حفظ حریم خصوصی در اینترنت اشیا برای انتقال داده‌ها در حوزهٔ سلامت با استفاده از زنجیرهٔ بلوکی

عباس حسن پورعسکری [۱]، عمید خطیبی بردسیری [۲]*، مختار محمدی قنات غستانی [۳]

دانشجوی دکترای گروه کامپیوتر، واحد علوم و تحقیقات- پردیس مرکز آموزش بین المللی قشم، دانشگاه آزاد اسلامی، قشم، ایران[۱]

استادیار گروه کامپیوتر، دانشگاه آزاد اسلامی واحد بردسیر، بردسیر، ایران[۲]

استادیار گروه کامپیوتر، دانشگاه آزاد اسلامی واحد بم، بم، ایران[۳]

چکیده

استفاده از زنجیرهٔ بلوکی در حفظ حریم خصوصی افراد موضوعی است که توانسته است نظرات پژوهش‌گران را به خود جلب کند و نیازمندی بسیار مهمی در سامانه‌های اطلاعاتی و داده‌ای به شمار می‌آید. از طرفی نظام سلامت پزشکی با توجه به حساسیت‌های موجود در حفظ اطلاعات بیماران و افراد درگیر در سلامت پزشکی مانند پزشکان و پرستاران، دارای زمینهٔ مساعدی برای به‌کارگیری نظام قدرتمند زنجیرهٔ بلوکی برای حفظ حریم خصوصی است. در پژوهش حاضر بر حفظ محرمانگی داده‌های سلامت پزشکی در اینترنت اشیا، مبتنی بر ابر با استفاده از زنجیرهٔ بلوکی و محاسبات لبه تأکید می‌شود؛ به‌گونه‌ای که این روش بتواند محرمانگی داده‌ها در این محیط‌ها و بسترهای پزشکی را به‌ویژه برای بیماران تحت مراقبت به شکل مطلوب فراهم آورد. ذخیرهٔ داده‌های پزشکی با این فناوری در پاسخ به نیازمندی هم‌زمان کارایی سامانه و حفظ محرمانگی پیشنهاد شده‌است. به‌طور مشخص این روش از طریق بهره‌گیری از احراز هویت با روش نامتقارن در لبهٔ ابر و تبادل کلید دیفی-هلمن برای موارد ناشناس‌بودن، استفاده از زنجیرهٔ بلوکی و پیرو آن درهم‌سازی SHA2 و رمزنگاری PKI سعی در ایجاد بستری با امنیت و به‌ویژه حریم خصوصی بالا جهت کاربردهای مراقبت پزشکی کرده‌است؛ این سامانه در ادامه شبیه‌سازی و نشان داده شده‌است که می‌تواند در نظام سلامت پزشکی بر روی ترکیب ابراینترنت اشیا از منظر عملکردی تأثیر مناسبی داشته باشد. مطابق نتایج با اجرای روش، از نظر نقض SLA سامانه در شرایطی قرار می‌گیرد که حتی درصورت حمله نقض SLA وجود نداشته باشد و کارایی حفظ شود؛ همچنین درصد دستیابی به اطلاعات مفید توسط هکر نزدیک به صفر خواهد بود. با جلوگیری از ورود گره‌های مخرب گذردهی حدود سی‌درصد افزایش نشان می‌دهد. همچنین در مقایسه با برخی روش‌های دیگر که در سال‌های اخیر توسط پژوهش‌گران ارائه شده‌اند، خنثی‌سازی مهاجمان موجب بهبود دست‌کم پنج‌درصدی در کارایی سامانه می‌شود. از دیگر محاسن این روش انعطاف‌پذیری و مقیاس‌پذیری بالا، مقاوم‌بودن، زمان اجرای مناسب و تأخیر کمابیش پایین است که به‌واسطهٔ استفاده از ابر لبه به‌وجود می‌آید.

واژگان کلیدی: Cloud-IoT، سوابق پزشکی الکترونیکی، زنجیرهٔ بلوکی، محرمانگی داده‌ها، محاسبات لبه.

IoT privacy for the transmission of data in the field of health using blockchain

Abbas Hassan Pour Askari[1], Amid Khatibi Bardsiri [2]*, Mokhtar Mohammadi Ghanat Ghestani [3]

Phd Student, Department of Computer, Science and Research Branch, Qeshm international educational center, Islamic Azad University, Qeshm, Iran[1]

Assistant Professor, Department of Computer, Bardsir Branch, Islamic Azad University, Bardsir, Iran[2]

Assistant Professor, Department of Computer, Bam Branch, Islamic Azad University, Bam, Iran[3]

Abstract

Data transmission and storage through blockchain is something that many studies have suggested for various security issues. Due to the sensitivities in securing information from patients and medical

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۱/۳/۱۰ • تاریخ پذیرش: ۱۴۰۳/۳/۱۲ • تاریخ انتشار: ۱۴۰۳/۱۰/۲۸ • نوع مطالعه: پژوهشی

[DOI: 10.61186/jsdp.21.3.149]

professionals, the healthcare system has a favorable context for deploying a powerful blockchain system for privacy. Blockchain application in the healthcare system allows physicians to store patient records with high security and make them available to other hospitals and clinics as needed. Besides increasing data transmission and storage security, this reduces data management risks and expenses.

The present study emphasizes the confidentiality of healthcare data in the cloud-based Internet of Things (IoT) using blockchain and edge computing. Also this method uses SHA2 hashing and PKI encryption. Therefore, it can optimally provide data confidentiality in medical settings, especially for patients under care.

The system proposed in this study includes five parts: users, IoT devices, edge devices, security server, and cloud computing. The proposed method uses the Diffie – Hellman key exchange in the authentication process for anomality case to achieve the goal of essential security compliance. This method is a cryptographic (encryption) protocol allowing two people or two organizations to create a shared password key without the need for any prior acquaintance and exchange it through an insecure connection path. This study used data sensed by IoT network sensors with medical data for loading on IoT and cloud simulated networks. These data were related to monitoring patients with cardiovascular disease and were sampled on 300 patients. The research dataset belonged to the Cleveland Clinic Foundation for Heart Disease Dataset. The study simulation software was NS-2.35, which used C++ and TCL programming languages.

The research findings revealed that if there were no method for data encryption, much of the data would be exposed. This rate reaches 50% for 50 attackers. Encryption using the proposed method causes the percentage of data disclosed to be very slight, and it equals zero, even though attackers may guess the password or data. As network traffic grows, the throughput difference between blocking and non-blocking access methods increases. It suggests that by blocking the attacking nodes' access, network traffic will not have a detrimental effect on attacking nodes by detecting and preventing their activity. However, if the access of these nodes is not blocked, the destructive impact is very high, and the network traffic will grow slightly. According to these results, in terms of SLA violation, the system is in a situation where even in case of an attack, there is no SLA violation and the efficiency is maintained. Also, the percentage of access to useful information by the hacker will be close to zero. By preventing the entry of malicious nodes, the throughput increases by about 30%. Some other advantages of this method are its high flexibility and comparability, robustness, and relatively low execution time and delay, which is caused by the use of cloud edge.

