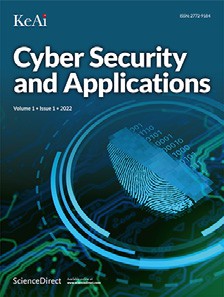
[Cyber Security and Applications 1 (2023) 100008](https://doi.org/10.1016/j.csa.2022.100008)

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 on “a secure three-factor user authentication and key agreement protocol for TMIS with user anonymity ”

Anjali Singh, Marimuthu Karuppiah[∗](#_bookmark1), Rajendra Prasad Mahapatra

*Department of Computer Science and Engineering, SRM Institute of Science and Technology, NCR Campus, Ghaziabad, Uttar Pradesh 201204, India*

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

*Keywords:* Authentication Smart cards

Telecare medicine information system User anonymity

The health-care delivery services were made possible by telecare medicine information systems (TMIS). These systems are paving the way for a world where computerised telecare facilities and automated patient medical records are the norm. Authentication schemes are common mechanisms for preventing unauthorised access to medical records via insecure networks. Amin and Biswas recently proposed an authentication scheme for TMIS, asserting that their scheme can withstand various attacks. Despite this, their scheme still has significant security weaknesses. In this paper, we present a cryptanalysis of Amin and Biswas’ scheme and show that it is subject to a variety of attacks.

# Introduction

The increased proliferation of distributed networks has resulted in more resource and service exchange among user devices. As a result, during this cyber-connected period, there has been an increase in trans- action volume.

Due to the open nature of network that is dispersed, for application systems, system security and robust privacy protection techniques have become an inevitable requirement. As a result, authentication of the user may be a critical security element that must be included in such systems in order to distinguish legitimate users from potential threats.

One of the applications of distributed networks is the Telecare med- ical information system (TMIS). TMIS creates an effective and practical connection through an insecure internet between the patient and the doctor. Therefore, in order to access critical medical data over unse- cure communication, data security, privacy, and user authentication are of utmost importance. There have been numerous user authentication mechanisms for TMIS proposed recently [[1–22](#_bookmark4)], but it has been shown that the majority of these protocols fall short of meeting all security requirements.

tication. It’s also susceptible to forging and password guessing attacks when used oﬄine.

The remainder of the paper is divided into the following sections. The scheme devised by Amin and Biswas is examined in [Section 2](#_bookmark0). [Section 3](#_bookmark2) discusses the problems in Amin and Biswas’ strategy. In [Section 4](#_bookmark3), you’ll find the conclusions.

# Review of the scheme [[24]](#_bookmark9)

Registration, login, authentication, and password update are the four sections of the authentication process. The explanations are as follows:

* 1. *Notations*

The notations used in this paper are defined in the table.

Notation Description

*𝑈𝑗* User

*𝑟* Random variable

*𝐴* Adversary

Recently, Mishra et al. [[23]](#_bookmark8) suggested a user authentication tech-

nique with anonymity for the users. Unfortunately, according to Amin

*𝐼𝐷𝑗*

Identity of the user

and Biswas [[24]](#_bookmark9), user anonymity is not guaranteed by the technique and mutual authentication in Mishra et al’s strategy. Furthermore, Amin and Biswas concluded that Mishra et al’s is susceptible to a variety of attacks. Then, to address the shortcomings in Mishra et al’s scheme, Amin and Biswas provided an updated authentication scheme. First, we show that Amin and Biswas’s strategy [[24]](#_bookmark9) is not able to satisfy the user anonymity property and doesn’t give complete forward secrecy and mutual authen-

∗ Corresponding author.

*E-mail address:* [marimuthume@gmail.com](mailto:marimuthume@gmail.com) (M. Karuppiah).

*𝑃𝑊 𝐷𝑗* Password of the user

*𝑇𝑗* fingerprint

H() Bio-hash function

*ℎ*(⋅) One-way hash function

SC Smart card

*𝑆𝐾* Session key

|| Concatenation operation

⋅ ECC based scalar point multiplication

*⊕* Bit-wise exclusive OR operation

<https://doi.org/10.1016/j.csa.2022.100008>

Received 3 May 2022; Received in revised form 4 July 2022; Accepted 10 September 2022

Available online 23 September 2022

2772-9184/© 2022 The Authors. Published by Elsevier B.V. on behalf of KeAi Communications Co., Ltd. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

* 1. *User registration phase*

The medical server accepts registrations from anyone during this phase to gain access to medical services.

