Electronic and Cyber Defens 2025/ Vol. 13/ No. 2/ 57-71

Electronic and Cyber Defens

ISSN: 2322-4347 , E-ISSN: 2980-8979

An Improved RFID-based Authentication Protocol with Application in Telecare Medical Systems

M. Noroozi[1*], K. Pormehr[2]

[1] Assistant Professor, Alzahra University, Tehran, Iran ([*]Correspondence: m.noroozi@alzahra.ac.ir)

[2] PhD Candidate in Computer Engineering at Islamic Azad University North Tehran Branc

[3] Master's degree, Higher Education Institute of Information Technology of Qom

A R T I C L E I N F O

Article history:

Article Type: Research paper

Received: 28 March 2025

Revised: 29 May 2025

Accepted: 18 June 2025

Available online: *28 June 2025*

How to cite this article:

M. Noroozi, K. Pormehr (2025). An Improved RFID-based Authentication Protocol with Application in Telecare Medical Systems. Electronic and Cyber Defens, 13 (2), 57-55.

Keywords:

Telecare Medical System

Internet of Things

RFID

Security

Privacy

Tracking Attack

A B S T R A C T

RFID technology has indeed revolutionized telecare medical systems by offering advantages such as non-contact, wireless communication, and unique identification capabilities. These features enable seamless integration and rapid development of RFID-based solutions in telecare, leading to benefits like continuous service delivery, reduced monitoring costs, accurate data recording, preventive care, and enhanced quality of services. Considering the sensitivity of medical data, various authentication protocols have been proposed to ensure secure deployment in telecare systems. This paper highlights the shortcomings of a recently proposed RFID authentication protocol and introduces a new improved protocol that meets the necessary security requirements. Comparisons with the related secure RFID protocols show the overall superiority of the proposed protocol in terms of computational and communication complexity.

Cite this article: Noroozi, M.©, Pormehr, K.© (2025). An Improved RFID-based Authentication Protocol with Application in Telecare Medical Systems. Journal of Electronic and Cyber Defens. 2025; 13l(2):57-71.
DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.6.3

Publisher: Imam Hossein University.

1- Introduction

The Internet of Things (IoT) has garnered significant attention in recent years by enabling communication and data exchange between diverse devices and systems. A critical application of this emerging technology is in the healthcare sector. IoT-based health systems can enhance medical services, predict diseases, manage patients, and improve the quality of healthcare. These systems are particularly vital for providing remote monitoring services to elderly, disabled, or contagious patients. The importance of remote care has been underscored during pandemics, such as COVID-19, by minimizing physical contact, especially for healthcare workers who are at higher risk and whose incapacitation could exacerbate public health crises. Remote Medical Care Systems (RMCS) ensure the continuous provision of routine care and regular remote assessments for patients without associated risks.

Security and user privacy are paramount in healthcare due to the sensitive nature of personal data, including medical history and treatment records. Radio Frequency Identification (RFID) technology is a crucial tool for addressing security and privacy challenges in IoT-based RMCS. Leveraging RFID solutions offers numerous advantages, including service continuity, reduced supervisory costs, accurate record-keeping, preventive care, and enhanced service quality. Features like non-contact operation, wireless communication, and unique identification facilitate the rapid deployment of RFID in RMCS.

A typical RFID system comprises tags attached to identifiable objects (patients/equipment), readers that read/write data from/to tags, and a backend server that stores sensitive patient information. While wireless data transmission via radio signals is convenient, it can introduce critical security and privacy vulnerabilities.

Recently, Shariq et al. [5] proposed a novel RFID-based authentication protocol for RMCS, designed for scenarios like the COVID-19 pandemic. While highly efficient, this paper demonstrates that, contrary to the authors' claims, Shariq et al. protocol is vulnerable to tag tracking attacks. Consequently, this paper proposes an improved protocol that addresses this vulnerability while maintaining high efficiency.

2- Objectives

The principal objectives of this research are:

- To perform a comprehensive security analysis of the recent RFID authentication protocol proposed by Shariq et al. [5], with a specific focus on investigating its resilience against tracking attacks.
- To design and propose a robust, enhanced RFID authentication protocol that effectively mitigates the identified tracking vulnerability in the original scheme.
- To conduct a formal security verification of the proposed protocol, demonstrating that it fulfills all essential security requirements for Remote Medical Care Systems (RMCS), including mutual authentication, forward secrecy, and resistance to known attacks.
- To evaluate the performance efficiency of the proposed protocol by analyzing its

computational and communication overhead, and to benchmark its performance against other state-of-the-art, secure RFID authentication protocols to establish its practical superiority

3- Achievements and Proposed Method

The main achievements of this work are as follows:

- Identification of Vulnerability: We successfully identified a critical vulnerability in the Shariq et al. protocol [5]. The protocol's design implicitly assumes the reader-server knows the shared secret (a_i) of the authenticating tag beforehand, which is impractical in large-scale systems. Addressing this by sending a_i in plaintext would make the protocol trivially traceable.
- Proposal of an Improved Protocol: We developed an enhanced authentication protocol based on the structure of the Shariq et al. protocol. The key modification involves the introduction of a new parameter, x_3, to securely and obliviously transmit the tag's secret a_i to the reader-server in an encrypted form.

4- Results and Analysis

After proposing an enhaced RFID authentication protocol for RMCS, we provide formal security proofs, demonstrating that the improved protocol achieves security properties such as confidentiality, mutual authentication, and forward secrecy. We also proved that the proposed protocol is secure against impersonation, replay, Denial-of-Service (DoS), tracking, and man-in-the-middle attacks. Our key achievement is resolving the tracking vulnerability present in the Shariq et al. protocol. We also analyzed the performance of the proposed protocol and compared it with other existing secure RFID authentication protocols in terms of computational and communication costs. The results demonsterate that the proposed protocol is more efficient than other existing fully secure protocols like [12] and [26]. In terms of the communication costs, the provided analysis demonstrates that protocols presented in [9] and [12] have slightly lower communication overhead compared to our protocol at the cost of lacking forward secrecy in [9] and being computationally far less efficient in [12].

5- Conclusion

This paper analyzed the security of a recently proposed RFID authentication protocol by Shariq et al. and identified its vulnerability to tracking attacks. An improved protocol was proposed, incorporating a novel mechanism to securely transmit the tag's secret. Security analysis confirms that the proposed protocol provides confidentiality, mutual authentication, forward secrecy, and resilience against a wide range of attacks. Performance comparisons reveal that the proposed protocol offers significantly higher computational efficiency than other fully secure protocols, making it a superior and practical choice for secure and efficient authentication in IoT-enabled remote healthcare systems.

پدافند الکترونیک و سایبری/ سال ۱۴۰۴/ دوره ۱۳/ شماره ۲/ صفحه ۷۱-۵۷

پدافند الکترونیک و سایبری

شاپا الکترونیکی: ۴۳۴۷- ۲۳۲۲۲ شاپا چاپی: ۸۹۷۹-۲۹۸۰

پروتکل احراز هویت بهبودیافته مبتنی بر RFID برای کاربرد در سامانه‌های مراقبت پزشکی از راه دور

مهناز نوروزی[۱]*، کوثر پرمهر[۲]

[۱] استادیار، گروه علوم کامپیوتر، دانشکده علوم ریاضی، دانشگاه الزهرا (س)، تهران، ایران (نویسنده مسئول: m.noroozi@alzahra.ac.ir)

[۲] دانشجوی کارشناسی ارشد، گروه ریاضی، دانشکده علوم ریاضی، دانشگاه الزهرا (س)، تهران، ایران (pormehr.kosar@yahoo.com)

چکیده (استایل عنوان چکیده)

ویژگی‌هایی مانند غیرتماسی بودن، مبتنی بر ارتباطات بی‌سیم بودن و فناوری شناسایی یکتا، امکان به‌کارگیری و توسعه سریع فناوری «شناسایی فرکانس‌های رادیویی» (RFID) را در سامانه‌های مراقبت پزشکی از راه دور فراهم می‌آورد. با استفاده از راهکارهای مبتنی بر RFID می‌توان مزایای زیادی ازجمله تداوم در دریافت خدمات، کاهش هزینه‌های نظارتی، ثبت دقیق سوابق و علائم، مراقبت‌های پیشگیرانه و بهبود کیفیت خدمات مراقبتی را در سامانه‌های مراقبت پزشکی از راه دور به دست آورد. در سالیان گذشته با توجه به حساسیت و اهمیت داده‌های پزشکی، پروتکل‌های احراز هویت زیادی برای به‌کارگیری در سامانه‌های مراقبت پزشکی از راه دور ارائه‌شده‌اند. در این مقاله یکی از پروتکل‌های اخیراً ارائه‌شده در این زمینه بررسی‌شده و نشان داده می‌شود که این پروتکل، یکی از نیازمندی‌های امنیتی ضروری یعنی امنیت در مقابل حمله ردیابی را تأمین نمی‌کند. در ادامه، یک پروتکل بهبودیافته ارائه‌شده و نشان داده می‌شود که پروتکل پیشنهادی، ویژگی‌های امنیتی موردنیاز را فراهم می‌کند. مقایسه پروتکل پیشنهادی با دیگر پروتکل‌های موجود ازنظر پیچیدگی محاسباتی و مخابراتی نشان می‌دهد که پروتکل پیشنهادی در مقایسه با یکی از پروتکل‌های امن مشابه ازنظر محاسباتی ۴۹ درصد و ازنظر مخابراتی ۸۵ درصد کاراتر بوده و در مقایسه با دیگر پروتکل امن مشابه ازنظر محاسباتی ۴۹۳ درصد کاراتر و ازنظر مخابراتی ۲۲ درصد غیرکاراتر است؛ که روی‌هم‌رفته، بیانگر کارایی بالاتر پروتکل پیشنهادی در مقایسه با پروتکل‌های امن مشابه است.