It is estimated that the improvement rate of the proposed method is more than 5% compared to other related approaches. In the design presented in this study, the processes are highly simplified, and there will be a relatively low processing overhead. At the same time, the steps meet all the requirements for cloud and IoT data centers in healthcare applications.

Keywords: cloud-based IoT, Electronic health record, blockchain, data confidentiality, edge computing.

۱-مقدمه

رایانش ابری تغییرات عمده‌ای در سبک زندگی و روش‌های کار افراد ایجاد کرده و کارایی زیادی داشته‌است. همان‌طور که شرکت‌ها برای ساده‌کردن کارها و صرفه‌جویی در هزینه‌ها به سمت فناوری‌های رایانش ابری پیش می‌روند، امنیت این سامانه‌ها دغدغه‌ای اساسی خواهد بود. حملات در این سامانه‌ها می‌توانند بر روی زیرساخت‌ها، شبکهٔ ارتباطات، اطلاعات و خدمات متمرکز شوند[۱]؛ بنابراین امنیت رایانش ابری همیشه مورد توجه مشتریان بالقوهٔ ابری و مانعی بزرگ برای استفادهٔ گسترده از آن است. از آنجا که سامانه‌های فناوری اطلاعات رایانش ابری برای کاربران غیرمشهود است، قابل درک است که مشتریان می‌خواهند از اطلاعاتشان به‌طور کامل محافظت شود و خدمات ارائه‌شده پایدار[1] باشند. این پایداری درواقع نمایان‌گر مفهومی به نام قابلیت اطمینان است که سامانه بتواند در ارائهٔ خدمات حتی با وجود مشکلاتی که ممکن است پیش بیاید، تداوم داشته باشد. پس نگرانی‌ها به‌ویژه در زمینهٔ امنیت و قابلیت اطمینان افزایش یافته‌است.

با رشد سریع کاربردهای اینترنت اشیا، مفاهیم امنیت و حفظ حریم خصوصی مورد توجه قرار می‌گیرند و نگرانی‌هایی در زمینهٔ محرمانگی، نبود تداوم سرویس و ناتوانی مردم در کنترل زندگی شخصی خود شکل می‌گیرد. اگر فعالیت روزانهٔ افراد نظارت شده و آن‌ها تولیدکنندهٔ خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت‌تأثیر قرار می‌گیرند، امنیت و حریم خصوصی شبکه و اطلاعات به‌وسیلهٔ مؤلفه‌های شناسایی، محرمانگی، یک‌پارچگی، انکارناپذیری و کارکرد مداوم و درست سامانه سنجیده می‌شوند.

[1] Stable

[DOI: 10.61186/jsdp.21.3.149]

اینترنت اشیا در حوزهٔ اقتصاد جهانی و در خدمات پزشکی، مراقبت‌های بهداشتی، حمل‌ونقل هوشمند و بسیاری دیگر از حوزه‌ها به‌کار گرفته می‌شود؛ لذا نیازمندی‌های امنیتی در آن از اهمیت بالایی برخوردارند. با داشتن اینترنت اشیا می‌توان پیش‌بینی کرد که مجرمان سایبری در مرحلهٔ نخست به نقاط به‌وجودآمدن و انتقال اطلاعات، مراکز ارسال دستورات، نقاط و مدخل‌های شبکه حمله خواهند کرد و محافظت را باید برای این نقاط فراهم کرد. ناهم‌گونی پروتکل‌ها و دستگاه‌ها، توسعهٔ سرویس‌های امنیتی با تحمل خطای بالا را به فعالیتی دشوار تبدیل می‌کند[۲].

یکی از مسائل اصلی در سامانه‌های فناوری اطلاعات، چگونگی محافظت از مقادیر داده‌ای در زمان انتقال داده ضمن حفظ الگوهای داده‌ای موجود در مجموعه‌های داده‌هاست[۳]؛ به عبارت دیگر، صاحبان داده علاوه بر حفظ حریم خصوصی باید قادر باشند صحت داده‌های انتقال‌داده‌شده و دریافت‌شده را نیز تضمین کنند. داده‌های پزشکی ضریب حساسیت بسیار بالایی دارند؛ بنابراین میزان توجه و حفاظت بالاتری را طلب می‌کنند؛ زیرا این داده‌ها با سلامتی بیماران در ارتباط هستند و هر تغییر نادرست در این داده‌ها و بروز خطا در سامانه شناخت داده‌ها می‌تواند منجر به خطرات زیادی شود. هرکدام از ویژگی‌هایی که در بطن داده‌ها وجود دارد، میزان اهمیت ویژهٔ خود را دارد و توجه خاصی را می‌طلبد. سامانه‌های ثبت الکترونیکی سلامت[1] (EHR) و یا مدارک الکترونیکی پزشکی[2] (EMR) سامانه‌هایی هستند که به‌تازگی به‌منظور نگهداری اطلاعات پزشکی استفادهٔ فراوانی یافته‌اند. EHRها ممکن است شامل طیف وسیعی از اطلاعات، از جمله جمعیت، سابقهٔ پزشکی، دارو و آلرژی، وضعیت ایمن‌سازی، نتایج آزمایش‌ها، تصاویر رادیولوژی، علائم حیاتی، آمار شخصی مانند سن و وزن و اطلاعات صورت‌حساب باشد.

حفظ حریم خصوصی از جمله مسائل مهم و پیچیده‌ای است که در انتشار داده‌ها، باید بدان توجه داشت[۴]. در حالت کلی امکان وجود داده‌های خصوصی یا محرمانه در بین داده‌های تحت پردازش وجود دارد؛ بنابراین حفظ محرمانگی اطلاعات، مانع دسترسی مستقیم به تمامی داده‌ها می‌شود. برای مثال ممکن است مؤسسه‌های پزشکی بخواهند با همکاری یکدیگر بر روی پایگاه داده‌های خود پژوهشی انجام بدهند، به‌طوری‌که محرمانگی اطلاعات بیمارانشان حفظ شود و هیچ‌کدام از آن‌ها از مقادیر پایگاه دادهٔ دیگران مطلع نشوند. برای حل این قبیل مشکلات، مبحث اشتراک داده‌ها با حفظ محرمانگی مطرح شده‌است. تبادل مقادیر بین رکوردها، تبادل مقادیر صفت خاصه‌ها، جایگزینی پایگاه داده‌های اصلی با یک نمونه از توزیع مشابه، اضافه‌کردن اختلال به داده‌های پایگاه داده، اضافه‌کردن اختلال به نتایج پرس‌وجو و نمونه نتایج پرس‌وجوها همگی جزو روش‌های مربوط به حفظ حریم خصوصی داده‌های منتشر شده‌اند.