1. User selects *𝐼𝐷𝑗* , password *𝑃 𝑊 𝐷𝑗* , and biometric template such as fingerprint *𝑇𝑗* . Then, *𝑈𝑗* submits *𝐼𝐷𝑗* , *𝐴𝑗* , and *𝐹𝑗* through se- cure link or in person to the medical server after computing *𝐴𝑗* = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑗* ) and *𝐹𝑗* = *𝐻* (*𝑇𝑗* ).
2. Then, Medical server *𝑆* computes *𝐴𝑗* = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑗* ), *𝐾* =

*ℎ*(*𝐼 𝐷𝑠* ||*𝑧*||*𝐼 𝐷𝑗* ), *𝐵𝑗* = *ℎ*(*𝐼 𝐷𝑗* ||*𝐴𝑗* ) *⊕ 𝐾* , *𝐶 𝐼 𝐷𝑗* = *𝐸𝑧* (*𝐼 𝐷𝑗* ||*𝑟*) and issues

a SC for the *𝑈* after storing *𝐹* , *𝐴* , *𝐵* , *𝐶𝐼𝐷* , *ℎ*(⋅), *𝐻* (⋅) into the

*2.5. Password change phase*

It’s a useful attribute for adding a password change phase to any password-based user authentication mechanism, allowing users to change their passwords without the need for a medical server.

1. The *𝑈𝑗* first puts the SC into the card reader and performs steps 1 and 2 of the login phase to verify the *𝑈* ′ s authenticity. After that, the

*𝑗*

card reader performs the procedures below to successfully change the password.

1. After user authentication, the card reader prompts the user to en-

ter a new password, *𝑃 𝑊 𝐷𝑛𝑒𝑤*, into the *𝑈𝑗* , and after doing so,

*𝑗 𝑗*

*𝑗 𝑗 𝑗*

*𝑗*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

memory of the SC using protected channel. We assume that a user

selects low entropy *𝐼𝐷* , *𝑃 𝑊 𝐷* that are individually guessable in

the card reader computes the values *𝐴𝑗* = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑗* ) and

*𝐵𝑛𝑒𝑤* = *ℎ*(*𝐼𝐷𝑗* ||*𝐴𝑛𝑒𝑤*) *⊕ 𝐾* , where *𝐾* is the old parameter, and then

*𝑗 𝑗*

*𝑗 𝑗*

*𝑛𝑒𝑤*

*𝑛𝑒𝑤*

time that is polynomial.

* 1. *Login phase*

the card reader replaces *𝐴𝑗* , *𝐵𝑗* with the new values *𝐴𝑗*

and the password change phase is successfully completed.

# Cryptanalysis of Amin and Biswa’s scheme

, *𝐵𝑗*

The *𝑈𝑗* can use a medical server with a card reader or terminal device

to access the medical server at any time and from any location after

successfully completing the registration procedure. The following is a list of all the steps in this phase:

1. The *𝑈𝑗* first embeds his or her SC into the card reader device, then embeds the biometric template *𝑇𝑗* into the sensor device. *𝐹* ∗ = *𝐻* (*𝑇𝑗* ) is computed by the card reader and compared to the stored *𝐹𝑗* . Bio- metric verification is successful if it matches, and the *𝑈𝑗* is asked to input *𝐼𝐷𝑗* , *𝑃 𝑊 𝐷𝑗* ; otherwise, the connection is terminated.

*𝑗*

1. *𝐴*∗ = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑗* ) is computed by the card reader and compared

*𝑗*

to the stored *𝐴𝑗* . The matching result determines whether or not the *𝑈𝑗* provided valid *𝐼𝐷𝑗* , *𝑃 𝑊 𝐷𝑗* . Proceed to the next stage if it

matches; Else, the connection will be canceled.