مشخصات مقاله

تاریخچه مقاله:

نوع مقاله: علمی پژوهشی

دریافت: ۱۴۰۴/۰۱/۰۸

بازنگری: ۱۴۰۴/۰۳/۰۸

پذیرش: ۱۴۰۴/۰۳/۲۸

ارائه آنلاین: ۱۴۰۴/۰۴/۰۷

کلید واژه‌ها:

مراقبت پزشکی از راه دور

اینترنت اشیا

RFID

امنیت

محرمانگی

حمله ردیابی

استناد: نوروزی، مهناز، پرمهر، کوثر. پروتکل احراز هویت بهبودیافته مبتنی بر *RFID* برای کاربرد در سامانه‌های مراقبت پزشکی از راه دور. پدافند الکترونیک و سایبری. (۱۴۰۴)؛ ۱۳ (۲): ۷۱-۵۷.

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.2.6.3

ناشر: دانشگاه جامع امام حسین(ع).

۱- مقدمه

با فراهم‌سازی امکان ارتباط و تبادل اطلاعات بین دستگاه‌ها و سامانه‌های مختلف، «اینترنت اشیا»[1] (IoT) توجه صنایع و حوزه‌های مختلفی را در سال‌های اخیر به خود جلب کرده است. یکی از کاربردهای مهم این فناوری نوظهور و روبه رشد در حوزه بهداشت و درمان است. سامانه‌های بهداشتی مبتنی بر اینترنت اشیا امکان بهبود خدمات بهداشتی، پیش‌بینی بیماری‌ها، مدیریت بیماران و افزایش کیفیت مراقبت‌های پزشکی را فراهم می‌سازد. با استفاده از این سامانه‌ها ارائه خدمات نظارت از راه دور به بیماران سالخورده، ناتوان یا مبتلابه بیماری‌های واگیردار ممکن خواهد بود. خدمات مراقبت از راه دور به‌ویژه در زمان وقوع همه‌گیری‌های مرگباری مانند شیوع ویروس کووید ۱۹ در سال‌های گذشته اهمیت پیدا می‌کند. در این شرایط، هرروزه افراد زیادی به‌ویژه از کادر درمان با تماس نزدیک به مبتلایان بیمار می‌شوند. محافظت بیشتر از کادر درمان در چنین همه‌گیری‌هایی ازآن‌جهت حائز اهمیت است که اولاً این افراد در تماس بیشتر با مبتلایان بوده و ثانیاً ابتلا و عدم امکان ارائه خدمت توسط آن‌ها منجر به افزایش خسارات جانی در عموم افراد جامعه خواهد شد. سامانه‌های پزشکی مراقبت از راه دور، ارائه مراقبت‌های معمول و ارزیابی منظم از راه دور را برای بیماران بدون هیچ‌گونه خطری تضمین می‌کند [۱-۳].

امنیت داده‌ها و اطلاعات کاربران در حوزه بهداشت و درمان از اهمیت بسیار زیادی برخوردار است؛ چراکه در این حوزه اطلاعات شخصی و حساسی مانند تاریخچه بیماری‌ها و درمان، داروهای مصرفی و غیره وجود داشته و افشای هر یک از این موارد می‌تواند تهدیدی جدی برای حریم خصوصی کاربران باشد. فناوری «شناسایی فرکانس‌های رادیویی»[2] (RFID) یکی از مهم‌ترین ابزارها برای رفع چالش‌های بیان‌شده در زمینه امنیت و حریم خصوصی کاربران در سامانه‌های مراقبت پزشکی از راه دور مبتنی بر اینترنت اشیا است. با استفاده از راهکارهای مبتنی بر RFID می‌توان مزایای زیادی ازجمله تداوم در دریافت خدمات، کاهش هزینه‌های نظارتی، ثبت دقیق سوابق و علائم، مراقبت‌های پیشگیرانه و بهبود کیفیت خدمات مراقبتی را در سامانه‌های مراقبت پزشکی از راه دور باهدف دسترسی برخط به خدمات مراقبت‌های پزشکی به دست آورد. همچنین امکان توسعه و به‌کارگیری سریع در امور درمانی با توجه به ویژگی‌هایی مانند غیرتماسی بودن، مبتنی بر ارتباطات بی‌سیم بودن و فناوری شناسایی یکتا از دلایل گسترش استفاده از فناوری RFID در سامانه‌های مراقبت پزشکی از راه دور هستند.

سامانه‌های RFID از ۳ بخش کلیدی تشکیل‌شده‌اند: برچسب‌ها[3]، خواننده[4]ها و سرور Backend که به‌طورمعمول خواننده و سرور تحت نام واحد خواننده - سرور در نظر گرفته می‌شود. در این سامانه‌ها، برچسب‌های RFID به اشیا قابل‌شناسایی الصاق شده؛ خواننده‌ها داده‌ها را از روی برچسب‌ها خوانده و بر روی آن‌ها می‌نویسند؛ و سرور اطلاعات حساس مرتبط با بیماران که توسط خواننده‌ها ارسال‌شده است را ذخیره می‌کند [۴]. در سامانه‌های مراقبت پزشکی از راه دور، می‌توان داده‌های پزشکی و اطلاعات بیماران را از طریق سیگنال‌های فرکانس رادیویی به‌صورت بی‌سیم منتقل کرد. بااین‌حال، این نوع انتقال می‌تواند منجر به وقوع مشکلاتی حیاتی در زمینه امنیت و حریم خصوصی شود.

اخیراً Shariq و همکاران در [۵] یک پروتکل احراز هویت مبتنی بر RFID جدید برای به‌کارگیری در سامانه‌های مراقبت پزشکی از راه دور و در شرایط وقوع همه‌گیری‌های مرگبار مانند شیوع ویروس کووید ۱۹ ارائه کرده‌اند. پروتکل ارائه‌شده توسط Shariq و همکاران از کارایی بسیار بالایی برخوردار است. بااین‌حال، در این مقاله نشان داده می‌شود که برخلاف ادعای مطرح‌شده توسط نویسندگان، این پروتکل امنیت در مقابل «حمله ردیابی»[5] برچسب‌ها را تأمین نمی‌کند. در ادامه، با اعمال تغییراتی بر روی این پروتکل، یک پروتکل بهبودیافته پیشنهاد خواهد شد. تحلیل امنیت و کارایی پروتکل پیشنهادی نشان می‌دهد که این پروتکل در مقایسه با دیگر پروتکل‌های موجود امن از کارایی بالاتری برخوردار است.

ادامه این مقاله از بخش‌های زیر تشکیل‌شده است: کارهای مرتبط پیشین در بخش ۲ مرور خواهند شد. در بخش ۳، مدل سامانه و مدل امنیت در نظر گرفته‌شده در این مقاله ارائه‌شده است. در بخش ۴ پروتکل ارائه‌شده توسط Shariq و همکاران مورد بازبینی واقع‌شده و آسیب‌پذیری آن در برابر حملات ردیابی نشان داده‌شده است. جزئیات پروتکل بهبودیافته پیشنهادی در بخش ۵ و تحلیل امنیت و کارایی آن به ترتیب در بخش‌های ۶ و ۷ ارائه‌شده است. در پایان، در بخش ۸ نتیجه‌گیری ارائه‌شده است.

۲- کارهای مرتبط

در سال‌های اخیر پژوهش‌های زیادی در زمینه به‌کارگیری روش‌های احراز هویت مبتنی بر RFID در سامانه‌های مراقبت پزشکی از راه دور صورت گرفته است [۶]. هدف اصلی پژوهش‌های صورت گرفته دسترسی امن به بیماران، حفاظت از نوزادان، ردیابی وضعیت سلامت بیماران، اطمینان از داده‌های پزشکی بیماران، امنیت دارویی، مدیریت سوابق بیماران، مدیریت تجهیزات و ردیابی مکان دارایی‌های پزشکی، امنیت اطلاعات حساس بیماران و ... است.

در سال ۲۰۱۳، یک پروتکل احراز هویت مبتنی بر RFID سبک‌وزن کارآمد برای افزایش امنیت دارویی بیماران در

[1] Internet of Things
[2] Radio Frequency Identification
[3] Tag
[4] Reader
[5] Tracking attack