در فناوری اطلاعات یکی از فناوری‌های کمابیش جدید برای تأمین امنیت زنجیره‌های بلوکی[3] هستند که اطلاعات را به‌صورت زنجیره‌هایی از داده‌های معنادار و پشت سر هم انتقال می‌دهد و نگهداری می‌کند. زنجیره‌های بلوکی از فناوری‌های رمزنگاری برای اطمینان از محرمانه‌بودن حتی در زنجیرهٔ عمومی استفاده می‌کنند. یکپارچگی داده‌ها از طریق وقایع منطقی بر روی یک دفترچهٔ تغییرناپذیر نگه داشته می‌شود، که امکان دستیابی به اطلاعات را نیز فراهم می‌کند[۵].

انتقال و ذخیره‌سازی اطلاعات توسط زنجیره‌های بلوکی اتفاقی است که در بسیاری پژوهش‌ها برای امنیت مسائل مختلف پیشنهاد شده‌است. تراکنش‌ها و رویدادهای اتفاق افتاده در این زنجیره‌ها به شکل بلوک‌های به‌هم‌پیوسته و دارای چندین مشخصهٔ اصلی ذخیره می‌شود. بلوک‌ها درواقع نوعی ساختار دادهٔ فهرست پیوندی را تداعی می‌کنند و شامل ارجاعاتی به بلوک‌های قبلی و بعدی و همچنین شامل زمان انجام تراکنش و اطلاعات دیگرند؛ همچنین این داده‌ها به‌واسطهٔ رمزنگاری و ارتباط آن با بلوک‌های دیگر که خود در سامانه رمزگذاری استفاده می‌شود، دارای یکپارچگی و امنیت بالایی هستند که شکست‌دادن آن را سخت و حتی غیرممکن می‌سازد.

استفاده از زنجیرهٔ بلوکی در مورد نظام سلامت پزشکی این فناوری به پزشکان اجازه می‌دهد تا پرونده‌ای از سوابق بیماران را با امنیت بالا ذخیره کنند و آن‌ها را در صورت لزوم در اختیار دیگر بیمارستان‌ها و مراکز درمانی قرار دهند؛ این کار علاوه‌بر افزایش امنیت ذخیره‌سازی و انتقال داده‌ها، باعث کاهش خطرها و هزینه‌های مدیریت داده‌ها می‌شود. با توجه به مزیت‌ها و جذابیت‌های موجود در زنجیرهٔ بلوکی در این پژوهش این روش برای ایجاد ساختاری مؤثر در حفظ محرمانگی اطلاعات در سامانه سلامت الکترونیک بر روی Cloud-IoT به‌کار برده شد و چنانچه بحث خواهد شد، مزایای

[1] Electronic health record
[2] Electronic medical records
[3] Blockchains

[DOI: 10.61186/jsdp.21.3.149]

آن می‌تواند موجب بهبود محرمانگی و کارایی در ساختار نظام سلامت پزشکی شود.

در ادامهٔ این مقاله، در بخش دوم بیان کلی شبکه‌های ترکیبی Cloud-IoT ارائه می‌شود و نیز به کارهای پیشین در این زمینه و تعادل بار پرداخته خواهد شد؛ بخش سوم روش پیشنهادی را برای اجرای سازوکار ایجاد محرمانگی با بهره‌گیری از تئوری زنجیرهٔ بلوکی به‌منظور افزایش کارایی و محرمانگی شبکه شرح می‌دهد؛ در بخش چهارم نتایج شبیه‌سازی و ارزیابی قابل مشاهده‌است؛ درنهایت در بخش پنجم نتیجه‌گیری و کارهای آینده بیان خواهد شد.

۲-ادبیات پژوهش

در این بخش در ارتباط با مفاهیم مورد نیاز مانند نظارت بر سلامت از طریق Cloud-IoT و ساختار زنجیرهٔ بلوکی صحبت می‌شود تا در بخش نوآوری مقاله طراحی برای محرمانگی دادهٔ سلامت از طریق زنجیرهٔ بلوکی بر پایهٔ آن بیان شود؛ همچنین پس از صحبت در ارتباط با مفاهیم، پژوهش‌های پیشین در این ارتباط مورد نظر قرار گرفته‌است.

۲-۱-کاربرد ابر-IOT با هدف نظارت بر سلامت

ارتباط اینترنت اشیا و رایانش ابری از بسیاری جهات واضح است[۷]: مؤلفه‌هایی همچون همه‌گیربودن و قابلیت ذخیره‌سازی و پردازش بالا، استفاده از منابع مجازی به جای منابع حقیقی، قدرت مانور بر روی مدیریت جامع و ارتباط بین چندین شبکه اینترنت اشیا، ارائهٔ سرویس‌های پیشرفته، مزایایی است که رایانش ابری می‌تواند به نحو مطلوبی در اینترنت اشیا فراهم سازد. می‌توان گفت که این ارتباط در صورت یک‌پارچه‌کردن هر دو فناوری یک‌سری امکانات ویژه را فراهم می‌سازد؛ با توجه به مقیاس‌پذیری ابر و منابعی که چه در نظریه و چه در عمل در ابر نامحدودند، محدودیت منابع در اینترنت اشیا و قدرت پایین پردازش جبران می‌شود، و از طرف دیگر اینترنت اشیا امکان داشتن خدمات متنوع و وسیعی در دنیای واقعی را می‌دهد که بر کارایی فناوری ابر می‌افزاید[۸]. به‌عنوان یکی از موارد مهم از این کاربردها امروزه نیازهای پزشکی بسیار فراوان‌اند که برخی از آن‌ها به اینترنت اشیا وابسته‌اند. از مزایای رایانش ابری برای این نیازها و برطرف‌کردن محدودیت اینترنت اشیا در برخورد با آن، مانند انعطاف‌پذیری برای برطرف‌کردن نیازمندی‌های پردازشی و ذخیره‌سازی در کنار پردازش پویای داده‌ها در تمام زمان‌ها و تمام مکان‌ها، دست‌یابی محرمانه و امن دستگاه‌ها به اطلاعات بیماران، مدیریت و کنترل پیشرفتهٔ اطلاعات و راه حل‌های بازیابی اطلاعات و داشتن قابلیت اطمینان بالا در زمان خرابی، مقرون به‌صرفه‌بودن اقتصادی با توجه به عدم نیاز به تهیهٔ سخت‌افزار [۹] می‌توان بهره گرفت. ترکیب اینترنت اشیا و رایانش ابری به‌صورت مناسب، تأثیر بسزایی بر روی بهبود کیفیت زندگی بیماران خواهد داشت. این امر به‌ویژه در زمان استفاده از سرویس‌های پزشکی برای مراقبت از بیماران با سابقهٔ طولانی، نمود بیشتری پیدا می‌کند[۱۰]. از جمله کاربرد این فناوری در حوزهٔ سلامت می‌توان به کمک به کادر درمان برای کنترل درمان بیماران در خانه‌ها، کاربردهای شخصی از این خدمات برای بیماران مانند هشدار و یادآوری برای مصرف دارو، دستیابی به اطلاعات پزشکی و پرونده‌های افراد در فضای مجازی، پشتیبانی از گروه‌های اجتماعی که ارتباط بین بیمار، پزشکان و پرستاران برای اطلاع بیمار از شرایط خودش را فراهم می‌کند، اشاره کرد.

