number. Later, *𝑇 𝑆𝑗* computes the pseudo-identity

*𝑃 𝑆𝐼𝐷* = *𝑆𝐼𝐷 ⊕ 𝑅𝑁* and transfers *𝑃 𝑆𝐼𝐷* , *𝑅𝑁* to Registration Cen-

*𝑗 𝑗*

*𝑠𝑗*

*𝑗 𝑠𝑗*

* 1. *Registration section*

To exchange the services in between the patient *𝑈𝑖* and the telecare server *𝑇 𝑆𝑗* , both the units need to register with RC, which results in

being part of the TMIS environment.

ter via a safe communication channel. Registration Center calculates

*𝑆𝐼𝐷𝑗* = *𝑃 𝑆𝐼𝐷𝑗 ⊕ 𝑅𝑁𝑠𝑗* and keeps *𝑆𝐼𝐷𝑗* to RC database. Later, Reg- istration Center extracts *𝐻𝐼𝐷𝑖* from its database and calculates *𝑘𝑠𝑗* = *ℎ*(*𝑆𝐼𝐷𝑗* ∥ *𝑘𝑟𝑐* ), *𝑝𝑘𝑠𝑗* = *𝑘𝑠𝑗* ∙ *𝑃* , *𝑇 𝐼𝐷𝑖* = *ℎ*(*𝐻𝐼𝐷𝑖* ∥ *𝑝𝑘𝑠𝑗* ), *𝑈𝑅𝑖* = *ℎ*(*𝐻𝐼𝐷𝑖* ∥

*𝑘𝑟𝑐* ), and *𝑉𝑖𝑗* = *ℎ*(*𝑃 𝑆𝐼𝐷𝑗* ∥ *𝑈𝑅𝑖*). Thereafter, RC makes *𝑃 𝑆𝐼𝐷𝑗 , 𝑝𝑘𝑠𝑗* pub-

lic to all and transfers the parameters (*𝑘𝑠𝑗 , 𝑇 𝐼𝐷𝑖, 𝑉𝑖𝑗* ) to *𝑇 𝑆𝑗* . *𝑇 𝑆𝑗* is de-

fined *𝑘𝑠𝑗* as a private key. Later, *𝑇 𝑆𝑗* computes *𝑆 𝑉𝑖𝑗* = *𝑉𝑖𝑗 ⊕ ℎ*(*𝑆𝐼𝐷𝑗* ∥

*𝑘𝑠𝑗* ) and stores the parameters (*𝑇 𝐼𝐷𝑖 , 𝑆𝑉𝑖𝑗* ) in the database.

and do the following computations in the minimum time accepted by the receiver. Attacker performs the computations by initially se-

lecting the nonce (*𝑛*′ ) and then calculates *𝑆* ′ = *𝑛*′ ∙ *𝑝*, *𝑆* ′ = *𝑛*′ ∙ *𝑝𝑘* ,

1 1 1

2 1 *𝑠𝑗*

* 1. *Login phase*

To access the application and utilize the medical facilities

*𝑈𝑅𝑖* = *ℎ*(*𝐻 𝐼 𝐷𝑖* ∥ *𝐾𝑟𝑐* ), where *𝐾𝑟𝑐* is under CK-Model and *𝐻 𝐼 𝐷𝑖* is

under DY-Model. The value *𝑈𝑅𝑖* will be same as patient *𝑈𝑅𝑖* ,

but *𝑆* ′ , *𝑆* ′ will change. *𝑃 𝐼 𝐷*′ = *ℎ*(*𝐻 𝐼 𝐷* ∥ *𝑝𝑘* ) *⊕ ℎ*(*𝑃 𝑆 𝐼𝐷* ∥ *𝑆* ′ ),

1 2 *𝑖*

*𝑖 𝑠𝑗*

*𝑗* 2

from the telecare medical server (*𝑇 𝑆𝑗* ), the users (*𝑈𝑖* ) need to where *𝐻 𝐼 𝐷𝑖* is under DY-Model, *𝑝𝑘𝑠𝑗* and *𝑃 𝑆𝐼𝐷𝑗* is the public

accomplish the following steps: User *𝑈𝑖* takes his Mobile device

information. *𝑈𝐼𝐷* = *ℎ*(*ℎ*(*𝐻 𝐼 𝐷* ∥ *𝑝𝑘*

) ∥ *ℎ*(*𝑃 𝑆𝐼𝐷*

∥ *𝑈𝑅* ) ∥ *𝑇* ), *𝑀* ′ =

*𝑖 𝑖*

*𝑠𝑗*

*𝑗 𝑖* 1 *𝑖*

*𝑀𝐷𝑖* and enters *𝐼𝐷𝑖* , *𝑃 𝑊𝑖* and *𝐵𝐼𝑖* . The mobile device *𝑀𝐷𝑖* per-

*ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ′ ∥ *ℎ*(*𝑃 𝑆𝐼𝐷*

∥ *𝑈𝑅* ) ∥ *𝑇* ). Eventually, Attacker discards the

forms computations, to compute *𝑅𝑃 𝑊* = *ℎ*(*𝐼𝐷* ∥ *𝑃 𝑊* ∥ *ℎ* (*𝐵𝐼* )),

*𝑖* 2

*𝑗 𝑖*

1

′ ′ ′

*𝑖 𝑖*

*𝑖 𝑏 𝑖*

user message and transmits the (*𝑃 𝐼 𝐷𝑖* , *𝑀𝑖* , *𝑆*1 , *𝑇*1 ) to *𝑇 𝑆𝑗* . *𝑇 𝑆𝑗* calcu-