1. The terminal generates a nonce at random *𝑟𝑗* and calculates *𝐷*1 = *𝑟𝑗* ⋅

*𝑁* , *𝐾* = *𝐵𝑗 ⊕ ℎ*(*𝐼 𝐷𝑗* ||*𝐴*∗), *𝐷*2 = *𝑟𝑗 ⊕ 𝐾*, *𝐷*4 = *ℎ*(*𝐼𝐷𝑗* ||*𝑟𝑗* ||*𝐾*) and sends

*𝐷*2 , *𝐷*4 and *𝐶𝐼𝐷𝑗* over the public/open channel as a login message

*𝑗*

to the medical server.

*2.4. Authentication and key agreement phase*

The *𝑈𝑗* and the medical server must establish mutual authentication and a shared session key agreement at this phase. All of the steps in this

phase are listed below:

1. The medical server decrypts *𝐶𝐼𝐷𝑗* using the server’s secret key *𝑧*

and gets (*𝐼𝐷*∗||*𝑟*) = *𝐷𝐸𝑧* (*𝐶𝐼𝐷𝑗* ), *𝐾* = *ℎ*(*𝐼𝐷𝑠* ||*𝑧*||*𝐼𝐷*∗), *𝑟*∗ = *𝐷*2 *⊕ 𝐾*,

This section describes the security limitations of the scheme in Amin and Biswas [[24]](#_bookmark9).

* 1. *Adversary model*

Adversary modeling is a crucial component of creating an authen- ticated protocol. A strategy for strengthening security by categorizing vulnerabilities and goals, and hence establishing protective measures against threats to the system, is known as adversary modeling. In this context, a threat could be a harmful attack carried out by an enemy, such as an adversary who could harm the resources. The adversary model is based on the assumptions below. These assumptions regarding an adver- sary’s prowess are legitimate, and they’ve been made in contemporary works as well:

1. The message that was communicated across the insecure communi- cation channels has little influence on the adversary. Intercepting, altering, and deleting any conveyed message are all examples of this [[25–27]](#_bookmark5)
2. Using a power analysis technique, the adversary can retrieve the security parameters encoded in the smart card [[28–31]](#_bookmark6).
3. The password dictionary can be enumerated oﬄine by adversary [[32,33]](#_bookmark7).
   1. *Fails to oﬀer user anonymity*

Assume Adversary acquires the value *𝐴𝑗* , *𝐵𝑗* under assumption 2

from the stolen smart card, and the adversary intercepts the *𝑈𝑗* ’s lo-

*𝑗 𝑗 𝑗*

*𝐷*∗ = *𝑟*∗ ⋅ *𝑁* , *𝐷*∗ = *ℎ*(*𝐼𝐷𝑗* ||*𝑟*∗||*𝐾*) and matches *𝐷*∗ with the received

gin request message (*𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑢* ). Now, Adversary has values

1 *𝑗* 4 *𝑗* 4

*𝐷*4. The medical server trusts it if it matches the *𝑈𝑗* ’s legitimacy.

1. The medical server generates a nonce at random *𝑟𝑘* and cal-

culates *𝐷*1 = *𝑟𝑘* ⋅ *𝑁* , *𝑆𝐾* = *𝑟𝑘* ⋅ *𝐷*∗ = *𝑟𝑘* ⋅ *𝑟*∗ ⋅ *𝑁* , *𝐽*1 = *𝐻*1 + *𝐷*∗, *𝐿𝑗* =

(*𝐴𝑗* , *𝐵𝑗* , *𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑢* ). Adversary can find the user *𝑈𝑗* ’s *𝐼𝐷𝑗* by

doing the following:

1 *𝑗*

∗ ′ ∗ ′

1 1. Adversary assumes the identify of the user as *𝐼𝐷𝑎* .

*ℎ*(*𝐼𝐷𝑗* ||*ℎ*(*𝐻*1 )||*𝐾* ), *𝐶 𝐼𝐷𝑗* = *𝐸𝑧* (*𝐼𝐷𝑗* ||*𝑟* ) and transmits a reply mes-

sage *𝐿* , *𝐽*1 and *𝐶𝐼𝐷*′ to the *𝑈* through the public channel, where

* 1. Compute *𝐾𝑎* = *𝐵𝑗 ⊕ ℎ*(*𝐼𝐷𝑎* ||*𝐴𝑗* ) = *ℎ*(*𝐼𝐷𝑗* ||*𝐴𝑗* ) *⊕ ℎ*(*𝐼𝐷𝑠* ||*𝑧*||*𝐼𝐷𝑗* ) *⊕*

*ℎ*(*𝐼𝐷* ||*𝐴* ).