۲-۱-۱-لایه‌های مختلف معماری Cloud-IoT در پزشکی

در سطح بالای ساختار پروژهٔ مراقبت از سلامت توسط اینترنت اشیا و رایانش ابر اجزای زیر با ارتباطات شبکه‌ای و استفاده از رایانش ابری در مرکز پردازش و ذخیره‌سازی داده‌ها [۱۰] ارتباط دارند: مرکز درمانی (بیمارستان یا کلینیک)، بخش خدمات ضروری و اضطراری، مکان استراحت (یا حتی کار) بیمار و محیط‌های وابسته و اختصاص‌یافته به بیمار و خانوادهٔ او و تمام این مکان‌ها نیاز به استفاده از زیرساخت شبکه‌ای و ارتباط دارند. چارچوب معماری در یک نظام مراقبت پزشکی با بهره‌گیری از دستگاه‌های اینترنت اشیا، شبکه‌های ارتباطی و رایانش ابری پیشنهادی در [۱۱]، در سه لایهٔ مختلف سازماندهی شده‌است:

(۱) لایهٔ به‌دست‌آوردن داده‌ها (که در این لایه اطلاعات خام با مفاهیم ویژهٔ پزشکی در قالب انواع ساختارها از منابع مختلف به‌دست آورده و قبل از انتقال به لایهٔ بعدی، پیش‌پردازش می‌شوند).

(۲) لایهٔ مدیریت داده (که در آن قابلیت توزیع و ذخیره‌سازی داده‌های غیرهمسان و روش‌های پیشرفته‌ای برای پردازش و تجزیه و تحلیل داده‌ها وجود دارد).

(۳) لایهٔ کاربرد یا سرویس بر روی برنامه (که برای دسترسی به نتایج تجزیه و تحلیل داده‌های بصری، رابط یکپارچه به داده‌ها برای توسعهٔ برنامه‌ها و خدمات کاربر محور توسعه داده شده‌است).

ساختار هوشمند شبکهٔ بیمارستانی به همراه شناسایی، مکان‌یابی و نظارت هوشمند مبتنی بر اشیا که در [۱۲]

[DOI: 10.61186/jsdp.21.3.149]

ارائه شده‌است در شش‌لایه سازماندهی شده‌است: لایهٔ جمع‌آوری و پردازش داده‌ها (جمع‌آوری بی‌درنگ داده‌ها با استفاده از سامانه‌های شبکهٔ حس‌گر ویژه)، لایهٔ اجماع یا ترکیب داده‌ها (تبدیل داده‌های خام گرفته‌شده از لایهٔ قبلی و ذخیره‌سازی آن‌ها بر روی پایگاه دادهٔ مربوطه)، لایهٔ ابری و محاسباتی (که در آن از سامانه‌های رایانش ابری در جهت ذخیره‌سازی و بازیابی داده‌ها به همراه انجام نیازمندی‌های محاسباتی استفاده می‌شود)، لایهٔ شبکه (که در آن سامانه پایه برای انتقال داده‌ها از مبدأهای مختلف به یک یا چند مقصد در سامانه اطلاعاتی اتفاق می‌افتد)، لایهٔ تحلیل دانش (تلاش برای دریافت دانش و اطلاعات مفید از روی داده‌ها)، و لایهٔ نمایش (مشخص‌سازی داده‌ها و آماده‌سازی آن برای رساندن مفهوم و سپردن کنترل آن‌ها به کاربر). معماری Cloud-IoT در اینجا جهت توسعهٔ کاربرد پزشکی با بهره‌برداری و ترکیب برنامه‌ها و اجرای عملکردهای مربوط به IoT در مراقبت از بیماران با استفاده از خدمات خاص ابر است[۱۳].

۲-۱-۲-انواع کاربردهای مبتنی بر اینترنت اشیا در مراقبت پزشکی

تنوع زیادی در برنامه‌های مراقبت پزشکی وجود دارد که بر مبنای خدمات اینترنت اشیا شکل گرفته‌اند. برخی از موارد مهم از [۱۴] انتخاب شده‌است: نظارت بر دیابت (از طریق یک حس‌گر فیزیولوژیکی با اندازه‌گیری سطح قند خون یا برخی پارامترهای عملکردی در زمان افزایش قند)، نظارت بر تپش قلب (الکترودهای مخصوص متصل به یک فرستندهٔ بی‌سیم)، نظارت بر فشارخون (یک حس‌گر پوشیدنی با اندازه‌گیری تورم خودکار)، کنترل دمای بدن افراد (اندازه‌گیری درجه حرارت بدن بر روی پوست با سنسور پوشیدنی)، نظارت بر اجرای توان‌بخشی (از طریق حس‌گرهای مختلف پوشیدنی یا داخلی؛ همراه با تشخیص جریان، پیگیری ردپای رویداد، رساندن گزارش، بازخورد)، مراقبت از آسم که یک بیماری انسدادی مزمن ریوی است (توسط یک دستگاه صوتی و میکروفون کارگزاری‌شده داخل تلفن همراه؛ تشکیل و تحلیل نمودارهای حجم جریان بر پایهٔ زمان)، تشخیص سرفه (دستگاه صوتی مشابه؛ تجزیه و تحلیل اسپکتروگرام‌های ضبط‌شده)، تشخیص ملانوما (یک دوربین گوشی هوشمند برای مطابقت تصاویر مشکوک با کتابخانه‌ای از تصاویر پوست سرطانی).