*𝑅𝑁𝑢* = *𝐴*1 *⊕ 𝑅𝑃 𝑊𝑖* , *𝐻 𝐼 𝐷𝑖* = *ℎ*(*𝐼 𝐷𝑖* ∥ *𝑅𝑁𝑢* ), *𝐻 𝑃 𝑊𝑖* = *ℎ*(*𝑃 𝑊𝑖* ∥ *ℎ𝑏* (*𝐵𝐼𝑖* )),

lates *𝑆* ∗ = *𝑘*

* *𝑆* ′ , *𝑇 𝐼𝐷* =

′ (*𝑃 𝑆 𝐼𝐷* ∥ *𝑆* ′ ). *𝑇 𝑆*

retrieves *𝑆𝑉*

and *𝐴*∗ = *ℎ*(*𝐻 𝐼 𝐷𝑖* ∥ *𝐻 𝑃 𝑊𝑖* ∥ *𝑅𝑃 𝑊𝑖* ∥ *𝑅𝑁𝑢* ). *𝑀𝐷𝑖* checks whether

2 *𝑠𝑗* 1

*𝑗 𝑃 𝐼𝐷𝑖 ⊕ℎ*

*𝑗* 2 *𝑗*

*𝑖𝑗*

*𝐴*∗? = 2 . If there is a matching, move to the next step. If there is

2 *𝐴*2

corresponding to *𝑇 𝐼𝐷𝑖* and then computes *𝑉𝑖𝑗* = *𝑆 𝑉𝑖𝑗 ⊕ ℎ*(*𝑆𝐼𝐷𝑗* ∥ *𝑘𝑠𝑗* ),

*𝑈𝐼𝐷* = *ℎ*(*𝑇 𝐼 𝐷* ∥ *𝑉* ∥ *𝑇* ), *𝑀* ∗ = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ∗ ∥ *𝑉* ∥ *𝑇* ) and verifies

no matching, *𝑀𝐷𝑖* discards the login phase. *𝑀𝐷𝑖* chooses a random

*𝑖 𝑖*

∗ ′

*𝑖𝑗* 1 1

*𝑖* 2

*𝑖𝑗* 1

number *𝑛*1 along with a timestamp *𝑇*1 . Later on, *𝑀𝐷𝑖* performs com-

putations to *𝑐𝑜𝑚𝑝𝑢𝑡𝑒𝑆* = *𝑛* ∙ *𝑃* , *𝑆* = *𝑛* ∙ *𝑝𝑘* , *𝑈𝑅* = *𝐴*3 *⊕ 𝐻𝑃𝑊* ,

*𝑀*1 ? = *𝑀*1 . Later *𝑇 𝑆𝑗* selects random number (*𝑁*2 ) and timestamp(*𝑇*2 )

and then it calculates *𝑆*3 = *𝑁*2 ∙ *𝑃* , *𝑆*4 = *𝑁*2 ∙ *𝑆* ′ , *𝑆* = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ∗ ∥

1 1 2 1

*𝑠𝑗 𝑖 𝑖*

1 *𝑘*

*𝑖* 2

*𝑃 𝐼 𝐷𝑖* = *ℎ*(*𝐻 𝐼 𝐷𝑖* ∥ *𝑝𝑘𝑠𝑗* ) *⊕ ℎ*(*𝑃 𝑆𝐼𝐷𝑗* ∥ *𝑆*2 )*, 𝑈𝐼𝐷𝑖* = *ℎ*(*ℎ*(*𝐻 𝐼 𝐷𝑖* ∥ *𝑝𝑘𝑠𝑗* ) ∥

*ℎ*(*𝑃 𝑆𝐼𝐷𝑗* ∥ *𝑈𝑅𝑖* ) ∥ *𝑇*1 ), and *𝑀𝑖* = *ℎ*(*𝑈𝐼𝐷𝑖* ∥ *𝑆*2 ∥ *ℎ*(*𝑃 𝑆𝐼𝐷𝑗* ∥ *𝑈𝑅𝑖* ) ∥ *𝑇*1 ).

Later, *𝑀𝐷* transfers (*𝑃 𝐼 𝐷 , 𝑀 , 𝑆 , 𝑇* ) to *𝑇 𝑆* via an open communica-

*𝑆*4 ), *𝑀𝑗* = *ℎ*(*𝑈𝐼𝐷𝑖* ∥ *𝑆𝐾* ∥ *𝑇*2 ) and later forwards (*𝑀𝑗 , 𝑆*3 *, 𝑇*2 ). When At-

tacker receives (*𝑀𝑗 , 𝑆*3 *, 𝑇*2 ) from open channel, it further calculates

*𝑆* ′ = *𝑁* ′ ∙ *𝑆* , *𝑆* ′ = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ′ ∥ *𝑆* ′ ) and *𝑀* ∗ = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ′ ∥ *𝑇* ). Fi-

*𝑖 𝑖*

*𝑖* 1 1 *𝑗*

4 1 3

*𝐾*∗

*𝑖* 2 4 *𝑗*

*𝑖 𝐾* 2

tion channel.