مراقبت‌های پزشکی ارائه شد [۷]. این پروتکل که در آن با توجه به محدودیت‌های محاسباتی و مخابراتی برچسب‌های RFID تنها از «مولدهای اعداد شبه تصادفی»[1]، عملگر یای انحصاری (XOR) و «توابع چکیده ساز»[2] استفاده‌شده است، خطاهای دارویی که می‌تواند صدمات جبران‌ناپذیری به بیماران وارد کند را کاهش می‌دهد. در [۸]، یک سامانه احراز هویت مبتنی بر RFID دیگر باهدف تأمین امنیت در برابر حملاتی مانند ردیابی، «جعل هویت»[3] و «غیر همگام‌سازی»[4] برچسب‌ها ارائه شد. این پروتکل از روش‌های «رمزنگاری مبتنی بر خم‌های بیضوی»[5] (ECC) استفاده می‌کند. بااین‌حال، برخلاف ادعای نویسندگان، در [۹] نشان داده‌شده است که این پروتکل «امنیت پیشرو»[6] را تأمین نکرده و در برابر حملات جعل هویت ناامن است. در [۱۰]، با استفاده از ECC یک پروتکل احراز هویت مبتنی بر RFID دیگر برای به‌کارگیری در سامانه‌های مراقبت پزشکی ارائه شد. بااین‌حال، در این پروتکل متخاصمین قادر به استخراج مقادیر مخفی برچسب‌ها از پیام‌های ارتباطی و در ادامه جعل هویت آن‌ها هستند [۱۱]. علاوه برنشان دادن نقطه‌ضعف امنیتی پروتکل [۱۰]، در [۱۱] یک پروتکل احراز هویت بهبودیافته نیز ارائه‌شده است که فراش[7] و همکاران در سال ۲۰۱۶ نشان دادند این پروتکل امنیت پیشرو را تأمین نمی‌کند [۱۲]. فراش و همکاران همچنین یک پروتکل بهبودیافته جدید با استفاده از ECC ارائه کرده و نشان دادند پروتکل پیشنهادی آن‌ها ویژگی‌های امنیتی موردنیاز را دارد. در [۱۳]، نویسندگان با استفاده از توابع چکیده ساز و عملگر XOR یک پروتکل احراز هویت مبتنی بر RFID جدید برای محیط‌های پزشکی ارائه کردند. بااین‌حال، در [۱۴] نشان داده شد که این پروتکل «احراز هویت دوسویه»[8] را تأمین نمی‌کند. در [۱۵]، نویسندگان همچنین با اعمال تغییراتی مانند در نظر گرفتن یک کانال امن بر روی پروتکل تحلیل‌شده، یک پروتکل بهبودیافته ارائه دادند. در [۱۵]، نویسندگان از ECC استفاده کرده و یک پروتکل احراز هویت مبتنی بر RFID دیگر ارائه کردند که در [۱۶] نشان داده شد این پروتکل در برابر حمله جعل هویت ناامن است. در [۱۷]، نویسندگان با حذف نیاز به کانال امن، پروتکل ارائه‌شده در [۱۵] را ارتقا دادند. بااین‌حال، این پروتکل از کارایی کمتری برخوردار است. در [۱۸] نشان داده شد که پروتکل احراز هویت مبتنی بر RFID ارائه‌شده در [۱۹] در برابر حملات منع خدمت[9] (DoS)، شبیه‌سازی[10] و ردیابی ناامن است.

در [۲۰]، نویسندگان نشان دادند که پروتکل احراز هویت مبتنی بر RFID ارائه‌شده در [۲۱] در مقابل حملات کشف کلیدهای مخفی، جعل هویت برچسب و ردیابی نا مقاوم بوده و یک پروتکل بهبودیافته ارائه کردند. بااین‌حال، در [۲۲] نشان داده شد که پروتکل بهبودیافته نیز در مقابل حملات کشف کلیدهای مخفی، و ردیابی نا مقاوم است.

در [۲۳] از نسخه مبتنی بر خم‌های بیضوی پروتکل توافق کلید دیفی - هلمان استفاده و یک پروتکل جدید ارائه شد. بااین‌حال، در [۲۴] نشان داده شد که این پروتکل در برابر حملات جعل هویت و غیرهم گام سازی ناامن است. در [۲۵] با استفاده از ECC، یک پروتکل احراز هویت مبتنی بر RFID دیگر ارائه شد. نویسندگان [۲۵] همچنین نشان دادند که پروتکل ارائه‌شده در برابر حملات امنیتی شناخته‌شده مانند جعل هویت، بازپخش[11]، مردی در میانه[12] و ... امن است. در [۲۶]، یک پروتکل احراز هویت مبتنی بر RFID جدید باهدف به‌کارگیری در سامانه‌های مراقبت پزشکی برای افزایش امنیت دارویی بیماران ارائه شد. این پروتکل از سامانه رمزگذاری El-Gamal برای حفظ محرمانگی استفاده می‌کند. نویسندگان در [۲۶] همچنین نشان دادند که پروتکل ارائه‌شده در برابر حملات شناخته‌شده‌ای مانند حمله DoS، حمله بازپخش، حمله ردیابی، حمله غیر همگام‌سازی و حمله جعل هویت امن است.

چن و همکاران [۲۷] در سال ۲۰۲۰ نشان دادند که پروتکل‌های احراز هویت مبتنی بر RFID ارائه‌شده در [۲۸] و [۲۹]، در برابر حملات جعل هویت و ردیابی آسیب‌پذیر بوده و یک پروتکل بهبودیافته پیشنهاد کردند. یک پروتکل احراز هویت مبتنی بر RFID بسیار کارا در [۳۰] و توسط Shariq و همکاران ارائه شد. در [۳۱] با استفاده از ECC و توابع کپی ناپذیر فیزیکی[13]، یک پروتکل احراز هویت مبتنی بر RFID دیگر برای کنترل دسترسی در سامانه‌های مراقبت پزشکی ارائه شد. در [۳۲] نویسندگان یک پروتکل احراز هویت جدید مبتنی بر RFID ارائه کرده و نشان دادند پروتکل پیشنهادی در برابر حملات شناخته‌شده امن است.

۳- مدل سامانه و امنیت

در این بخش مدل‌های سامانه و تخاصم و همچنین انواع حملات به پروتکل‌های احراز هویت مبتنی بر RFID مرور می‌شوند [۱].

۳-۱- مدل سامانه

همان‌طور که در شکل (۱) نشان داده‌شده است، در مدل در نظر گرفته‌شده در [۱]، مجموعه‌ای از برچسب‌های RFID، خواننده‌ها و یک سرور پزشکی قابل‌اعتماد وجود دارد. در این مدل، بیماران و تجهیزات پزشکی مجهز به برچسب هستند. این برچسب‌ها

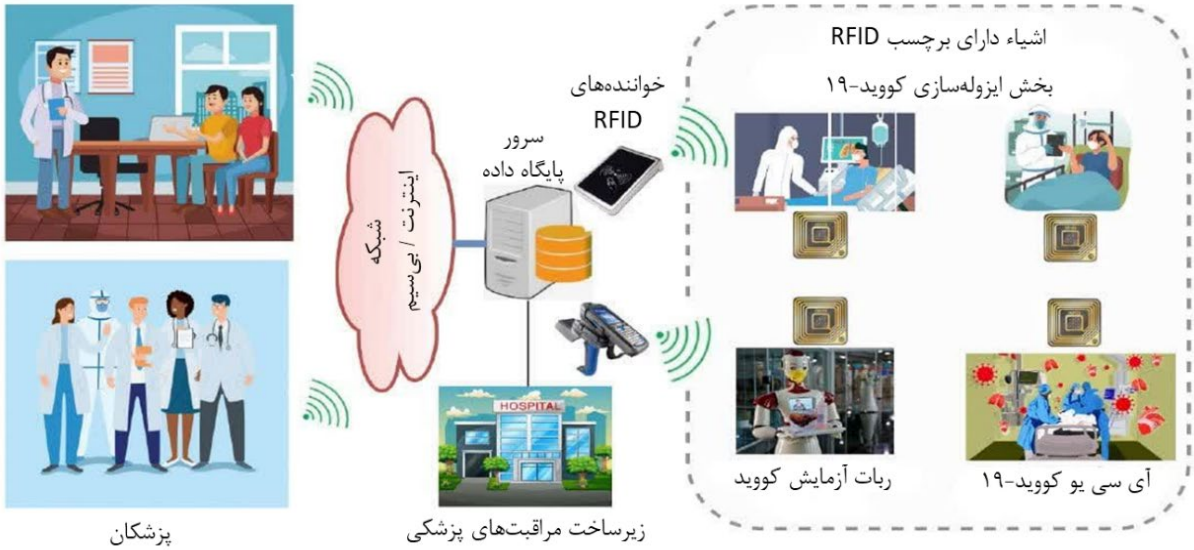
[1] Psuedo-Random Number Generator
[2] Hash Function
[3] Impersonation Attack
[4] De-Synchronization Attack
[5] Elliptic-Curve Cryptography
[6] Forward Secrecy
[7] Farash
[8] Mutual Authentication
[9] Denial of Service
[10] Simulation
[11] Replay Attack
[12] Man in the Middle Attack
[13] *Physically Unclonable Function (PUF)*

اطلاعات و علائم بی‌درنگ زیادی ازجمله نتایج سی-تی اسکن، رادیوگرافی قفسه سینه، نتیجه آزمایش PCR، سطح اکسیژن، درجه حرارت بدن و سایر علائم و گزارش‌های تشخیصی مرتبط با بیماران را جمع‌آوری و ذخیره می‌کنند. خواننده، اطلاعات برچسب‌های متصل به بیماران و تجهیزات پزشکی را از طریق یک کانال ارتباطی ناامن یا عمومی خوانده و برای ذخیره و پردازش بیشتر و درنهایت اعمال مراقبت‌های پزشکی از طریق یک کانال ارتباطی امن یا اختصاصی به سرور ارسال می‌کند.

۳-۲- مدل تخاصم

با توجه به اهمیت و میزان حساسیت اطلاعات پزشکی افراد، در سامانه‌های مراقبت پزشکی از راه دور باید تا حد امکان، مدل تخاصم قوی‌تری در نظر گرفت. بدین منظور در مدل ارائه‌شده در [۱] فرض شده که متخاصم قادر به انجام موارد زیر باشد:

- کنترل کامل بر کانال‌های ارتباطی
- شنود پیام‌های مخابره شده بین برچسب‌ها و خواننده‌ها
- استراق سمع، تغییر، حذف و حتی جعل پیام‌های ردوبدل شده در کانال‌های ارتباطی
- استخراج اطلاعات حساس با دریافت پیام‌ها از طریق کانال‌های ارتباطی ناامن
- افشای اطلاعات محرمانه و مهم جعل هویت برچسب‌ها یا خواننده‌های قانونی و مشروع.