*𝑗 𝑗 𝑗*

*𝑎 𝑗*

*𝑟*′ is the medical server generates a random number.

* 1. Compute *𝑟*∗ = *𝐷*2 *⊕ 𝐾* = *𝑟 ⊕ 𝐾 ⊕ 𝐾* .

*𝑗 𝑎 𝑗 𝑎*

1. The *𝑈𝑗* computes *𝐻* ∗ = *𝐽*1 − *𝐷*∗, *𝐿*∗ = *ℎ*(*𝐼 𝐷𝑗* ||*ℎ*(*𝐻* ∗)||*𝐾*), *𝑆𝐾* = *𝑟𝑗* ⋅ 4. Compute *𝐷*∗ = *ℎ*(*𝐼𝐷𝑎* ||*𝑟*∗||*𝐾𝑎* ).

∗ 1 1 *𝑗* 1

4 *𝑗*

?

*𝐻*1 = *𝑟𝑗* ⋅ *𝑟𝑘* ⋅ *𝑁* , and matches *𝐿*∗ with the received *𝐿𝑗* depending on the reply message received. If they match, the *𝑈𝑗* trusts the medical

*𝑗*

tion by sharing *𝑆𝐾*. After mutual authentication, the *𝑈𝑗* replaces the server’s legitimacy, then the protocol performs mutual authentica-

′previous *𝐶𝐼𝐷* in the SC’s memory with the new *𝐶𝐼𝐷* . Finally, the

*𝑈𝑗* computes *𝑍𝑗* = *ℎ*(*𝐼𝐷𝑟* ||*𝑆𝐾*) and sends it via the public channel to

*𝑗*

*𝑗*

the medical server.

1. Following receipt, the server calculates *𝑍* ∗ = *ℎ*(*𝐼𝐷*∗||*𝑆𝐾*) and com-
2. Compare *𝐷*∗ = *𝐷*4. If this is the case, the adversary’s guessed identity

is right.

4

1. If false, the adversary must repeat steps (1–4) until the current iden- tity is obtained.

have a time complexity of *𝑂*(∣ *𝐷𝐼𝐷* ∣ ×(4*𝑇𝑥𝑜𝑟* + 6*𝑇ℎ* )), where ∣ *𝐷𝐼𝐷* ∣ de- Hence, the attacker can learn the user’s identify. The foregoing steps

notes the identity space size, *𝑇𝑥𝑜𝑟* denotes the *𝑋𝑂𝑅* operation execution

*𝑗 𝑗*

pares it to the received *𝑍𝑗* . If they’re compatible, both sides begin

secure communication.

time, and *𝑇ℎ* denotes the hash operation execution time. As a result,

Amin and Biswas’s scheme fails to offer user anonymity.

* 1. *Prone to offiine passsword guessing attack*

Assume Adversary obtain the values {*𝐴𝑗* , *𝐵𝑗* , *𝐽𝑖* , *ℎ*(⋅)} under assump- tion 2, the login request message is intercepted by Adversary from the

stolen/lost *𝑆𝐶* of (*𝐼𝐷𝑗* , *𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑢* ) under assumption 1. As

previously stated, Adversary can uncover a user’s original identification

*𝐼𝐷𝑗* . Adversary can perform an oﬄine password guessing attack using

these values as follows:

the authenticity of the user, but the user can also verify the server’s le- gitimacy. Furthermore, no unauthorised users or cloud servers have the ability to impersonate a legitimate user or server. An attacker can mimic a valid user, as previously stated. As a result, the mutual authentication setup is broken. As a result, mutual authentication is not achievable.

# Conclusion

1. Adversary assumes password of the user *𝑈𝑗*

∗

as *𝑃 𝑊 𝐷𝑎* .

We investigated Amin and Biswas’s authentication technique and

found that it is not able to deliver user anonymity, mutual authenti-

1. Compute *𝑧𝑗* = *𝐽𝑖 ⊕ ℎ*(*𝐴𝑗 ⊕ 𝑃𝑊 𝐷𝑗* ) = *𝑧𝑗 ⊕ ℎ*(*𝐴𝑗 ⊕ 𝑃𝑊 𝐷𝑗* ) *⊕ ℎ*(*𝐴𝑗 ⊕*

*𝑃 𝑊 𝐷𝑗* ) = *𝑧𝑗* .