* 1. *Authentication phase*

The Authentication between *𝑈𝑖* and *𝑇 𝑆𝑗* is performed by *𝑇 𝑆𝑗* , utilizing the following procedure. *𝑇 𝑆𝑗* checks the condition whether Δ*𝑇* ≥ |*𝑇* ∗ − *𝑇*1 |. If the time is valid, *𝑇 𝑆𝑗* computes *𝑆*2 = *𝑘𝑠𝑗* ∙ *𝑆*1 and

1

*𝑇 𝐼 𝐷𝑖* = *ℎ*(*𝐻 𝐼 𝐷𝑖* ∥ *𝑝𝑘𝑠𝑗* ) = *𝑃 𝐼𝐷𝑖 ⊕ ℎ*(*𝑃 𝑆𝐼𝐷𝑗* ∥ *𝑆*2 ). Thereafter, *𝑇 𝑆𝑗* re-

trieves *𝑆𝑉𝑖𝑗* in its database corresponding to *𝑇 𝐼𝐷𝑖* and computes *𝑉𝑖𝑗* =

*𝑆 𝑉 ⊕ ℎ*(*𝑆𝐼 𝐷𝑗* ∥ *𝑘* ), *𝑈𝐼𝐷* = *ℎ*(*𝑇 𝐼 𝐷* ∥ *𝑉* ∥ *𝑇* ), and *𝑀* ∗ = *ℎ*(*𝑈𝐼𝐷* ∥

nally verifies *𝑀𝑗* ? = *𝑀𝑗* .

* 1. *Man-in-the-middle attack*

(*𝑃 𝐼𝐷𝑖* , *𝑀𝑖* , *𝑆*1 , *𝑇*1 ) to *𝑇 𝑆𝑗* , we assume that the Attacker received the mes- As the patient uses an insecure channel to transmit the message sage (*𝑃 𝐼𝐷𝑖* , *𝑀𝑖* , *𝑆*1 , *𝑇*1 ), and the Attacker performs the following compu-

tations in the shortest amount of time that the recipient will accept. The

computations are carried out by the Attacker by initially choosing the

nonce. *𝑆* ′ = *𝑛*′ ∙ *𝑝*, also computes *𝑆* ′ = *𝑛*′ ∙ *𝑝𝑘* , *𝑈𝑅* = *ℎ*(*𝐻 𝐼 𝐷* ∥ (*𝐾* ),

*𝑖𝑗*

*𝑠𝑗 𝑖*

*𝑖 𝑖𝑗* 1 1 *𝑖* 1 1

2 1 *𝑠𝑗 𝑖*

*𝑖 𝑟𝑐*

*𝑆*2 ∥ *𝑉𝑖𝑗* ∥ *𝑇*1 ). Next, *𝑇 𝑆𝑗* checks the condition whether *𝑀* ∗? = *𝑀𝑖* . If it has a match, *𝑇 𝑆𝑗* assumes a random no. (*𝑛*2 ) and a timestamp *𝑇*2 . At last,

*𝑖*

*𝑇 𝑆* calculates *𝑆* = *𝑛* ∙ *𝑃* , *𝑆* = *𝑛* ∙ *𝑆* , *𝑆𝐾* = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ∥ *𝑆* ), *𝑀* =

where *𝐾𝑟𝑐* is from CK-Model and *𝐻 𝐼 𝐷𝑖* is from the DY-Model. The pa- tient’s *𝑈𝑅𝑖* value will remain the same, but *𝑆*1 and *𝑆*2 will change.

*𝑃 𝐼 𝐷*′ = *ℎ*(*𝐻 𝐼 𝐷* ∥ *𝑝𝑘* ) *⊕ ℎ*(*𝑃 𝑆 𝐼𝐷* ∥ *𝑆* ′ ), where *𝐻 𝐼 𝐷* is under the DY-

*𝑗* 3 2

4 2 1

*𝑖* 2 4 *𝑗*

*𝑖 𝑖*

*𝑠𝑗*

*𝑗* 2 *𝑖*

*ℎ*(*𝑈𝐼𝐷𝑖* ∥ *𝑆𝐾* ∥ *𝑇*2 ) and transfers (*𝑀𝑗* , *𝑆*3 , *𝑇*2 ) to User *𝑈𝑖* via an insecure

communication route. Later getting the message (*𝑀𝑗* , *𝑆*3 , *𝑇*2 ) from *𝑇 𝑆𝑗* , User *𝑈𝑖* validates the timestamp *𝑇*2 with the condition Δ*𝑇*1 ≥ |*𝑇* ∗ − *𝑇*2 |.