شکل (۱): معماری سامانه مراقبت پزشکی از راه دور مبتنی بر اینترنت اشیاء [۱]

۳-۳- انواع حملات به پروتکل‌های احراز هویت مبتنی بر RFID

با توجه به استفاده از کانال ارتباطی ناامن و بی‌سیم مابین برچسب و خواننده، سامانه‌های احراز هویت مبتنی بر RFID ممکن است در مقابل حملات متعددی ناامن باشند. با توجه به ادبیات موضوع، مهم‌ترین حملات در نظر گرفته در این زمینه عبارت‌اند از:

- حمله استراق سمع[1]: در این حمله، مهاجم مابین برچسب و خواننده قرارگرفته و با شنود مکالمات، داده‌های احراز هویت را به دست می‌آورد. در این نوع حمله، مهاجم یک خواننده RFID غیرمجاز در نظر گرفته می‌شود.
- حمله بازپخش: این حمله نیز بر اساس استراق سمع است. در این حمله، مهاجم بخشی از پیام‌های مخابره شده را ضبط کرده و پس از گذشت مدت‌زمانی، آن را برای سرقت اطلاعات یا دسترسی به دریافت‌کننده دوباره ارسال می‌کند.
- حمله مردی در میانه: در این حمله نیز مهاجم بین برچسب و خواننده قرارگرفته و پس از شنود پیام‌های مخابره شده، آن‌ها را دست‌کاری کرده و پیام دست‌کاری شده را به برچسب یا خواننده ارسال می‌کند.
- حمله شبیه‌سازی: هدف این نوع حمله، کپی هویت برچسب است. در این نوع حمله، مهاجم ابتدا با جعل هویت خواننده، درخواستی را به برچسب ارسال می‌کند و پاسخ را دریافت می‌کند. در ادامه، وقتی‌که خواننده واقعی درخواست احراز هویت را به برچسب ارسال می‌کند، مهاجم پاسخی که قبلاً از برچسب دریافت کرده را برای خواننده ارسال نموده و خود را به‌عنوان برچسب قانونی معرفی می‌کند.
- حمله ردیابی: این حمله باهدف ردیابی پاسخ دریافت شده به یک برچسب خاص انجام می‌شود. برای امنیت در برابر این حمله، مهاجم نباید با استفاده از پیام‌های دریافت شده از یک برچسب در یک‌زمان، قادر به تمایز پیام‌هایی ردوبدل

[1] Eavesdropping Attack

شده بین این برچسب یا برچسب دیگری با خواننده باشد.

- حمله منع خدمت (DoS): این حمله می‌تواند بر ارتباط بین برچسب‌ها و خواننده‌های قانونی تأثیرگذار باشد. در این حمله، مهاجم تعداد زیادی پیام را به‌صورت هم‌زمان و در قالب پاسخ به درخواست‌های احراز هویت به سرور ارسال کرده و سامانه را غیرقابل‌دسترس می‌نماید.

۴- مرور و تحلیل پروتکل ارائه‌شده توسط Shariq و همکاران

۴-۱- مرور پروتکل ارائه‌شده توسط Shariq و همکاران

در پروتکل ارائه‌شده در [۱] برای مراقبت از راه دور بیماران در همه‌گیری کرونا، چندین برچسب برای ثبت و ارسال علائم پزشکی به بیماران متصل شده و اطلاعات دریافتی از بیماران را از طریق یک خواننده در یک سرور پشتیبان ذخیره کرده و در اختیار کادر درمان قرار می‌دهد. امنیت این پروتکل مبتنی بر مسائل سخت دیفی - هلمن و لگاریتم گسسته بوده، و در آن از توابع چکیده ساز رمزنگاشتی استفاده‌شده است. این پروتکل از ۲ مرحله تشکیل‌شده که جزئیات هر یک از این مراحل در ادامه ارائه‌شده است.

مرحله راه‌اندازی

- عدد اول بزرگ p با طول ۱۰۲۴ بیت و عدد اول q با طول ۱۶۰ بیت به‌طوری‌که $q|p-1$ انتخاب می‌شود.
- مولد g $(1 < g < p-1)$ به‌عنوان مولد زیرگروهی از Z_p^* با مرتبه q انتخاب می‌شود.
- عدد تصادفی a $(0 < a < q)$ به‌عنوان کلید مخفی سرور انتخاب می‌شود.
- مقدار $v = g^{-a} \ (mod\ p)$ به‌عنوان کلید عمومی سرور محاسبه می‌شود.
- به ازای هر برچسب با شناسه ID_i (که طول شناسه برابر با ۱۶۰ بیت است):
  - عدد تصادفی a_i $(0 < a_i < q)$ به‌عنوان مقدار مشترک برچسب و خواننده انتخاب می‌شود. این مقدار، در واحد خواننده - سرور به‌صورت رمزگذاری شده ذخیره می‌شود.
  - مقادیر (p, q, v, ID_i, a_i) در حافظه برچسب ذخیره می‌شود.
  - مقادیر (ID_i, a_i) در پایگاه داده سرور ذخیره می‌شود.

مرحله احراز هویت

- واحد خواننده - سرور:
  - مقدار تصادفی $k_1 \in Z_q^*$ را انتخاب کرده، و به برچسب T_i ارسال می‌کند.
- برچسب T_i با دریافت k_1:
  - مقادیر تصادفی $r_1, r_2 \in Z_q^*$ را انتخاب می‌کند.
  - مقادیر زیر را محاسبه می‌کند:

$$x_1 = g^{r_1} \ (mod\ p)\ ,\ x_2 = r_2 \cdot v^{-r_1} \ (mod\ p),$$
$$e = h(r_2||x_2||x_1)\ ,\ y = r_2 + a_i \cdot e \ (mod\ q),$$
$$Auth_i = ID_i \oplus h(r_2, k_1, e, y)$$

  - سه‌تایی $(x_1, x_2, Auth_i)$ را به خواننده -سرور ارسال می‌کند.
- واحد خواننده - سرور با دریافت $(x_1, x_2, Auth_i)$،
  - مقادیر $S_1 = {x_1}^a \ (mod\ p)$، $S_2 = S_1 \ (mod\ p)$، ${r_2}' = x_2 \cdot {S_2}^{-1} \ (mod\ p)$، $e' = h({r_2}'||x_2||x_1)$ و $y' = {r_2}' + a_i \cdot e' (mod\ q)$ را محاسبه می‌کند.
  - شناسه ${ID_i}'$ را با استفاده از رابطه $ID_i' = Auth_i \oplus h({r_2}', k_1, e', y')$ استخراج و در پایگاه داده جستجو می‌کند. در صورت وجود ${ID_i}'$ در پایگاه داده، برچسب احراز هویت شده و معتبر در نظر گرفته‌شده و در غیر این صورت نامعتبر.
  - مقدار $k_2 = h(ID_i', r_2', k_1, e', y', Auth_i)$ را محاسبه و به برچسب T_i ارسال می‌کند.
- برچسب T_i با دریافت k_2:
  - مقدار ${k_2}' = h(ID_i, r_2, k_1, e, y, Auth_i)$ را محاسبه می‌کند. در صورت برقراری رابطه $k_2' = k_2$، واحد خواننده - سرور احراز هویت شده و معتبر در نظر گرفته‌شده و در غیر این صورت نامعتبر.

۴-۲- تحلیل پروتکل ارائه‌شده توسط Shariq و همکاران

در مرحله احراز هویت پروتکل ارائه‌شده توسط Shariq و همکاران [۱]، مقدار مخفی مشترک بین واحد خواننده – سرور و برچسب (یعنی a_i) بدون محاسبه قبلی (از روی پیام‌های دریافت شده از برچسب) در محاسبه مقدار y استفاده‌شده است؛ به‌عبارت‌دیگر، در این پروتکل فرض شده که واحد خواننده – سرور در آغاز فرایند احراز هویت از مقدار مخفی مشترک با برچسبی که در حال احراز هویت آن است، مطلع بوده و آن برچسب را می‌شناسد. چنین فرضی از اساس اشتباه است؛ چراکه تعداد برچسب‌های موجود در سامانه ممکن است بسیار زیاد بوده و واحد خواننده – سرور نمی‌تواند قبل از انجام فرایند احراز هویت تشخیص دهد که با کدام‌یک از برچسب‌ها در ارتباط است. برای حل این مشکل می‌توان فرض نمود که برچسب باید در هر دور احراز هویت، مقدار مخفی مشترک یعنی a_i را به‌عنوان بخشی از پیام به واحد خواننده - سرور ارسال نماید؛ اما در این صورت، این پروتکل

به‌راحتی قابل‌ردیابی و درنتیجه در مقابل حمله ردیابی ناامن خواهد بود. به عبارتی با استفاده از پیام‌های دریافت شده از یک برچسب در یک‌زمان، به‌سادگی می‌توان پیام‌های ردوبدل شده بین این برچسب را از برچسب‌های دیگر تمایز داد.

۵- پروتکل بهبودیافته پیشنهادی

در این بخش، با اعمال تغییراتی بر روی پروتکل پیشنهادشده توسط Shariq و همکاران، نقطه‌ضعف بیان‌شده در مورد این پروتکل برطرف خواهد شد. در پروتکل پیشنهادی برای رفع مشکل گزارش‌شده از یک پارامتر جدید x_3 برای انتقال مقدار مخفی a_i متناظر با برچسب به‌صورت رمزگذاری شده به واحد خواننده - سرور استفاده‌شده است. با استفاده از این راه‌کار، واحد خواننده - سرور قادر به انجام محاسبات موردنیاز بوده و همچنین نیازی به ارسال خام مقدار a_i و آسیب‌پذیری در مقابل حمله ردیابی نیست. جزئیات پروتکل بهبودیافته پیشنهادی که از دو مرحله تشکیل‌شده به شرح زیر است.