۲-۲-روش مالی و امنیتی زنجیرهٔ بلوکی

این فناوری توسط ناکاموتو [۱۵] به‌منظور ارائهٔ راه حلی برای انجام کار محبوب خود در رابطه با ارز دیجیتالی یا ارز با رمزنگاری امن، یعنی بیت‌کوین، معرفی شد. ناکاموتو فناوری زنجیرهٔ بلوکی[1] را برای حل یکی از مشکلات بیت‌کوین که به‌خاطر هزینهٔ دوبرابری آن ایجاد می‌شود، به‌کار برد؛ اما به‌سرعت به شکل یک فناوری امنیتی در بسیاری از مسائل دیگر مورد استفاده قرار گرفت. زنجیرهٔ بلوکی مجموعه‌ای از بلوک‌های پشت سر هم است که به یکدیگر زنجیر شده و اندازهٔ این زنجیره با جای‌گذاری تراکنش‌ها در بلوک‌ها و پیوست به انتهای آن مدام افزایش پیدا می‌کند. سکوی[2] زنجیرهٔ بلوکی از رویکرد غیرمتمرکز استفاده و این موضوع امکان توزیع اطلاعات را به‌آسانی ایجاد می‌کند. با وجود این توزیع‌شدگی هر قسمت از اطلاعات توزیع‌شده به‌عنوان داده، مالکیت مشترکی را دارند که مربوط به مبدأ پیدایش آن داده‌است. در زنجیرهٔ بلوکی تراکنش‌ها به شکل مؤثر درهم‌سازی[3] شده‌اند و دستهٔ تراکنش‌ها را ایجاد می‌کند؛ بنابراین یک راه‌کار امنیتی را برای آن‌ها فراهم کرده و برای مدیریت آن از یک زیرساخت شبکه‌های نظیربه‌نظیر استفاده می‌کند. زنجیره‌های بلوکی دارای مزایای ویژه‌ای هستند که شامل امنیت، ناشناسی[4]، صحت داده‌ها و عدم دخالت شخص ثالث در تراکنش است. این ویژگی‌ها باعث می‌شود که سوابق پزشکی بیمار با

امنیت بالاتری در آن ذخیره شود؛ زیرا امروزه با وجود فناوری و داده‌های بسیار در صنعت مراقبت‌های پزشکی، امنیت داده‌های پزشکی بیمار جزو اصول اولیه محسوب می‌شود. همچنین تعدادی از پژوهش‌گران به این نتیجه رسیده‌اند که استفاده از فناوری زنجیرهٔ بلوکی در بهداشت و درمان یک راه‌حل با عاقبت مطلوب و به‌طور کامل عملی است[۱۶].

۲-۲-۱-ساختار و معماری زنجیرهٔ بلوکی

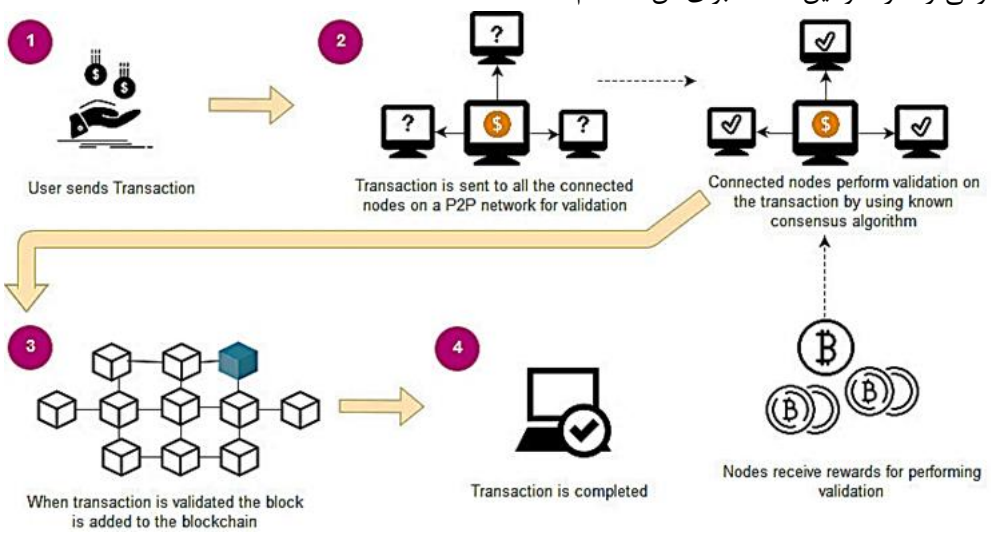
برای مشخص‌کردن معماری زنجیرهٔ بلوکی می‌توانید شکل (۱) را مشاهده کنید که در آن تمام روند ارسال تراکنش‌ها از یک کاربر در شبکهٔ زنجیرهٔ بلوکی مشخص شده‌است[۹].

۱. ابتدا یک تراکنش جدید که توسط یک کاربر در شبکهٔ زنجیرهٔ بلوکی ارسال می‌شود، مشخص‌کنندهٔ یک بلوک جدید خواهد بود.
۲. هر بلوک در زنجیرهٔ بلوکی برای نگهداری تراکنش‌ها در آن استفاده می‌شود و بلوک‌ها بین تمام گره‌های

[1] Blockchain
[2] Platform
[3] Hash
[4] Anonimity

[DOI: 10.61186/jsdp.21.3.149]

متصل به شبکه به اشتراک گذاشته می‌شوند؛ بنابراین تراکنش‌هایی که در داخل بلوک‌ها قرار داده شده‌است بین تمام گره‌های شبکه توزیع می‌شود. تمام گره‌های موجود در شبکه یک نسخهٔ کامل از زنجیرهٔ بلوکی را دارند و این نسخه برای آن‌ها حکم مرجع را دارد و برای تأیید تراکنش‌ها مورد استفاده قرار می‌گیرد. در زمانی که بلوکی که حاوی تراکنش کاربر است در گره‌های متصل به شبکه پخش می‌شود، توسط آن‌ها مورد تأیید قرار می‌گیرد تا



(شکل-۱): مروری بر معماری زنجیرهٔ بلوکی [۹]
(Figure-1): An overview of blockchain architecture [9]

مشخص شود که دست‌کاری صورت نگرفته باشد. اگر رأی عدم دست‌کاری با موفقیت روبه‌رو شود، بلوک به نسخهٔ گره‌ها از زنجیرهٔ بلوکی اضافه می‌شود[۲].

سازوکار اضافه‌کردن بلوک به زنجیرهٔ بلوکی به‌وسیلهٔ تمام گره‌های متصل به شبکه صورت می پذیرد؛ یعنی تشخیص اعتبار بلوک برای اضافه‌شدن در زنجیرهٔ بلوکی یک تصمیم همگانی است و باید بر روی آن اتفاق نظر پیدا کنند. به‌دلیل اعتبارسنجی چندتایی این روش از نظر امنیتی بسیار قدرتمند است، اما نیاز به ارتباطات کمابیش زیاد و سربار محاسباتی نیز دارد که البته اندازهٔ آن قابل تحمل و حتی قابل چشم‌پوشی است. برای فرایند اعتبارسنجی از برخی الگوریتم‌های شناخته‌شده در تأیید تراکنش و اطمینان از فرستنده استفاده می‌شود. در زمانی که گرهی موفق به اجرای اعتبارسنجی و در اصطلاح استخراج[1] شد، گره با ارز رمزپایه پاداش می‌گیرد؛ به این گره‌ها، گره استخراج‌کننده[2] می‌گویند[۵].