2

Then, User *𝑈* computes *𝑆* = *𝑛*1 ∙ *𝑆* , *𝑆𝐾* = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ∥ *𝑆 𝑀* ∗ =

Model, *𝑝𝑘𝑠𝑗* , and *𝑃 𝑆𝐼𝐷𝑗* is the publicly available information.

* 1. *Session key disclosure attack*

*𝑖* 4 3

*𝑖* 2

4), *𝑗*

*ℎ*(*𝑈𝐼𝐷𝑖* ∥ *𝑆𝐾* ∥ *𝑇*2 ), and verifies the condition *𝑀* ∗? = *𝑀𝑗* . If a match is found, it means between User *𝑈𝑖* and *𝑇 𝑆𝑗*, a mutual authentication and

*𝑗*

session key agreement has been created.

ment have been initiated between User *𝑈𝑖* and *𝑇 𝑆𝑗* . If there is a match, the mutual authentication and session key agree-

The telecare server performs further computations to compute *𝑆*3,

*𝑆*4, *𝑆𝐾*, and *𝑀𝑗* , only when there is a proper authentication estab-

care server sends (*𝑀𝑗 , 𝑆*3 *, 𝑇*2 ) to User through a public channel. But the lished between patient and telecare medical server and then the tele- Attacker tries to get *𝑀𝑗 , 𝑆*3 *, 𝑇*2 from the insecure channel and attempts

to compute *𝑆* ′ = *𝑁* ′ ∙ *𝑆*3 , *𝑆* ′ = *ℎ*(*𝑈𝐼𝐷* ∥ *𝑆* ′ ∥ *𝑆* ′ ) and *𝑀* ∗ = *ℎ*(*𝑈𝐼𝐷* ∥

′ 4 1 *𝐾*

*𝑖* 2 4 *𝑗 𝑖*

# Security limitations of Jongseok Ryu et al

*𝑗*

*𝑆𝐾*

∥ *𝑇*2 ) and finally verifies *𝑀* ∗? = *𝑀𝑗* .

* 1. *Adversary model*

To perform security protocol analysis, we apply the “Dolev-Yao (DY) model” [[56]](#_bookmark55) in this research work. According to the DY model, an at- tacker can use an insecure channel to intercept, change, and delete the transmitted message. Below is a definition of an Attacker’s capabilities.

* + - An Attacker may use forgery, impersonation, MITM Attack, etc. [[57]](#_bookmark43).
  1. *Privileged insider attack*

(*𝑃 𝐼𝐷𝑖 , 𝑀𝑖, 𝑆*1 *, 𝑇*1 ) to *𝑇 𝑆𝑗* , we assume that the Attacker received the mes- As the patient uses an insecure channel to transmit the message sage (*𝑃 𝐼𝐷𝑖 , 𝑀𝑖, 𝑆*1 *, 𝑇*1 ), and the Attacker performs the following compu-

tations in the shortest amount of time that the recipient will accept. The

computations are carried out by the Attacker by initially choosing the

nonce. *𝑆* ′ = *𝑛*′ ∙ *𝑝*, also computes *𝑆*2′ = *𝑛*′ ∙ *𝑝𝑘* , *𝑈𝑅* = *ℎ*(*𝐻 𝐼 𝐷* ∥ (*𝐾* ),

* + - Using power analysis, an adversary can access a legitimate patient’s 1 1

1 *𝑠𝑗 𝑖*

*𝑖 𝑟𝑐*

information stored on his mobile device [[58,59]](#_bookmark45).

* + - A legitimate patient or privileged individual could be an opponent

where *𝐾𝑟𝑐* is from CK-Model and *𝐻 𝐼 𝐷𝑖* is from the DY-Model. The pa-

tient’s *𝑈𝑅𝑖* value will remain the same, but *𝑆*1 and *𝑆*2 will change.

*𝑃 𝐼 𝐷*′ = *ℎ*(*𝐻 𝐼 𝐷* ∥ *𝑝𝑘* ) *⊕ ℎ*(*𝑃 𝑆 𝐼𝐷* ∥ *𝑆* ′ ), where *𝐻 𝐼 𝐷* is under the DY-

at the registration desk, as an Attacker.

*𝑖 𝑖*

*𝑠𝑗*

*𝑗* 2 *𝑖*

We take into account the “Canetti–Krawczyk (CK) model” [[60]](#_bookmark46), hav- ing a stronger hypothesis compared to the DY model. Using the CK ap- proach, an attacker can compromise sensitive information, including the secret session key, master key, and private key credentials.

* 1. *Message substitution attack*

Under the CK Model, the Attacker can get the private key *𝐾𝑟𝑐* of RC. User sends the message (*𝑃 𝐼𝐷𝑖 , 𝑀𝑖, 𝑆*1 *, 𝑇*1 ) to *𝑇 𝑆𝑗* through insecure channel. we assume that Attacker gets the message (*𝑃 𝐼𝐷𝑖 , 𝑀𝑖, 𝑆*1 *, 𝑇*1 )

Model, *𝑝𝑘𝑠𝑗* , and *𝑃 𝑆𝐼𝐷𝑗* is the publicly available information.