۵-۱- مرحله راه‌اندازی

- عدد اول بزرگ p با طول ۱۰۲۴ بیت و عدد اول q با طول ۱۶۰ بیت به‌طوری‌که $q|p-1$ انتخاب می‌شود.
- تابع چکیده ساز $h:\{0,1\}^* \rightarrow Z_q$ انتخاب می‌شود.
- مولد g $(1 < g < p-1)$ به‌عنوان مولد زیرگروهی از Z_p^* با مرتبه q انتخاب می‌شود.
- عدد تصادفی a $(0 < a < q)$ به‌عنوان کلید مخفی واحد خواننده - سرور انتخاب می‌شود.
- مقدار $v = g^{-a} \ (mod\ p)$ به‌عنوان کلید عمومی سرور محاسبه می‌شود.
- مقادیر p, q, g, a, v در سرور ذخیره می‌شود.
- به ازای هر برچسب با شناسه ID_i (که طول شناسه برابر با ۱۶۰ بیت است):
  - عدد تصادفی a_i $(0 < a_i < q)$ به‌عنوان مقدار مخفی برچسب انتخاب می‌شود.
  - مقادیر (p, q, g, v, ID_i, a_i) در حافظه برچسب ذخیره می‌شود.
  - مقادیر (ID_i, a_i) در پایگاه داده سرور ذخیره می‌شود.

۵-۲- مرحله احراز هویت

جزئیات این فاز که در شکل (۲) ارائه‌شده، به شرح زیر است:

- واحد خواننده - سرور:
  - مقدار تصادفی $k_1 \in Z_q^*$ را انتخاب کرده، و به برچسب T_i ارسال می‌کند.
- برچسب T_i با دریافت k_1:
  - مقادیر تصادفی $r_1, r_2 \in Z_q^*$ را انتخاب می‌کند.

واحد خواننده - سرور R/S $\{p, q, g, a, DB = \{ID_j, a_j\}_{j=1,..,n}\}$		برچسب T_i $\{p, q, g, v, ID_i, a_i\}$
$k_1 \leftarrow_R Z_q^*$		
	$k_1 \rightarrow$	
		$r_1, r_2 \leftarrow_R Z_q^*$ $x_1 = g^{r_1} \ (mod\ p)$ $x_2 = r_2 \cdot [v^{-r_1} \ (mod\ p) \ (mod\ q)] \ (mod\ q)$ $x_3 = [a_i \cdot h(v^{-r_1} (mod\ p) (mod\ q))] (mod\ q)$ $e = h(r_2 \| x_3 \| x_2 \| x_1)$ $y = r_2 + a_i \cdot e \ (mod\ q)$ $Auth_i = ID_i \oplus h(r_2, k_1, e, y)$
	$\leftarrow (x_1, x_2, x_3, Auth_i)$	
$S = [{x_1}^a \ (mod\ p)\ ] \ (mod\ q)$ $r_2' = x_2 \cdot S^{-1} \ (mod\ q)$ $a_i' = x_3 \cdot \big(h(S)\big)^{-1} (mod\ q)$ $e' = h(r_2' \| x_3 \| x_2 \| x_1)$ $y' = r_2' + a_i' \cdot e' (mod\ q)$ $ID_i' = Auth_i \oplus h(r_2', k_1, e', y')$ $ID_i \leftarrow DB(a_i')$ $\{\times, \checkmark\} \leftarrow ID_i' =^? ID_i$ $k_2 = h(ID_i', r_2', k_1, e', y', Auth_i)$		
	$k_2 \rightarrow$	
		$k_2' = h(ID_i, r_2, k_1, e, y, Auth_i)$ $\{\times, \checkmark\} \leftarrow k_2' =^? k_2$

شکل (۲): مرحله احراز هویت پروتکل پیشنهادی. $Z_q^* \leftarrow_R Z_q^*$ به معنای انتخاب تصادفی از Z_q^* و $\leftarrow \{\text{✗}, \text{✓}\}$ به معنای پذیرش یا عدم پذیرش است

- مقادیر زیر را محاسبه می‌کند:

$x_1 = g^{r_1}\ (mod\ p)$
$x_2 = r_2 \cdot [v^{-r_1}\ (mod\ p)\ (mod\ q)]\ (mod\ q)$
$x_3 = [a_i \cdot h(v^{-r_1}\ (mod\ q))](mod\ q)$
$e = h(r_2||x_3||x_2||x_1)$
$y = r_2 + a_i \cdot e\ (mod\ q)$
$Auth_i = ID_i \oplus h(r_2, k_1, e, y)$

- چهارتایی $(x_1, x_2, x_3, Auth_i)$ را به خواننده - سرور ارسال می‌کند.

▪ واحد خواننده - سرور با دریافت چهارتایی $(x_1, x_2, x_3, Auth_i)$،

- مقادیر زیر را محاسبه می‌کند:

$S = [{x_1}^a\ (mod\ p)\ ]\ (mod\ q)$
$r_2' = x_2 \cdot S^{-1}\ (mod\ q)$
$a_i' = x_3 \cdot \big(h(S)\big)^{-1}(mod\ q)$
$e' = h(r_2'||x_3||x_2||x_1)$
$y' = r_2' + a_i' \cdot e'(mod\ q)$

- مقدار a_i' را در پایگاه داده جستجو کرده و شناسه متناظر یعنی ID_i را می‌یابد.
- شناسه ID_i' را با استفاده از رابطه $ID_i' = Auth_i \oplus h(r_2', k_1, e', y')$ استخراج کرده و برقراری رابطه $ID_i' = ID_i$ را بررسی می‌کند. در صورت برقراری رابطه، برچسب احراز هویت شده و معتبر در نظر گرفته‌شده و در غیر این صورت نامعتبر.
- مقدار $k_2 = h(ID_i', r_2', k_1, e', y', Auth_i)$ را محاسبه و به برچسب T_i ارسال می‌کند.

▪ برچسب T_i با دریافت k_2:

- مقدار $k_2' = h(ID_i, r_2, k_1, e, y, Auth_i)$ را محاسبه می‌کند. در صورت برقراری رابطه $k_2' = k_2$، واحد خواننده - سرور احراز هویت شده و معتبر در نظر گرفته‌شده و در غیر این صورت نامعتبر.

۴- تحلیل امنیت پروتکل بهبودیافته پیشنهادی

در این بخش نشان می‌دهیم که پروتکل بهبودیافته پیشنهادی ویژگی‌های امنیتی موردنیاز را تأمین کرده و در برابر انواع حملات شناخته‌شده امن است.

قضیه ۱. پروتکل پیشنهادی ویژگی محرمانگی را تأمین می‌کند.

اثبات. در پروتکل پیشنهادی، شناسه و مقدار مخفی i-امین برچسب در پیام‌های $Auth_i = ID_i \oplus h(r_2, k_1, e, y)$ و $x_3 = [a_i \cdot h(v^{-r_1}\ (mod\ q))](mod\ q)$ مخفی‌شده است. متخاصم قادر به دستیابی به پیام‌های ارسالی $\{k_1\}$، $\{x_1, x_2, x_3, Auth_i\}$، و $\{k_2\}$ و اطلاعات و مقادیر عمومی $\{p, q, g, v\}$ است. بااین‌حال، با توجه فرض سختی مسئله دیفی – هلمن قادر به دستیابی به مقدار $S = {x_1}^a\ (mod\ p)$ نبوده و درنتیجه نمی‌تواند به شناسه و مقدار مخفی متناظر با برچسب یابد. بنابراین، پروتکل پیشنهادی ویژگی محرمانگی برچسب را تأمین می‌کند.

قضیه ۲. پروتکل پیشنهادی ویژگی احراز هویت دوسویه را دارا است.

اثبات. در پروتکل پیشنهادی، بدون اطلاع از شناسه ID_i و مقدار مخفی a_i، یک متخاصم قادر به ایجاد پیام معتبر $(x_1, x_2, Auth_i)$ نیست. بااین‌حال، خواننده - سرور می‌تواند با محاسبه مقدار $S = {x_1}^a$ مقادیر r_2 و a_i را محاسبه و با استفاده از آن‌ها شناسه ID_i را استخراج کرده و درنهایت هویت برچسب را احراز نماید. در سمت مقابل، با توجه به فرض سختی مسئله دیفی - هلمان محاسباتی، واحد خواننده - سرور تنها موجودیتی است که قادر است مقادیر S، r_2، a_i، e، y، و $Auth_i$ را محاسبه کرده و با استفاده از آن‌ها مقدار k_2 معتبر را ایجاد و به برچسب بازگرداند. درنتیجه، پروتکل پیشنهادی تأمین‌کننده احراز هویت واحد خواننده - سرور به برچسب است. با توجه به اثبات هر دو سمت، پروتکل پیشنهادی تأمین‌کننده احراز هویت دوسویه است.

قضیه ۳. پروتکل پیشنهادی امنیت پیش رو را فراهم می‌کند.

اثبات. در پروتکل پیشنهادی، متخاصم حتی در صورت دسترسی به اطلاعات محرمانه (شناسه و مقدار مخفی) یک برچسب نیز قادر به ردیابی پیام‌های قبلاً ارسال‌شده نخواهد بود. این مهم بدین دلیل است که پیام‌های ارسالی به واحد خواننده - سرور به‌نوعی با کلید سرور رمزگذاری شده و متخاصم به آن دسترسی ندارد. همچنین، در مقایسه با پروتکل پیشنهادشده در [۱]، در پروتکل پیشنهادی در این مقاله تنها مؤلفه x_3 به مقادیر ارسالی اضافه‌شده است که برابر است با حاصل‌ضرب a_i در یک خروجی از تابع چکیده ساز یا به عبارتی حاصل‌ضرب a_i در یک مقدار شبه تصادفی. با توجه به این مسئله، مقدار جدید اضافه‌شده نیز قابلیت اضافه‌ای در اختیار متخاصم قرار نداده و پروتکل پیشنهادی امنیت پیش رو را تأمین خواهد کرد.