1. Compute *𝐴*∗ = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑎* ).

*𝑗*

1. Compare *𝐴* =? *𝐴*∗. If this is the case, adversary’s guessed *𝑃 𝑊 𝐷* is

*𝑗 𝑗 𝑎*

correct.

1. If false, the adversary must repeat steps (1–4) till you get your hands on the current password.

Hence, the attacker can learn the user’s password.

The foregoing steps take *𝑂*(∣ *𝐷𝑃𝑊 𝐷* ∣ ×(6*𝑇𝑥𝑜𝑟* + 4*𝑇ℎ* )), where ∣ *𝐷𝑃𝑊 𝐷* ∣ denotes the identity space size, *𝑇𝑥𝑜𝑟* presents the XOR operation execu- tion time, and *𝑇ℎ* presents the hash operation execution time. In reality, the password space is usually somewhat limited, such as ∣ *𝐷𝑃𝑊 𝐷* ∣*<*=

106 . As a result, Amin and Biswas’s strategy is susceptible to an oﬄine

password guessing attack.

* 1. *Fails to oﬀer perfect forward secrecy*

umented the messages that had previously been conveyed (*𝐼𝐷𝑗* , *𝐷*2, Assume that under assumption 2, Adversary intercepted and doc-

*𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑢* ) and (*𝑇𝑠* , *𝑀𝑗* ) and obtained the value (*𝐴𝑗* , *𝐵𝑗* , *𝐽𝑖* , *ℎ*(⋅))

from the *𝑆𝐶*. If the attacker has the user password *𝑃 𝑊 𝐷𝑗* as previously

discussed, the previously traded session key can be calculated as follows:

1. Adversary computes *𝐴𝑗* = *ℎ*(*𝐼𝐷𝑗* ||*𝑃 𝑊 𝐷𝑗* ) and *𝑧𝑗* = *𝐽𝑖 ⊕ ℎ*(*𝐴𝑗* ||*𝑃 𝑊 𝐷𝑗* ).
2. Then Adversary computes the *𝑆𝐾* = *ℎ*(*𝐼𝐷 ⊕ 𝐴 ⊕ 𝑧 ⊕ 𝑇 ⊕ 𝑇* ).

cation and perfect forward secrecy. Oﬄine password guessing and forg- ing attacks are also possible. As a result, Amin and Biswas’s technique for wireless network communication is unsafe. Future efforts will be fo- cused on bolstering Amin and Biswas’s scheme, which will be capable of meeting all security criteria and objectives.

# Funding statement

This research received no specific grant from any funding agency in the public, commercial, or not for profit sectors.

# Data availability statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

# Declaration of Competing Interest

Authors declare that they have no conflict of interest.

# References

1. [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(22)00008-X/sbref0001)
2. [C.-M. Chen, B. Xiang, E.W. Ke, T.-Y. Wu, J.C.-W. Lin, Improvement of an anonymous and lightweight authentication scheme for TMIS, J. Appl. Math. Phys. 6 (1) (2018)](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0002)

*𝑗 𝑗 𝑗*

*𝑢 𝑠*

[18–28.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0002)

As a result, since revealing the user’s password affects the secrecy of previous session keys, Amin and Biswa’s scheme doesn’t provide perfect forward secrecy.

* 1. *Prone to forgery attack*

Under assumption 2, Adversary acquires the values { *𝐴𝑗* , *𝐵𝑗* , *𝐽𝑖* , *ℎ*(⋅)

} from the smart card. As previously stated, Adversary can obtain *𝑈𝑗* ’s identification *𝐼𝐷𝑗* and password *𝑃 𝑊 𝐷𝑗* . Using this information, the ad-

message {*𝐼𝐷𝑗* , *𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑎* } to the server, where *𝑇𝑎* represents versary can complete the login phase steps and submit the login request

timestamp *𝑇𝑎* when it receives the message {*𝐼𝐷𝑗* , *𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑎* the Adversary’s current time stamp. Server can check the newness of the