# Proposal for enhancement

In the Adversary Model” Canetti–Krawczyk (CK) model [[60]](#_bookmark46), there is a chance for the adversary to pull out sensitive information, includ- ing the secret session key, private key, master key credentials. From the attacker model, it is clearly understood that the intruder will try to ab- stract the credentials to compromise the confidentiality, integrity and authenticity. If the attacker abstracts any clue related to credentials, the attacker can easily get the user credentials and create vulnerabilities by

accessing the Remote server. To prevent the attacker from abstracting the credentials, we employ the ECC based cryptosystem. In this cryp-

tosystem, ECC based point multiplication is used. From Sender *𝐴*1, the

private key of sender (*𝑃 𝑟𝐴* ) is point multiplied with the public key of the receiver (*𝑃 𝑢𝐵* ), which results in generation of two coordinates (*𝐴𝑥, 𝐴𝑦* )

on the other side of the receiver, resulting in (*𝐵𝑥, 𝐵𝑦* ). If the verification with the help of a generator function. The same set of operations occur results on both sides as (*𝐴*1 = *𝐵*1) and if the result has a matching, it

means that attacker is unable to guess the credentials and failed to per- form attacks. If there is a mismatch, it means that attacker has modified the data.

To witness this solution, we can follow the below steps:

**Step 1:** We consider the encryption from sender *𝐴*1 with a private key of A as *𝐴*1 = (*𝑃 𝑟𝐴* ∙ *𝑃 𝑢𝐵* ) and this can be evaluated as *𝐴*1 =

*𝑃 𝑟𝐴* ∙ (*𝑃 𝑟𝐵* ∙ *𝐺*), which generates two coordinates (*𝐴𝑥, 𝐴𝑦* ).

**Step 2:** We consider the encryption from receiver *𝐵*1 with a private key of B as *𝐵*1 = (*𝑃 𝑟𝐵* ∙ *𝑃 𝑢𝐴* ) and this can be written as *𝐵*1 = *𝑃 𝑟𝐵* ∙ (*𝑃 𝑟𝐴* ∙ *𝐺*), which generates two coordinates (*𝐵𝑥, 𝐵𝑦* ).

sender(*𝐴*1) and receiver (*𝐵*1), then the verification should result **Step 3:** When the computations are evaluated correctly on both the in (*𝐴*1) = *𝐵*1). And if there is a match, then it indicates that the

attacker is unable to guess the credentials required to perform the attacks.

rent protocol we can assume that *𝐴* = (*𝑃 𝑟𝐴* ∙ *𝑃 𝑢𝐵* ), which generates two *Note:* By implementing the above-mentioned solution in the cur- points on the curve as (*𝐴𝑥, 𝐴𝑦* ) and we get *𝑆*1 = *𝑛*1 ∙ *𝑝* and then based on this value we get *𝑀*1 = *ℎ*(*𝑈𝐼𝐷𝑖* ∥ *𝑆* ∗ ∥ *𝑉𝑖𝑗* ∥ *𝐴𝑥* ∥ *𝑇*1 ). In *𝑀*1 , If the attacker is unable to guess the exact value of *𝐴𝑥* , then there is no pos-

2

sibility for the attacker to compute the exact coordinates to perform an

attack, and the same thing is applicable on the receiver side as well.

# Concluding remarks

In the current paper, we initially reviewed Jongseok Ryu et al.’s re- cently published Three Factor Mutual Authentication Protocol for TMIS based on ECC. Later, we have shown that their proposal is defenseless to session key disclosure attack, MITM attack, Message Substitution attack, stolen verifier attack and privileged insider attack which results in inse- curity to the application. In this paper, we have projected the loopholes by performing the cryptanalysis on the Jongseok Ryu et al. proposal, and we have also addressed the suggestions for the improvement of the protocol. We are proposing an authentication protocol to prevent the above mentioned security threats in the near future.

# Declaration of Competing Interest

Authors declare that they have no conflict of interest.