قضیه ۴. پروتکل پیشنهادی در برابر حمله جعل هویت امن است.

اثبات. فرض کنید یک متخاصم علیه پروتکل پیشنهادی وجود داشته باشد که باهدف جعل هویت یک برچسب نزد واحد خواننده - سرور یک نشست را شنود کند. متخاصم پیام k_1 را دریافت کرده و سعی می‌کند پیام‌های معتبر $(x_1, x_2, x_3, Auth_i)$ را تولید کند. بااین‌حال، ازآنجاکه متخاصم به شناسه و مقدار مخفی متناظر با برچسب، و یا به مقادیر تصادفی استفاده‌شده توسط برچسب در نشست شنود شده دسترسی ندارد، قادر به تولید پیام معتبر و درنتیجه جعل هویت برچسب نیست.

قضیه ۵. پروتکل پیشنهادی در برابر حمله بازپخش امن است.

اثبات. با توجه به استفاده از یک مقدار تصادفی جدید k_1 در هر نشست توسط واحد خواننده - سرور و استفاده از این مقدار در پاسخ ارسالی از سمت برچسب در قالب $Auth_i = ID_i \oplus h(r_2, k_1, e, y)$، ارسال پیام‌های مربوط به نشست‌های پیشین به واحد خواننده - سرور، به‌راحتی از سوی این واحد قابل‌شناسایی است. از سوی دیگر، پیام‌های ارسالی از سوی برچسب در هر نشست نیز بر اساس مقادیر تصادفی جدید r_1, r_2 انتخاب‌شده در آن نشست است که مقدار مخفی r_2 در پاسخ ارسالی از سمت واحد خواننده - سرور به برچسب یعنی $k_2 = h(ID_i', r_2', k_1, e', y', Auth_i)$ جانمایی شده است. با توجه به این مهم، برچسب نیز به‌راحتی قادر به تشخیص پیام‌های بازپخش شده است. درنتیجه پروتکل پیشنهادی در برابر حمله بازپخش امن است.

قضیه ۶. پروتکل پیشنهادی در برابر حمله منع خدمت امن است.

اثبات. در دسته‌ای از پروتکل‌های احراز هویت مبتنی بر *RFID* که در آن‌ها لازم است مقادیر مخفی برچسب‌ها پس از هر دور احراز هویت به‌روزرسانی می‌شود. در این دسته از پروتکل‌ها، متخاصم می‌تواند با قرار گرفتن مابین برچسب و واحد خواننده - سرور هم‌زمانی را از بین برده و برچسب را از خدمت‌دهی خارج می‌کند. بااین‌حال، در دسته دوم پروتکل‌های احراز هویت مبتنی بر *RFID* که شامل پروتکل پیشنهادی است، مقادیر مخفی (شناسه و مقدار مخفی متناظر با برچسب در پروتکل پیشنهادی) توسط متخاصم قابل‌مشاهده نیست درنتیجه نیازی به به‌روزرسانی مقادیر نیست. با توجه به این مسئله، حتی در صورت مسدودسازی برخی پیام‌ها، با توجه به عدم نیاز به همگام‌سازی، برچسب در پروتکل پیشنهادی از خدمت‌دهی خارج نخواهد شد؛ لذا پروتکل پیشنهادی در برابر حمله منع خدمت امن است.

قضیه ۷. پروتکل پیشنهادی در برابر حمله ردیابی امن است.

اثبات. پیام‌های مخابراتی در پروتکل پیشنهادی از ۳ قسمت تشکیل‌شده‌اند. در ابتدا واحد خواننده - سرور یک مقدار تصادفی k_1 را به برچسب ارسال می‌کند. با توجه به تصادفی بودن، این پیام هیچ‌گونه استفاده‌ای در ردیابی ندارد. در ادامه برچسب، پیام چهارتایی $(x_1, x_2, x_3, Auth_i)$ را به سرور ارسال می‌کند که در هر چهار مؤلفه، از مقادیر تصادفی جدید و انتخاب‌شده در نشست احراز هویت فعلی استفاده‌شده است. با توجه به این مسئله، چهارتایی $(x_1, x_2, x_3, Auth_i)$ نیز هیچ‌گونه قابلیت ردیابی در اختیار مهاجم قرار نمی‌دهد. در خاتمه واحد خواننده - سرور مقدار k_2 را به برچسب بازمی‌گرداند که حاصل اعمال یک تابع چکیده ساز بر روی مجموعه‌ای از مقادیر ازجمله مقادیر تصادفی انتخاب‌شده در نشست احراز هویت جاری توسط برچسب و واحد خواننده - سرور است. با توجه به خواص توابع چکیده ساز رمزنگاشتی، این مقدار نیز هیچ قابلیتی در اختیار متخاصم قرار نمی‌دهد. با توجه به این توضیحات، پروتکل پیشنهادی در برابر حمله ردیابی امن است. لازم به بیان است که ناامنی پروتکل ارائه‌شده در [۱] در مقابل حمله ردیابی بدین‌جهت بود که همان‌طور که در بخش ۴ نیز بیان شد، در آن پروتکل برای عملکرد صحیح مقدار مخفی a_i باید در هر دور احراز هویت توسط برچسب ارسال می‌گردید. در پروتکل پیشنهادی با استفاده از مؤلفه x_3 این مسئله حل‌شده است.

قضیه ۸. پروتکل پیشنهادی در برابر حمله مردی در میانه امن است.

اثبات. در پروتکل پیشنهادی، مهاجم می‌تواند مابین برچسب و واحد خواننده - سرور قرار گیرد. بااین‌حال تنها قادر به ارسال k_1 از طرف واحد خواننده - سرور به برچسب است. با توجه به استفاده از مقدار مخفی و شناسه برچسب، مهاجم امکان تولید پیام به‌جای برچسب را ندارد. علاوه‌براین، با توجه به استفاده از مقدار تصادفی k_1 در قالب بخشی از ورودی یک تابع چکیده ساز برای تولید پیام‌های ارسالی از سمت برچسب به واحد خواننده - سرور، مهاجم قادر به تغییر پیام‌های دریافت شده از سوی برچسب، با جا زدن خود در نقش واحد خواننده - سرور و ارسال آن‌ها در پاسخ به درخواست احراز هویت از سوی واحد خواننده - سرور نیست. آخرین قسمت از پیام‌های ارسالی در پروتکل پیشنهادی از مقدار k_2 تشکیل‌شده است که با توجه به وابستگی آن به دیگر پیام‌ها و مقادیر مخفی برچسب و واحد خواننده - سرور، امکان تولید آن از سوی متخاصم و یا تغییر پیام دریافتی از یک برچسب و ارسال آن در پاسخ به یک درخواست جدید از واحد خواننده - سرور وجود ندارد. با توجه به این توضیحات، پروتکل پیشنهادی در برابر حمله مردی در میانه امن است.

۷- تحلیل کارایی و مقایسه پروتکل بهبودیافته پیشنهادی با پروتکل‌های مرتبط

در این بخش ابتدا پروتکل پیشنهادی را با پروتکل‌های مرتبط ازنظر ویژگی‌های امنیتی و سپس ازنظر پیچیدگی محاسباتی مورد مقایسه قرار می‌دهیم.

۷-۱- مقایسه ویژگی‌های امنیتی

مقایسه امنیتی پروتکل پیشنهادی و برخی پروتکل‌های احراز هویت مبتنی بر RFID مرتبط در جدول (۱) ارائه‌شده است. مقایسات صورت گرفته با توجه به ویژگی‌ها امنیتی احراز هویت دوسویه، امنیت پیش رو، امنیت در برابر حمله جعل هویت، امنیت در برابر حمله بازپخش، امنیت در برابر حمله منع خدمت، امنیت در برابر حمله ردیابی، و امنیت در برابر حمله مردی در میانه صورت گرفته است. همان‌طور که از نتایج این جدول می‌توان مشاهده کرد پروتکل پیشنهادی در کنار پروتکل‌های

ارائه‌شده در [۱۲] و [۲۶] تنها پروتکل‌هایی هستند که تمام ویژگی‌های امنیتی موردنیاز را تأمین می‌کنند. دیگر پروتکل‌های موجود مرتبط همان‌طور که این جدول نشان می‌دهد، حداقل یکی از ویژگی‌های موردنیاز را فراهم نکرده (مانند پروتکل‌های ارائه‌شده در [۱] و [۹] که به ترتیب امنیت در برابر حمله ردیابی و امنیت پیش رو را تأمین نمی‌کنند) یا جزئیاتی در مورد تأمین یا عدم تأمین برخی از این ویژگی‌ها توسط این پروتکل‌ها مشخص نیست (مانند پروتکل ارائه‌شده در [۲۳] که امنیت در برابر حمله منع خدمت در مورد این پروتکل بررسی نشده است).

جدول (۱): مقایسه پروتکل پیشنهادی با پروتکل‌های مرتبط با توجه به معیارهای امنیتی: SF1: محرمانگی، SF2: احراز هویت دوسویه، SF3: امنیت پیش رو، SF4: امنیت در برابر حمله جعل هویت، SF5: امنیت در برابر حمله بازپخش، SF6: امنیت در برابر حمله منع خدمت، SF7: امنیت در برابر حمله ردیابی، SF8: امنیت در برابر حمله مردی در میانه.