} from attacker. Because Adversary utilises the correct timestamp, the verification is valid. The server then performs the processes of the au- thentication phase to verify that the adversary is a valid user. It’s obvious

request {*𝐼𝐷𝑗* , *𝐷*2 , *𝐶𝐼𝐷𝑗* , *𝐷*4 , *𝑇𝑗* , *𝑇𝑎* } is genuinely made by adversary that the server won’t notice anything or any deformity because the login

using the valid *𝑈* ’s identity *𝐼𝑑* and password *𝑃 𝑊 𝐷* . The message (*𝑇* ,

1. [N. Radhakrishnan, M. Karuppiah, An eﬃcient and secure remote user mutual au- thentication scheme using smart cards for telecare medical information systems, Inform. Med. Unlocked 16 (2019) 100092.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0003)
2. [P. Chandrakar, A.S. Chauhan, R. Ali, Cryptanalysis and improvement of a secure mutual authentication scheme for remote users, in: 2019 IEEE International Con- ference on Electrical, Computer and Communication Technologies (ICECCT), IEEE, 2019, pp. 1–9.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0004)
3. [T.-T. Truong, M.-T. Tran, A.-D. Duong, Improved chebyshev polynomials-based authentication scheme in client-server environment, Secur. Commun. Netw. 2019 (2019) 11 4250743.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0005)
4. [Y. Park, K. Park, Y. Park, Secure user authentication scheme with novel server mu- tual verification for multiserver environments, Int. J. Commun. Syst. 32 (7) (2019) e3929.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0006)
5. [M. Hasson, A.A. Yassin, A.J. Yassin, A.M. Rashid, A.A. Yaseen, H. Alasadi, Password authentication scheme based on smart card and QR code, Indones. J. Electr. Eng. Comput. Sci. 23 (1) (2021) 140–149.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0007)
6. [L. Chen, K. Zhang, Privacy-aware smart card based biometric authentication scheme for e-health, Peer-to-Peer Netw. Appl. 14 (3) (2021) 1353–1365.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0008)
7. [M. Adeli, N. Bagheri, H.R. Meimani, On the designing a secure biometric-based re- mote patient authentication scheme for mobile healthcare environments, J. Ambient Intell. Humaniz. Comput. 12 (2) (2021) 3075–3089.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0009)
8. [Y. Zhou, Y. Luo, M.S. Obaidat, P. Vijayakumar, X. Wang, PAMI-anonymous pass- word authentication protocol for medical internet of things, in: 2021 IEEE Global Communications Conference (GLOBECOM), IEEE, 2021, pp. 1–6.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0010)

*𝑗 𝑗*

*𝑗 𝑠*

1. [M.A. Khan, A. Ghani, M.S. Obaidat, P. Vijayakumar, K. Mansoor, S.A. Chaudhry,](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0011)

*𝑀𝑗* ) is then sent to user *𝑈𝑗* by Server *𝑆*. As a result, *𝑆* will accept Adver-

sary’s login request from *𝑈𝑗* . Adversary intercepts the (*𝑇𝑠* , *𝑀𝑗* ) commu-

nication and finds *𝑆𝐾* = *ℎ*(*𝐼𝐷 ⊕ 𝐴 ⊕ 𝑧 ⊕ 𝑇 ⊕ 𝑇* ). Finally, both the

[A robust anonymous authentication scheme using biometrics for digital rights man- agement system, in: 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), IEEE, 2021, pp. 1–5.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0011)

*𝑗 𝑗 𝑗*

*𝑢 𝑠*

1. [S. Jegadeesan, M.S. Obaidat, P. Vijayakumar, M. Azees, M. Karuppiah, Eﬃcient pri-](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0012)

Server and the Adversary will have the same *𝑆𝐾*. As a result, since the

the credentials of server *𝑆*, Amin and Biswa’s scheme is vulnerable to adversary can impersonate a valid user by successfully signing in using

forgery attack.