# References

1. [C.-L. Hsu, T.-V. Le, M.-C. Hsieh, K.-Y. Tsai, C.-F. Lu, T.-W. Lin, Three-factor UC- SSO scheme with fast authentication and privacy protection for telecare medicine information systems, IEEE Access 8 (2020) 196553–196566.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0001)
2. [S. Son, J. Lee, M. Kim, S. Yu, A.K. Das, Y. Park, Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain, IEEE Access 8 (2020) 192177–192191.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0002)
3. [S.S. Sahoo, S. Mohanty, B. Majhi, A secure three factor based authentication scheme for health care systems using IoT enabled devices, J. Ambient Intell. Humaniz. Com- put. 12 (1) (2021) 1419–1434.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0003)
4. [S. Shamshad, M.F. Ayub, K. Mahmood, S. Kumari, S.A. Chaudhry, C.-M. Chen, An enhanced scheme for mutual authentication for healthcare services, Digit. Commun. Netw. 8 (2) (2022) 150–161.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0004)
5. [M. Tanveer, A. Alkhayyat, S.A. Chaudhry, Y.B. Zikria, S.W. Kim, et al., REAS-TMIS: resource-eﬃcient authentication scheme for telecare medical information system, IEEE Access 10 (2022) 23008–23021.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0005)
6. [J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, Y. Park, Secure ECC-based three-factor mutual authentication protocol for telecare medical information system, IEEE Access 10 (2022) 11511–11526.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0006)
7. [C.S. Nayak, et al., An improved user authentication scheme for electronic medical record systems, Multimed. Tools Appl. 79 (29) (2020) 22007–22026.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0007)
8. [R. Madhusudhan, C.S. Nayak, A robust authentication scheme for telecare medical information systems, Multimed. Tools Appl. 78 (11) (2019) 15255–15273.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0008)
9. [K. Renuka, S. Kumari, X. Li, Design of a secure three-factor authentication scheme for smart healthcare, J. Med. Syst. 43 (5) (2019) 1–12.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0009)
10. [M.K. Khan, S. Kumari, An authentication scheme for secure access to healthcare services, J. Med. Syst. 37 (4) (2013) 1–12.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0010)
11. [D. Giri, T. Maitra, R. Amin, P.D. Srivastava, An eﬃcient and robust RSA-based re- mote user authentication for telecare medical information systems, J. Med. Syst. 39](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0011)

[(1) (2015) 1–9.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0011)

1. [R. Amin, G.P. Biswas, An improved RSA based user authentication and session key agreement protocol usable in TMIS, J. Med. Syst. 39 (8) (2015) 1–14.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0012)
2. [A.K. Sutrala, A.K. Das, V. Odelu, M. Wazid, S. Kumari, Secure anonymity-preserv- ing password-based user authentication and session key agreement scheme for tele- care medicine information systems, Comput. Methods Progr. Biomed. 135 (2016) 167–185.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0013)
3. [L. Zhang, S. Zhu, Robust ECC-based authenticated key agreement scheme with pri- vacy protection for telecare medicine information systems, J. Med. Syst. 39 (5) (2015) 1–11.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0014)
4. [W. Liu, Q. Xie, S. Wang, B. Hu, An improved authenticated key agreement protocol for telecare medicine information system, SpringerPlus 5 (1) (2016) 1–16.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0015)
5. [A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, A robust and eﬃcient ECC-based mutual authentication and session key generation scheme for healthcare applications, J. Med. Syst. 43 (1) (2019) 1–22.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0016)
6. [S. Kumari, P. Chaudhary, C.-M. Chen, M.K. Khan, et al., Questioning key compromise attack on Ostad-Sharif et al.’s authentication and session key generation scheme for healthcare applications, IEEE Access 7 (2019) 39717–39720.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0017)
7. [M. Burrows, M. Abadi, R.M. Needham, A logic of authentication, Proc. R. Soc. Lond. A 426 (1871) (1989) 233–271.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0018)
8. [M. Abdalla, P.-A. Fouque, D. Pointcheval, Password-based authenticated key ex- change in the three-party setting, in: International Workshop on Public key Cryp- tography, Springer, 2005, pp. 65–84.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0019)
9. [J. Lee, G. Kim, A.K. Das, Y. Park, Secure and eﬃcient honey list-based authentication protocol for vehicular ad hoc networks, IEEE Trans. Netw. Sci. Eng. 8 (3) (2021) 2412–2425.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0020)
10. [J. Srinivas, A.K. Das, M. Wazid, A.V. Vasilakos, Designing secure user authentication protocol for big data collection in IoT-based intelligent transportation system, IEEE Internet Things J. 8 (9) (2020) 7727–7744.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0021)
11. [Y. Lu, L. Li, H. Peng, Y. Yang, An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem, J. Med. Syst. 39 (3) (2015) 1–8.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0022)
12. [R. Amin, S.K.H. Islam, P. Gope, K.-K.R. Choo, N. Tapas, Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical infor- mation system, IEEE J. Biomed. Health Inform. 23 (4) (2018) 1749–1759.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0023)
13. [Q. Jiang, Z. Chen, B. Li, J. Shen, L. Yang, J. Ma, Security analysis and improve- ment of bio-hashing based three-factor authentication scheme for telecare medical information systems, J. Ambient Intell. Humaniz. Comput. 9 (4) (2018) 1061–1073.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0024)
14. [N. Ravanbakhsh, M. Nazari, An eﬃcient improvement remote user mutual authenti- cation and session key agreement scheme for e-health care systems, Multimed. Tools Appl. 77 (1) (2018) 55–88.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0025)
15. [A. Ostad-Sharif, D. Abbasinezhad-Mood, M. Nikooghadam, An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utiliza- tion of ECC, Int. J. Commun. Syst. 32 (5) (2019) e3913.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0026)
16. [M. Qi, J. Chen, New robust biometrics-based mutual authentication scheme with key agreement using elliptic curve cryptography, Multimed. Tools Appl. 77 (18) (2018) 23335–23351.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0027)
17. [S.S. Sahoo, S. Mohanty, B. Majhi, Improved biometric-based mutual authentica- tion and key agreement scheme using ECC, Wirel. Pers. Commun. 111 (2) (2020) 991–1017.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0028)
18. [X. Zeng, G. Xu, X. Zheng, Y. Xiang, W. Zhou, E-AUA: an eﬃcient anonymous user authentication protocol for mobile IoT, IEEE Internet Things J. 6 (2) (2018) 1506–1519.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0029)
19. [S. Mandal, B. Bera, A.K. Sutrala, A.K. Das, K.-K.R. Choo, Y. Park, Certificateless-sign- cryption-based three-factor user access control scheme for IoT environment, IEEE Internet Things J. 7 (4) (2020) 3184–3197.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0030)
20. [M. Shuai, B. Liu, N. Yu, L. Xiong, Lightweight and secure three-factor authentica- tion scheme for remote patient monitoring using on-body wireless networks, Secur. Commun. Netw. 2019 (2019) 1–15.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0031)
21. [J. Mo, Z. Hu, Y. Lin, Cryptanalysis and security improvement of two authentica- tion schemes for healthcare systems using wireless medical sensor networks, Secur. Commun. Netw. 2020 (2020) 1–11.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0032)
22. [M. Fotouhi, M. Bayat, A.K. Das, H.A.N. Far, S.M. Pournaghi, M.-A. Doostari, A lightweight and secure two-factor authentication scheme for wireless body area net- works in health-care IoT, Comput. Netw. 177 (2020) 107333.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0033)
23. [H. Taleb, A. Nasser, G. Andrieux, N. Charara, E. Motta Cruz, Wireless technologies, medical applications and future challenges in WBAN: a survey, Wirel. Netw. 27 (8) (2021) 5271–5295.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0034)
24. [J. Li, Z. Su, D. Guo, K.-K.R. Choo, Y. Ji, PSL-MAAKA: provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in in- ternet of medical things, IEEE Internet Things J. 8 (17) (2021) 13183–13195.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0035)
25. [M.A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar, K. Mahmood, Security analysis on ‘a secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems’, IEEE Syst. J. 15 (4) (2021) 5557–5559.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0036)
26. [X. Xia, S. Ji, P. Vijayakumar, J. Shen, J.J. Rodrigues, An eﬃcient anonymous authen- tication and key agreement scheme with privacy-preserving for smart cities, Int. J.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0037)