پروتکل	[۸]	[۹]	[۱۲]	[۱۹]	[۲۳]	[۲۶]	[۱]	پیشنهادی
SF1	✓	✓	✓	✓	✓	✓	✓	✓
SF2	×	✓	✓	✓	✓	✓	✓	✓
SF3	×	×	✓	✓	✓	✓	✓	✓
SF4	×	✓	✓	✓	✓	✓	✓	✓
SF5	✓	✓	✓	✓	✓	✓	✓	✓
SF6	✓	✓	✓	×	N/A	✓	✓	✓
SF7	×	✓	✓	×	N/A	✓	×	✓
SF8	×	✓	✓	✓	✓	✓	✓	✓

۷-۲- تحلیل کارایی

در این بخش کارایی پروتکل بهبودیافته پیشنهادی مورد ارزیابی قرارگرفته و مقایسه پروتکل پیشنهادی با مهم‌ترین پروتکل‌های احراز هویت مبتنی بر RFID باهدف به‌کارگیری در سامانه‌های مراقبت پزشکی از راه دور ازنظر پیچیدگی محاسباتی و مخابراتی برچسب‌ها و واحد خواننده - سرور صورت می‌گیرد.

پیچیدگی محاسباتی

برای ممکن سازی مقایسات، در این بخش از زمان‌های گزارش‌شده در [۲۶] استفاده کرده و همچنین از هزینه محاسباتی اعمال کم‌هزینه مانند جمع، تفریق و یای انحصاری ($\oplus$) صرف‌نظر می‌کنیم. همچنین، با توجه به قضیه کوچک فرما، پیچیدگی محاسباتی محاسبه وارون ضربی تقریباً برابر با پیچیدگی محاسباتی توان رسانی پیمانه‌ای است که از این نکته نیز در ساده‌سازی مقایسه‌ها استفاده‌شده است. با توجه به نتایج گزارش‌شده در [۲۶] زمان محاسبه عملگرهای به‌کاررفته در پروتکل‌های احراز هویت مبتنی بر RFID به شرح زیر است:

- محاسبه مقدار یک تابع چکیده ساز (T_h): ۰,۰۰۰۴ میلی‌ثانیه (ms).
- ضرب پیمانه‌ای (T_{mm}): ۰,۰۱۵ میلی‌ثانیه.
- توان رسانی پیمانه‌ای (T_{me}): ۱,۸۳ میلی‌ثانیه.
- جمع نقاط منحنی بیضوی (T_{aec}): ۰,۰۰۹ میلی‌ثانیه.
- ضرب اسکالر (T_{sm}): ۷,۳۵ میلی‌ثانیه.

در پروتکل پیشنهادی، یک برچسب در هر دور احراز هویت دو عمل توان رسانی، سه عمل ضرب پیمانه‌ای و چهار عمل چکیده‌سازی انجام می‌دهد. با توجه به این مسئله، سربار محاسباتی برچسب در یک دور احراز هویت برابر با ۳,۷۰۶۶ میلی‌ثانیه خواهد بود. در سوی مقابل، واحد خواننده - سرور دو عمل توان رسانی، ۳ عمل ضرب پیمانه‌ای، ۴ عمل چکیده‌سازی و یک عمل محاسبه وارون ضربی پیمانه‌ای صورت می‌دهد. درنتیجه سربار محاسباتی واحد خواننده - سرور برابر با ۴,۵۳۶۶ میلی‌ثانیه خواهد بود.

مقایسه پروتکل پیشنهادی با پروتکل‌های مرتبط موجود ازنظر محاسباتی در جدول (۲) آورده شده است. همان‌طور که نتایج این جدول نشان می‌دهد، از بین پروتکل‌های تأمین‌کننده تمام نیازمندی‌های امنیتی (پروتکل پیشنهادی، و پروتکل‌های ارائه‌شده در [۱۲] و [۲۶])، پروتکل بهبودیافته پیشنهادی از پیچیدگی محاسباتی کمتر و درنتیجه کارایی بالاتری برخوردار است.

جدول (۲): مقایسه پروتکل پیشنهادی با پروتکل‌های مرتبط ازنظر پیچیدگی محاسباتی با نماد T به‌عنوان برچسب و R/S به‌عنوان واحد خواننده – سرور.

پروتکل	موجودیت	پیچیدگی محاسباتی	کلی (ms)
[۸]	T	$2T_h + 2T_{ac} + 2T_{sm}$	≈ 22.0876
	R/S	$2T_h + 2T_{ac} + 1T_{sm} + 2T_{mi}$	
[۹]	T	$2T_h + 1T_{ac} + 2T_{sm}$	≈ 22.0969
	R/S	$2T_h + 1T_{ac} + 1T_{sm} + 2T_{mi}$	
[۱۲]	T	$2T_h + 1T_{ac} + 2T_{sm}$	≈ 21.9796
	R/S	$2T_h + 1T_{ac} + 1T_{sm}$	
[۱۹]	T	$4T_h + 1T_{ac} + 3T_{sm}$	≈ 44.1208
	R/S	$3T_h + 1T_{ac} + 3T_{sm} + 2T_{mi}$	
[۲۳]	T	$1T_{ac} + 4T_{sm}$	≈ 66.168
	R/S	$1T_{ac} + 5T_{sm}$	
[۲۶]	T	$2T_h + 1T_{mm} + 2T_{me}$	≈ 5.5216
	R/S	$2T_h + 1T_{mm} + 1T_{me} + 1T_{mi}$	
[۱]	T	$3T_h + 2T_{mm} + 2T_{me}$	≈ 3.6912

	$3T_h + 2T_{mm} + 1T_{me} + 1T_{mi}$	R/S	
≈ 3.7066	$3T_h + 3T_{mm} + 2T_{me}$	T	پیشنهادی
	$3T_h + 3T_{mm} + 1T_{me} + 1T_{mi}$	R/S	

پیچیدگی مخابراتی

در پروتکل پیشنهادی از ۳ دور مخابراتی استفاده‌شده است. در دور اول پیام k_1 توسط واحد خواننده – سرور به برچسب ارسال می‌شود. در دور دوم، پیام $(x_1, x_2, x_3, Auth_i)$ توسط برچسب به واحد خواننده – سرور ارسال‌شده و در دور سوم، پیام k_2 توسط واحد خواننده – سرور به برچسب بازگردانده می‌شود. با توجه به مفروضات در نظر گرفته‌شده، طول پیام ارسالی در دورهای اول و سوم ۱۶۰ بیت و طول پیام ارسالی در دور دوم برابر با ۱۵۰۸ بیت است. مقایسه پروتکل پیشنهادی با پروتکل‌های مرتبط موجود ازنظر هزینه مخابراتی در جدول (۳) آورده شده است. همان‌طور که نتایج این جدول نشان می‌دهد از بین پروتکل‌های موجود، تنها پروتکل‌های ارائه‌شده در [۹] و [۱۲] ازنظر اندازه کلی پیام‌های ارسال‌شده از پروتکل ارائه‌شده کاراتر هستند که همان‌طور که در بخش‌های پیشین بیان شد، پروتکل ارائه‌شده در [۹] فاقد امنیت پیش رو بوده و پروتکل ارائه‌شده در [۱۲] نیز ازنظر محاسباتی به‌شدت از پروتکل پیشنهادی ناکاراتر است. ازنظر تعداد دور مخابراتی نیز همه پروتکل‌های موردبررسی به‌جز پروتکل ارائه‌شده در [۱۹] از ۳ دور مخابراتی تشکیل‌شده‌اند. این در حالی است که پروتکل ارائه‌شده در [۱۹] امنیت در برابر حملات منع خدمت و ردیابی را تأمین نمی‌کند.

جدول (۳). مقایسه پروتکل پیشنهادی با پروتکل‌های مرتبط ازنظر پیچیدگی مخابراتی با نماد N_R به‌عنوان تعداد دور مخابراتی، MS_T به‌عنوان اندازه پیام ارسالی توسط برچسب، $MS_{R/S}$ به‌عنوان اندازه پیام ارسالی توسط واحد خواننده – سرور، و MS به‌عنوان اندازه کل پیام‌های ارسالی.

پروتکل	N_R	MS_T	$MS_{R/S}$	MS
[۸]	۳	۱۱۸۴	۶۷۲	۱۸۵۶
[۹]	۳	۱۱۸۴	۴۱۶	۱۶۰۰
[۱۲]	۳	۱۰۲۴	۴۱۶	۱۴۴۰
[۱۹]	۲	۱۰۲۴	۱۲۸۰	۲۳۰۴
[۲۳]	۳	۱۰۲۴	۱۵۳۶	۲۵۶۰
[۲۶]	۳	۲۲۰۸	۱۱۸۴	۳۳۹۲
[۱]	۳	۲۲۰۸	۴۸۰	۲۶۸۸
پیشنهادی	۳	۱۵۰۸	۳۲۰	۱۸۲۸

نتایج جدول (۱) نشان می‌دهد که از بین پروتکل‌های مشابه موجود، تنها دو پروتکل ارائه‌شده در [۱۲] و [۲۶] تمام ویژگی‌های امنیتی موردنیاز را تأمین می‌کنند. علاوه‌براین، نتایج جدول‌های (۲) و (۳) بیانگر این است پروتکل پیشنهادی در مقایسه با پروتکل ارائه‌شده در [۱۲] ازنظر محاسباتی ۴۹ درصد و ازنظر مخابراتی ۸۵ درصد کاراتر بوده، و در مقایسه با پروتکل ارائه‌شده در [۲۶] ازنظر محاسباتی ۴۹۳ درصد کاراتر و ازنظر مخابراتی ۲۲ درصد غیرکاراتر است. نتایج ارائه‌شده روی‌هم‌رفته بیانگر کارایی بالاتر پروتکل پیشنهادی در مقایسه با پروتکل‌های امن مشابه است.