* 1. *Fails to oﬀer mutual authentication*

Mutual authentication is accomplished using an effective password authentication approach, which means that the server not only verifies

[vacy-preserving anonymous authentication scheme for human predictive online ed- ucation system, Cluster Comput. 25 (4) (2021) 2557–2571.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0012)

1. [M. Karuppiah, R. Saravanan, Cryptanalysis and an improvement of new remote mu- tual authentication scheme using smart cards, J. Discrete Math. Sci. Cryptogr. 18 (5) (2015) 623–649.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0013)
2. [P. Vijayakumar, M. Azees, S.A. Kozlov, J.J. Rodrigues, An anonymous batch au- thentication and key exchange protocols for 6G enabled VANETs, IEEE Trans. Intell. Transp. Syst. 23 (2) (2021) 1630–1638.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0014)
3. [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. Distrib. Sens. Netw. 17 (6) (2021) 1–13.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0015) [15501477211026804](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0015)
4. [L. Xiao, S. Xie, D. Han, W. Liang, J. Guo, W.-K. Chou, A lightweight authentica- tion scheme for telecare medical information system, Connect. Sci. 33 (3) (2021) 769–785.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0016)
5. [K. Chatterjee, A secure three factor-based authentication scheme for telecare medicine information systems with privacy preservation, Int. J. Inf. Secur. Privacy (IJISP) 16 (1) (2022) 1–24.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0017)
6. [V.P. Gaikwad, J.V. Tembhurne, C. Meshram, C.-C. Lee, Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function,](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0018)

[J. Supercomput. 77 (8) (2021) 8281–8304.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0018)

1. [Y. Chen, J. Chen, An eﬃcient and privacy-preserving mutual authentication with key agreement scheme for telecare medicine information system, Peer-to-Peer Netw. Appl. 15 (1) (2022) 516–528.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0019)
2. [H. Amintoosi, M. Nikooghadam, M. Shojafar, S. Kumari, M. Alazab, Slight: a lightweight authentication scheme for smart healthcare services, Comput. Electr. Eng. 99 (2022) 107803.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0020)
3. [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(22)00008-X/sbref0021)
4. [M. Soni, D.K. Singh, Privacy-preserving authentication and key-management proto- col for health information systems, in: Data Protection and Privacy in Healthcare, CRC Press, 2021, pp. 37–50.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0022)
5. [D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, M.K. Khan, et al., Crypt- analysis and improvement of Yan et al.’s biometric-based authentication scheme for telecare medicine information systems, J. Med. Syst. 38 (6) (2014) 1–12.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0023)
6. [R. Amin, G.P. Biswas, A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity, J. Med. Syst. 39 (8) (2015) 1–19.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0024)
7. [D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0025)

[(2) (1983) 198–208.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0025)

1. [M. Karuppiah, R. Saravanan, A secure remote user mutual authentication scheme using smart cards, J. Inf. Secur. Appl. 19 (4–5) (2014) 282–294.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0026)
2. [A. Pradhan, M. Karuppiah, R. Niranchana, M.A. Jerlin, S. Rajkumar, Design and analysis of smart card-based authentication scheme for secure transactions, Int. J. Internet Technol. Secur. Trans. 8 (4) (2018) 494–515.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0027)
3. [P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Annual International Cryp- tology Conference, Springer, 1999, pp. 388–397.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0028)
4. [T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0029)
5. [M. Karuppiah, A.K. Das, X. Li, S. Kumari, F. Wu, S.A. Chaudhry, R. Niranchana, Secure remote user mutual authentication scheme with key agreement for cloud environment, Mob. Netw. Appl. 24 (3) (2019) 1046–1062.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0030)
6. [A. Maria, V. Pandi, J.D. Lazarus, M. Karuppiah, M.S. Christo, BBAAS: blockchain-based anonymous authentication scheme for providing secure commu- nication in VANETs, Secur. Commun. Netw. 2021 (2021) 1–11 6679882.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0031)
7. [C.-G. Ma, D. Wang, S.-D. Zhao, Security flaws in two improved remote user authenti- cation schemes using smart cards, Int. J. Commun. Syst. 27 (10) (2014) 2215–2227.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0032)
8. [M. Azees, P. Vijayakumar, M. Karuppiah, A. Nayyar, An eﬃcient anonymous au- thentication and confidentiality preservation schemes for secure communications in wireless body area networks, Wirel. Netw. 27 (3) (2021) 2119–2130.](http://refhub.elsevier.com/S2772-9184(22)00008-X/sbref0033)