[Distrib. Sens. Netw. 17 (6) (2021).](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0037) [15501477211026804](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0037)

1. [P. Vijayakumar, M.S. Obaidat, M. Azees, S.K.H. Islam, N. Kumar, Eﬃcient and secure](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0038)

[anonymous authentication with location privacy for IoT-based WBANs, IEEE Trans. Ind. Inf. 16 (4) (2019) 2603–2611.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0038)

1. [C.M. Kumar, R. Amin, M. Brindha, Cryptanalysis and improvement of REAS-TMIS: resource-eﬃcient authentication scheme for telecare medical information system, Secur. Privacye 6 (1) (2023) e268 Security and Privacy, Wiley.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0039)
2. [K. Prateek, F. Altaf, R. Amin, S. Maity, A privacy preserving authentication proto- col using quantum computing for V2I authentication in vehicular ad hoc networks, Secur. Commun. Netw. 2022 (2022) 1–17.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0039)
3. [X. Li, T. Liu, M.S. Obaidat, F. Wu, P. Vijayakumar, N. Kumar, A lightweight pri- vacy-preserving authentication protocol for VANETs, IEEE Syst. J. 14 (3) (2020) 3547–3557.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0040)
4. [P. Yu, W. Ni, G. Yu, H. Zhang, R.P. Liu, Q. Wen, Eﬃcient anonymous data authen- tication for vehicular ad hoc networks, Secur. Commun. Netw. 2021 (2021) 1–14.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0041)
5. [T.-Y. Wu, Z. Lee, L. Yang, C.-M. Chen, A provably secure authentication and key exchange protocol in vehicular ad hoc networks, Secur. Commun. Netw. 2021 (2021) 1–17.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0042)
6. [S. Olariu, A survey of vehicular cloud research: trends, applications and challenges, IEEE Trans. Intell. Transp. Syst. 21 (6) (2019) 2648–2663.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0043)
7. [S. Kona, S.V.K.R. Morthala, R. Konathala, P.K. Pinninti, H.K. Mavuru, A. Maria, An eﬃcient key agreement and anonymous mutual authentication protocols for secure communication in VANETs, in: 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC), IEEE, 2022, pp. 146–151.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0044)
8. [O. Galindo, V. Kreinovich, O. Kosheleva, Current quantum cryptography algorithm is optimal: a proof, in: 2018 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE, 2018, pp. 295–300.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0045)
9. [C. Ottaviani, M.J. Woolley, M. Erementchouk, J.F. Federici, P. Mazumder, S. Piran- dola, C. Weedbrook, Terahertz quantum cryptography, IEEE J. Sel. Areas Commun. 38 (3) (2020) 483–495.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0046)
10. [Y. Li, P. Zhang, R. Huang, Lightweight quantum encryption for secure transmission of power data in smart grid, IEEE Access 7 (2019) 36285–36293.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0047)
11. [D. Jin, P. Verma, S. Kartalopoulos, Key distribution using dual quantum channels, in: 2008 The Fourth International Conference on Information Assurance and Security, IEEE, 2008, pp. 327–332.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0048)
12. [P. Bagga, A.K. Das, J.J. Rodrigues, Bilinear pairing-based access control and key agreement scheme for smart transportation, Cyber Secur. Appl. 1 (2023) 100001.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0049)
13. [W. Yan, S. Ji, A secure and eﬃcient DSSE scheme with constant storage costs in smart devices, Cyber Secur. Appl. 1 (2022) 100006.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0050)
14. [L. Zhang, S. Zhu, S. Tang, Privacy protection for telecare medicine information sys- tems using a chaotic map-based three-factor authenticated key agreement scheme, IEEE J. Biomed. Health Inform. 21 (2) (2016) 465–475.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0051)
15. [S. Qiu, G. Xu, H. Ahmad, L. Wang, A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems, IEEE Access 6 (2017) 7452–7463.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0052)
16. [S.A. Chaudhry, H. Naqvi, M.K. Khan, An enhanced lightweight anonymous biomet- ric based authentication scheme for TMIS, Multimed. Tools Appl. 77 (5) (2018) 5503–5524.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0053)
17. [S.A. Chaudhry, K. Yahya, M. Karuppiah, R. Kharel, A.K. Bashir, Y.B. Zikria, GCAC- S-IoD: a certificate based generic access control scheme for internet of drones, Com- put. Netw. 191 (2021) 107999.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0054)
18. [D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0055)