۸- نتیجه‌گیری

در این مقاله، امنیت پروتکل احراز هویت کارای مبتنی بر RFID اخیراً پیشنهادشده توسط Shariq و همکاران بررسی‌شده و نشان داده شد که این پروتکل در برابر حمله ردیابی ناامن است. در ادامه با اعمال تغییراتی در پروتکل Shariq و همکاران، یک پروتکل بهبودیافته ارائه و نشان داده شد که پروتکل پیشنهادی ویژگی‌های امنیتی موردنیاز یعنی محرمانگی، احراز هویت دوسویه و امنیت پیش رو را تأمین کرده و در برابر حملات جعل هویت، بازپخش، منع خدمت، ردیابی، و مردی در میانه امن است. مقایسه صورت گرفته با دیگر پروتکل‌های امن مشابه بیانگر این است که پروتکل پیشنهادی در مقایسه با یکی از این پروتکل‌ها ازنظر پیچیدگی محاسباتی ۴۹ درصد و ازنظر پیچیدگی مخابراتی ۸۵ درصد کاراتر، و در مقایسه با دیگر پروتکل امن مشابه ازنظر پیچیدگی محاسباتی ۴۹۳ درصد کاراتر و ازنظر پیچیدگی مخابراتی ۲۲ درصد غیرکاراتر است؛ که روی‌هم‌رفته، بیانگر کارایی بالاتر پروتکل پیشنهادی در مقایسه با پروتکل‌های امن مشابه است.

۹- مراجع

[1] B. Moazzami, N. Razavi-Khorasani, A. D. Moghadam, E. Farokhi, and N. Rezaei, "Covid-19 and telemedicine: Immediate action required for maintaining healthcare providers well-being," J. Clin. Virol., vol. 126, 104345, 2020. https://doi.org/10.1016/j.jcv.2020.104345.

[2] J. Vidal-Alaball, R. Acosta-Roja, N. P. Hern´andez, U. S. Luque, D. Morrison, S. N. P´erez, J. Perez-Llano, A. S. V`erges, and F. L. Seguí, "Telemedicine in the face of the covid-19 pandemic," Aten. Prim., vol. 52, no. 6, pp. 418-422, 2020. https://doi.org/10.1016/j.aprim.2020.04.003.

[3] V. Chauhan, S. Galwankar, B. Arquilla, M. Garg, S. Di Somma, A. El-Menyar, V. Krishnan, J. Gerber, R. Holland, and S. P. Stawicki, "Novel coronavirus (covid-19): Leveraging telemedicine to optimize care while

[15] C. Jin, C. Xu, X. Zhang, and F. Li, "A secure ECC-based RFID mutual authentication protocol to enhance patient medication safety," J. Med. Syst., vol. 40, no. 1, pp. 1-6, 2016. https://doi.org/10.1007%2Fs10916-015-0362-8.

[16] J. prakash Pokala, M. C. Reddy, S. Bapana, and C. S. Vorugunti, "A secure RFID protocol for telecare medicine information systems using ECC," 2016 international conference on wireless communications, signal processing and networking (WISPNET), pp. 2295-2300, 2016. https://doi.org/10.1109/WiSPNET.2016.7566552.

[17] Z. Zhou, P. Wang, and Z. Li, "A quadratic residue-based RFID authentication protocol with enhanced security for TMIS," J. Amb. Intel. Hum. Comp., vol. 10, no. 9, pp. 3603-3615, 2019. https://doi.org/:10.1007/s12652-018-1088-5.

[18] T. Afroz, M. N. U. Bhuiyan, and M. N. Uddin, "A secure mutual authentication protocol for IoT using ID verifier based on ECC," 2019 international conference on sustainable technologies for industry 4.0 (STI), pp. 1-6, 2019. https://doi.org/10.1109/STI47673.2019.9068089.

[19] H. Shen, J. Shen, M. K. Khan, and J.-H. Lee, "Efficient RFID authentication using elliptic curve cryptography for the internet of things," Wireless Pers. Commun., vol. 96, no. 4, pp. 5253-5266, 2017. https://doi.org/10.1007/s11277-016-3739-1.

[20] F. Xiao, Y. Zhou, J. Zhou, H. Zhu, and X. Niu, "Security Protocol for RFID System Conforming to EPC-C1G2 Standard," J. Computers, vol. 8, no. 3, pp. 605-612, 2013.

[21] M. Mardani Shahrbabak, B. Abdolmaleki, and K. Baghery, "Weaknesses of SPRS Authentication Protocol and Present a Developed Protocol for RFID Systems," Journal of Electronical & Cyber Defence, vol. 3, no. 3, pp. 39-48, 2016 (in Persian). https://dorl.net/dor/20.1001.1.23224347.1394.3.3.5.4.

[22] M. Safkhani, "Cryptanalysis of the Improved SPRS Protocol: an Authentication Protocol for RFID Systems," Journal Of Electronical & Cyber Defence, vol. 5, no. 2, pp. 59-66, 2017 (in Persian). https://dorl.net/dor/20.1001.1.23224347.1396.5.2.5.6.

[23] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for internet of things," J. Supercomput., vol. 74, no. 9, pp. 4281-4294, 2018. https://doi.org/10.1007/s11227-016-1861-1.

[24] Y.-J. Tu, G. Kapoor, and S. Piramuthu, "Security of lightweight mutual authentication protocols," J. Supercomput., vol. 77, no. 5, pp. 4565-4581, 2020. https://doi.org/10.1007/s11227-020-03448-y.

[25] D. Noori, H. Shakeri, and M. N. Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for internet of things in healthcare environment," EURASIP J. Inform. Sec., vol. 20, no. 1, pp. 1-11, 2020. https://doi.org/10.1186/s13635-020-00114-x.

minimizing exposures and viral transmission," J. Emerg. Trauma Shock, vol. 13, no. 1, pp. 20-24, 2020. https://doi.org/10.4103/JETS.JETS_32_20.

[4] M. Shariq, and K. Singh, "A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment," J. Supercomput., vol. 77, no. 8, pp. 8532-8562, 2021. https://doi.org/10.1007/s11227-020-03550-1.

[5] M. Shariq, K. Singh, M. Y. Bajuri, A. A. Pantelous, A. Ahmadian, and M. Salimi, "A secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario," Sustain. Cities Soc., vol. 75, 103354, 2021. https://doi.org/10.1016/j.scs.2021.103354.

[6] D. Dharminder, D. Mishra, and X. Li, "Construction of RSA-based authentication scheme in authorized access to healthcare services," J. Med. Syst., vol. 44, no. 1, pp. 1-9, 2020. https://doi.org/10.1007/s10916-019-1471-6.

[7] S. D. Kaul, and A. K. Awasthi, "RFID authentication protocol to enhance patient medication safety," J. Med. Syst., vol. 37, no. 6, pp. 1-6, 2013. https://doi.org/10.1007/s10916-013-9979-7.

[8] J.-S. Chou, "An efficient mutual authentication RFID scheme based on elliptic curve cryptography," J. Supercomput., vol. 70, no. 1, pp. 75-94, 2014. https://doi.org/10.1007/s11227-013-1073-x.

[9] Z. Zhang, and Q. Qi, "An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography," J. Med. Syst., vol. 38, no. 5, pp. 1-7, 2014. https://doi.org/10.1007/s10916-014-0047-8.

[10] Y.-P. Liao, and C.-M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," Ad Hoc Netw., vol. 18, pp. 133-146, 2014. https://doi.org/10.1016/j.adhoc.2013.02.004.

[11] Z. Zhao, "A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem," J. Med. Syst., vol. 38, no. 5, pp. 1-7, 2014. https://doi.org/10.1007/s10916-014-0046-9.

[12] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A provably secure RFID authentication protocol based on elliptic curve for healthcare environments," J. Med. Syst., vol. 40, no. 7, pp. 1-7, 2016. https://doi.org/10.1007/s10916-016-0521-6.

[13] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system," J. Med. Syst., vol. 39, no. 1, pp. 1-5, 2015. https://doi.org/10.1007/s10916-014-0153-7.

[14] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system," J. Med. Syst., vol. 39, no. 8, pp. 1-8, 2015. https://doi.org/10.1007/s10916-015-0260-0.

information system," Wireless Pers. Commun., vol. 96, no. 4, pp. 6221-6238, 2017. https://doi.org/10.1007/s11277-017-4474-y.

[30] M. Shariq, and K. Singh, "A novel vector-space-based lightweight privacy preserving RFID authentication protocol for IoT environment," J. Supercomput., vol. 77, no. 8, pp. 8532-8562, 2021. https://doi.org/10.1007/s11227-020-03550-1.

[31] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo, and W.-K. Chou, "A lightweight authentication scheme for telecare medical information system," Connect. Sci., vol. 33, no. 3, pp. 769-785, 2021. https://doi.org/10.1080/09540091.2021.1889976.

[32] W. R. Liu, Z. Y. Ji, and C. C. Chu, "An Improved Secure RFID Authentication Protocol Using Elliptic Curve Cryptography," Int. J. Netw. Sec., vol. 26, no. 1, pp. 106-115, 2024. https://doi.org/10.6633/IJNS.202401_26(1).14.

[26] F. M. Salem, and R. Amin, "A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS," Inform. Sciences, vol. 527, pp. 382-393, 2020. https://doi.org/10.1016/j.ins.2019.07.029.

[27] X. Chen, D. Geng, J. Zhai, W. Liu, H. Zhang, and T. Zhu, "Security analysis and enhancement of the most recent RFID protocol for telecare medicine information system," Wireless Pers. Commun., vol. 114, no. 2, pp. 1371-1387, 2020. https://doi.org/10.1007/s11277-017-4474-y.

[28] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," IEEE T. Ind. Inform., vol. 14, no. 4, pp. 1656-1665, 2018. https://doi.org/10.1109/TII.2018.2794996.

[29] M. Benssalah, M. Djeddou, and K. Drouiche, "Security analysis and enhancement of the most recent RFID authentication protocol for telecare medicine