۳. زمانی‌که اعتبارسنجی تراکنش با موفقیت انجام گرفت، بلوک مربوط به آن به زنجیره اضافه می‌شود.
۴. تراکنش با شرط موفقیت در اجرای مراحل قبلی، به اتمام می‌رسد.

[1] mining
[2] miner

برخی از واژه‌های مهم فناوری زنجیرهٔ بلوکی در ادامه توضیح داده شده‌اند:

۲-۲-۲-بلوک‌ها

چنان‌چه تاکنون بیان شد، زنجیرهٔ بلوکی از تعدادی بلوک پشت‌سر هم و به‌هم پیوسته تشکیل شده‌است که در یک شبکهٔ نظیربه‌نظیر توسط گره‌های آن به‌هم پیوند داده می‌شود و زنجیره را تشکیل می‌دهد؛ درنتیجه ساختاری غیرمتمرکز دارد. سربرگ این بلوک‌ها از درهم‌سازی بلوک‌های قبلی ساخته می‌شود. بلوک‌ها شامل سه قسمت دادهٔ اصلی، درهم‌سازی بلوک فعلی و درهم‌سازی بلوک قبلی هستند. داده‌های اصلی با توجه به نوع زنجیرهٔ بلوکی و کاربرد آن متغیر است. برای مثال در مورد بیت‌کوین، داده‌ها ارزهایی هستند که درواقع پول نقد الکترونیکی را شامل می‌شوند[۱۵]. درهم‌سازی مورد استفاده در این بلوک‌ها الگوریتم درهم‌سازی SHA-256 است و این درهم‌سازی برای شناسایی منحصربه‌فرد یک بلوک روی زنجیره به‌کار می‌رود.

۲-۲-۳-الگوریتم اجماع[3]

بر طبق قاعده بلوک‌هایی که به زنجیرهٔ بلوکی اضافه می‌شود، باید از برخی قوانین رعایت کنند تا بتوان آن‌ها را در زنجیره اضافه کرد. به عمل اضافه‌کردن بلوک‌ها به

[3] consensus

[DOI: 10.61186/jsdp.21.3.149]

زنجیره با قواعد خاص آن الگوریتم اجماع می‌گویند؛ از رایج‌ترین الگوریتم‌های اجماع قابل استفاده در زنجیرهٔ بلوکی الگوریتم اثبات کار[1] (PoW) را می‌توان نام برد که Nakamoto [15]، در شبکه بیت‌کوین مورد استفاده قرار داد. وظیفهٔ اصلی الگوریتم این است که هنگام درخواست اجرای تراکنش به‌وسیلهٔ گره‌های موجود، با توجه به گره‌ها یا شرکت‌کنندگانی که در یک شبکهٔ نظیربه‌نظیر در زنجیرهٔ بلوکی وجود دارد، محاسبات لازم را انجام دهد. فرایند محاسبات در این سامانه همان استخراج[2] است و استخراج‌کننده‌ها گره‌هایی هستند که در این محاسبات شرکت می‌کنند[۱۷].

۲-۲-۴-ویژگی‌های ممتاز زنجیرهٔ بلوکی

۱) توزیع‌شدگی[3] و نبود مرکزیت واحد:

در زنجیرهٔ بلوکی، ذخیره‌سازی و بهره‌برداری از اطلاعات و پردازش‌ها هیچ نقطهٔ مرکزی ندارد و داده‌ها و فرایندها در شبکه توزیع می‌شوند؛ این امر در زمینهٔ مدیریتی نیز موجب می‌شود، کنترل اطلاعات و داده‌های مشترک بین گره‌های متصل به صورت توزیع‌شده صورت پذیرد. کنترل و نظارت بر داده‌ها به صورت توزیع‌شده به جای نقطهٔ واحد، موجب ایجاد اعتماد بالاتر می‌شود؛ زیرا همگان آن را قبول خواهند داشت[۶].

۲) شفافیت اطلاعاتی

ایجاد شفافیت اطلاعاتی در فناوری‌های مختلف، نیازمند وجود رابطهٔ مبنی بر اعتماد بین نهادهای موجود در آن فناوری است. اطمینان از ایمنی و صحت داده‌ها و مقاومت آن‌ها از شروط داشتن شفافیت اطلاعات است. با توزیع‌شدگی که در زمینهٔ داده‌ها وجود دارد در واقع می‌توان قابلیت اطمینان داده و در نهایت شفافیت داده را در شبکه ایجاد کرد به گونه‌ای که با اشتراک مالکیت داده از هرگونه مداخلهٔ شخص ثالث در داده‌ها جلوگیری می‌شود[۵].

۳) ایجاد صحت و حریم خصوصی

فناوری زنجیرهٔ بلوکی مانند بسیاری از فناوری‌های امن برای تأمین امنیت داده‌ها در بین گره‌های شبکه از توابع رمزنگاری استفاده می‌کند. الگوریتم معمول رمزنگاری مورد استفاده در آن، الگوریتم SHA-256 است که از آن بر روی هش‌هایی که در بلوک‌ها ذخیره شده‌اند استفاده می‌شود. SHA یک الگوریتم رمزنگاری مبتنی بر درهم‌سازی و مخفف الگوریتم درهم‌سازی کردن امن[4] است. درهم‌سازی ایجاد شده موجب امنیت زنجیرهٔ بلوکی می‌شود؛ زیرا تضمین صحت داده‌ها را برعهده دارد. استفاده از درهم‌سازی‌ها برای رمزنگاری محدودهٔ بزرگی را برای رمزها ایجاد می‌کند که قابل پوشش برای انواع داده‌های دیجیتال است و داده‌های دیجیتال را از دست‌کاری عمدی یا سهوی در فرایند استخراج محافظت می‌کند و از طرفی به‌دست‌آوردن اصل داده‌ها را در صورت نداشتن کلید رمز غیرقابل وصول می‌کند. این باعث می‌شود زنجیرهٔ بلوکی به‌عنوان یک سکوی توزیع‌شده از طریق الگوریتم رمزنگاری دارای حریم خصوصی شود و گزینهٔ مناسبی را برای ایجاد محرمانگی داده در بسیاری از کاربردها فراهم می‌کند[۹].