[(2) (1983) 198–208.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0055)

1. [D. Kwon, Y. Park, Y. Park, Provably secure three-factor-based mutual authentication scheme with PUF for wireless medical sensor networks, Sensors 21 (18) (2021) 6039.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0056)
2. [J. Oh, S. Yu, J. Lee, S. Son, M. Kim, Y. Park, A secure and lightweight authentication protocol for IoT-based smart homes, Sensors 21 (4) (2021) 1488.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0057)
3. [S. Yu, N. Jho, Y. Park, Lightweight three-factor-based privacy-preserving authenti- cation scheme for IoT-enabled smart homes, IEEE Access 9 (2021) 126186–126197.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0058)
4. [R. Canetti, H. Krawczyk, Universally composable notions of key exchange and se- cure channels, in: International Conference on the Theory and Applications of Cryp- tographic Techniques, Springer, 2002, pp. 337–351.](http://refhub.elsevier.com/S2772-9184(23)00001-2/sbref0059)

**C Madan Kumar** received the B.Tech. degree in Computer Science and Engineering from Dr. Paul Raj Engineering College (JNT University), Hyderabad, India, in the year 2004, M.Tech. degree in Software Engineering from Vaagdevi College of Engineering (JNTU- niversity, Hyderabad) India, in the year 2012 and also pursuing his Ph.D. degree from NIT Tiruchirappalli. He is working as Assistant Professor in the Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal, Telan- gana, India. His areas of interest include Multimedia Security, Cryptography and Network Security, Cryptanalytic attacks, Authentication Protocols, WSN Security, IoT Security and Image Security.

**Ruhul Amin** received doctoral (Ph.D.) degree in Computer Science and Engineering from the Indian Institute of Technology(ISM) Dhanbad, Jharkhand, India, in 2017. Dr. Amin received B.Tech and M.Tech both in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology, West Bengal, India in 2009 and 2013, respec- tively. Presently, he is working as an Assistant Professor in the Department of Computer Science and Engineering, Dr. Shyama Prasad Mukherjee International Institute of Infor- mation Technology, Naya Raipur, India. He has authored many technical research papers published in leading international conferences and peer reviewed international journals from the IEEE, Elsevier, Springer, John Wiley, etc. Some of his research findings are pub- lished in top cited journals such as IEEE Transactions on cloud computing, IEEE Trans- action on Consumer Electronics, IEEE Internet of Things, IEEE System Journal, Ad-Hoc Networks, Computer Networks, Future Generation Computer Science, Journal of Network and Computer Application of Elsevier. He is also serving as Associate Editor of ‘Security and Privacy Journal’ published by John Wiley. He has been included in the subject-wise ranking of top 2 percent scientists from India (all fields) in the area of Networking & Telecommunications. His research interest includes Cryptography and Network Security, Authentication protocol, WSN Security, IoT Security and blockchain technology.

**Dr. M. Brindha** was born in Nagercoil, Tamil Nadu, India, in 1983. She received her B.E. degree from Dr. SivanthiAditanar College of Engineeing, Tiruchendur, India in the year of 2004; and her M. E. Degree from Government College of Engineering, Tirunelveli, India in the year of 2006. She received her Ph.D. degree from National Institute of Technology, Tiruchirappalli, in 2016. From February 2009 onwards she is working as an Assistant Professor in the Department of Computer Science and Engineering, National Institute of Technology Tiruchirappalli, Tamilnadu, India. Her areas of interest include Multimedia security, Cryptanalytic attacks, Multimedia compression.