۲-۲-۵-چالش‌های زنجیرهٔ بلوکی

۱) دسترسی همگانی و قابلیت مقیاس‌پذیری

ذخیرهٔ توزیع‌شدهٔ داده در زنجیرهٔ بلوکی باعث بروز دو مسئلهٔ مهم می‌شود که شامل در دسترس‌بودن بیش از اندازهٔ داده‌ها و از طرفی کاهش مقیاس‌پذیری است. مشاهدهٔ داده‌های موجود در زنجیرهٔ بلوکی برای تمام افراد حاضر در زنجیره می‌تواند خطرناک باشد به‌گونه‌ای که با وجود استفاده از الگوریتم‌های درهم‌سازی و رمزنگاری، این امر می‌تواند موجب آسیب‌پذیرشدن داده‌ها شود که برای یک سیستم‌عامل غیرمتمرکز نتیجهٔ مطلوبی نیست. از طرفی نیز داده‌های زنجیرهٔ بلوکی در ساختار مراقبت و سوابق پزشکی متشکل از سوابق پرونده و بیماری افراد، داده‌های آزمایشگاهی، گزارش‌های مختلف، تصاویر تصویربرداری تشدید مغناطیسی[5] (MRI) و بسیاری از موارد دیگر است؛ در صورتی‌که بخواهد تمام این داده‌های حجیم در زنجیرهٔ بلوکی ذخیره شود ظرفیت انتقال داده و ذخیره‌سازی زنجیرهٔ بلوکی به‌شدت تحت‌تأثیر قرار می‌گیرد و مقیاس‌پذیری را کاهش می‌دهد[۱۸].

۲) دشواری درک برخی مفاهیم و نحوهٔ استفاده از آن برای افراد

چگونگی عملکرد فناوری زنجیرهٔ بلوکی برای تمام افراد به‌آسانی قابل درک نیست؛ بااین‌حال این فناوری همچنان به مسیر خود ادامه داده و مداوم با توجه به نیازمندی‌ها تغییر می‌کند که کار را برای افراد علاقه‌مند می‌تواند مشکل کند؛ علاوه‌براین،

[1] Proof of Work
[2] Mining
[3] distribution

[4] Secure Hashing Algorithm
[5] Magnetic Resonance Imaging

[DOI: 10.61186/jsdp.21.3.149]

تبدیل سامانه‌های EHR کنونی که در آن‌ها از زنجیرهٔ بلوکی استفاده نشده به فناوری مجهز به زنجیرهٔ بلوکی زمان‌بر خواهد بود؛ زیرا بیمارستان‌ها یا سایر مؤسسات مراقبت‌های پزشکی در برابر تغییرات با گستردگی زیاد مقاومت می‌کنند[۶].

۳) نبود استانداردهای مشخص جهانی

با وجود ظهور چندین سالهٔ این فناوری و طی‌کردن مراحل اولیه و پیشرفت مداومی که داشته‌است، تاکنون استاندارد جهانی مشخصی برای آن ارائه نشده‌است؛ درنتیجه پیاده‌سازی تمام و کمال آن در بخش مراقبت پزشکی نیازمند صرف زمان و هزینهٔ بیشتر است. یک استانداردسازی می‌تواند بسیاری از راه‌ها را کوتاه کند و فقدان آن موجب سرگردانی بین انواع پیاده‌سازی‌ها و فناوری‌های مختلف می‌شود [۱۹]. این استاندارد جهانی می‌تواند برای مصارف پزشکی به‌صورت جداگانه مطرح شود تا تصمیم‌گیری در مورد انواع، قالب‌ها و اندازهٔ داده‌هایی که می‌توانند در زنجیرهٔ بلوکی در نظام مراقبت پزشکی ذخیره شوند نیز به‌سادگی صورت پذیرد؛ علاوه‌براین، سازگاری این فناوری با ساختار پزشکی هر بیمارستان به‌دلیل استفاده از استانداردهای مشخص آسان‌تر خواهد شد؛ زیرا آن‌ها می‌توانند از قبل داده‌های خود را بر طبق استاندارد تعریف کنند[۹].

۲-۳-پژوهش‌های پیشین

تمام روش‌های اطلاعاتی جدید باید در یک سامانه اطلاعات و پردازش داده‌های پزشکی موفق حضور داشته باشند. پژوهش‌گران بر این باورند که دسترس‌پذیربودن این سامانه برای تمام کاربران یکی از عوامل موفقیت این سامانه‌هاست، اما این موضوع باعث می‌شود که حفظ محرمانگی داده‌ها پیچیده شود. استخراج داده‌ها در سامانه پزشکی همیشه برای اهداف بالینی مانند تشخیص و درمان کاربرد داشته‌است و در کنار آن مسئلهٔ ازدیاد احتمال افشای داده‌ها و اطلاعات افراد نیز وجود دارد.

پژوهش [۱۹] داده‌های بزرگ به‌عنوان یک پدیده که در دههٔ اخیر و به‌واسطهٔ پیشرفت‌های علمی و وجود حجم زیاد داده‌های الکترونیکی مطرح‌شده مورد بحث بوده و کاربردهای آن در مسائل پزشکی و دارویی مطرح شده‌است؛ همچنین مزیت‌ها و چالش‌های کاربرد مفاهیم داده‌های بزرگ در پزشکی و سلامت و روش‌های مختلفی که برای تحلیل داده‌های بزرگ پزشکی می‌تواند مورد استفاده قرار بگیرد و یا در گذشته پیشنهاد شده‌است، محوریت این مقاله را تشکیل می‌دهد.

پژوهش [۲۰] یک طرح اشتراک‌گذاری امن و حفظ حریم خصوصی در اطلاعات سلامت افراد[1] PHI مبتنی بر زنجیرهٔ بلوکی (BSPP[2]) برای پیشرفت تشخیص در سامانه‌های سلامت الکترونیکی ارائه داده‌است. در مرحلهٔ نخست، دو نوع زنجیرهٔ بلوکی، زنجیرهٔ بلوکی خصوصی و زنجیرهٔ بلوکی کنسرسیوم، با ابداع ساختار داده‌های خود و سازوکارهای اجماع ساخته می‌شوند. زنجیرهٔ بلوکی خصوصی مسئول ذخیرهٔ PHI است؛ درحالی‌که زنجیرهٔ بلوکی کنسرسیوم سوابق مربوط به شاخص‌های امن PHI را نگه می‌دارد. به‌منظور دست‌یابی به امنیت داده‌ها، کنترل دسترسی، حفظ حریم خصوصی و جستجوی ایمن، کلیهٔ داده‌ها از جمله PHI، واژگان کلیدی و هویت بیماران با کلید عمومی مبتنی بر جستجوی واژگان کلیدی رمزگذاری شده‌اند؛ علاوه‌براین، ژنراتورهای بلوک موظف‌اند اثبات مطابقت را برای اضافه‌کردن بلوک‌های جدید به کلکسیون‌ها ارائه دهند، که این امر دسترسی به سامانه را تضمین می‌کند. تجزیه و تحلیل امنیتی نشان می‌دهد که پروتکل پیشنهادی می‌تواند با برخی اهداف امنیتی مطابقت داشته باشد.

پژوهش‌های [۲۱]، [۲۲]، [۲۳]، [۲۴]، [۲۵] و [۲۶] نیز به نوعی سعی در امنیت و حفظ محرمانگی داده‌های سلامت پزشکی با استفاده از فناوری زنجیرهٔ بلوکی کرده‌اند. هر روش ایدهٔ خود را در این مورد اجرا کرده‌است؛ اگرچه در نهایت نقاط مشترک دارند و نقاط ضعف و قوت مشترک. مسئله این است که افراد درگیر با نظام سلامت در انتقال داده‌ها بر روی یک محیط عمومی، اطلاعات شخصی دارند که می‌تواند در معرض خطر قرار بگیرد. همچنین به‌کارگیری داده‌های این سامانه در امور خارج از نظام سلامت همچون Cloud-IoT و تأمین محرمانگی داده‌های سلامت الکترونیک در چنین شرایطی می‌تواند موضوع قابل توجهی باشد که بدان پرداخته نشده‌است.

در زمینهٔ بستر اینترنت اشیا به‌ویژه IoT-Cloud و امنیت و محرمانگی اطلاعات نیز پژوهش‌های بسیاری صورت گرفته‌است از جمله:

در مرجع [۲۷] به بیان پژوهشی با عنوان بررسی ارتباط رایانش ابری، کلان‌داده و اینترنت اشیا بیان کردند که رایانش ابری یک فناوری است که با هدف مرتفع‌سازی نیازهای مربوط به نگهداری سخت‌افزارهای محاسباتی گران‌قیمت فضای اختصاصی و نرم‌افزار به‌وجود آمد. این فناوری سازمان‌ها را قادر می‌سازد تا بدون درنظرگرفتن مسائل مرتبط با زیرساخت انعطاف‌پذیری و دردسترس‌بودن منابع، روی کسب‌وکار اصلی خود متمرکز

[1] Personal Health Information
[2] blockchain-based secure and privacy-preserving

[DOI: 10.61186/jsdp.21.3.149]

شوند. واژهٔ کلان‌داده نیز به داده‌هایی اطلاق می‌شود که حجم آن‌ها از داده‌های معمولی بسیار بزرگ‌تر بوده و پردازش و نگهداری آن‌ها به سادگی امکان‌پذیر نیست. این داده‌ها می‌توانند شامل موارد متعددی از جمله متون، تصاویر، کلیپ‌های ویدیویی و داده‌های گردآوری‌شدهٔ بسیاری از جمله داده‌های متنوع تولیدشده به‌وسیلهٔ اینترنت اشیا باشند. منظور از اینترنت اشیا اتصال اشیای فیزیکی به اینترنت و دستیابی به داده‌های حس‌گرهای بی‌سیم است که نتیجهٔ آن کنترل دنیای فیزیکی را ممکن می‌سازد. در این مقاله پس از معرفی ادبیات موضوع و تعاریف اولیه، ظهور و رشد کلان‌داده‌ها در رایانش ابری و چالش‌های به‌کارگیری این ترکیب از جنبه‌های گوناگون مورد بحث و بررسی قرار خواهد گرفت. در ادامه نیز توضیحاتی درخصوص کلان‌دادهٔ ایجادشده توسط اینترنت اشیا و فرصت‌های پژوهشی آینده در این زمینه ارائه می‌شود.

در مرجع [۲۸] به بررسی ساختار نسل پنجم دارای تأخیر کم برای خدمات و سرویس‌های مبتنی بر اینترنت اشیا پرداختند. در این پژوهش یک سرویس جدید ساختار نسل پنجمی که دارای تأخیر کم است برای اطمینان از اینکه از سرویس‌های نسل چهارم بهتر کار می‌کند؛ برای استفاده در شبکه‌های مختلف و همچنین برای استفاده در اینترنت اشیا مورد بررسی قرار گرفته‌است. شبکه‌های موبایل پهن باند، اینترنت‌های اشیای بسیار گسترده بیشترین کاربردهایی هستند که این نوع ساختارهای نسل پنجمی دارا هستند. درعمل یک سرویس مبتنی بر اینترنت اشیا مانند یک ماشینی که از دور کنترل می‌شود، یکی از مواردی هستند که می‌توانند بهترین مثال برای این استفاده باشند.

در مرجع [۲۹] به بررسی مدل همسایگی بر پایهٔ اعوجاج برای پیش‌بینی کیفیت سرویس خدمات ابری و خدمات اینترنت اشیا پرداختند. این پژوهش یک مدل بر پایهٔ اعوجاج اصلی را برای پیش‌بینی کیفیت سرویس آگاه از متن در خدمات اینترنت اشیا و خدمات ابری ارائه می‌دهد. راه حلی که ارائه شد اجازهٔ بهینه‌سازی کلی مؤثر را برای مدل‌های پارامتر داده‌است. المان‌های همسایگی و اطلاعات متنی در نتیجه‌ها مشارکت می‌کنند. درنهایت ثابت شد که استفاده از این مدل می‌تواند به شکل بسیار مؤثری مفید باشد و می‌توان با استفاده از این مدل کاری کرد که پیش‌بینی‌های مرتبط با سرویس‌های بر پایهٔ اینترنت اشیا به‌درستی مورد استفاده قرار داد.

در مرجع [۳۰] به بیان پژوهشی به‌عنوان بررسی سکوی MASSIF: یک سکوی ماژولار و معنایی برای ساخت سرویس‌های انعطاف‌پذیر مبتنی بر اینترنت اشیا پرداختند. با استفاده از روش‌های مختلفی که مورد بررسی قرار گرفت این سکو به‌عنوان روشی بسیار مناسب برای استفاده در اینترنت اشیا معرفی شد تا بتوان سرویس‌های مبتنی بر اینترنت اشیا را بهبود بخشید. درنهایت ثابت شده‌است که استفاده از این سکو می‌تواند برای سرویس‌های اینترنت اشیا مفید باشد.

در مرجع [۳۱] به بیان پژوهشی به‌عنوان بررسی خدمات اینترنت اشیا برای حل مشکلات در ویتنام پرداختند. در این پژوهش استفاده از خدماتی از اینترنت اشیا در حل مشکلات ویتنام مورد بررسی قرار گرفته‌است. در اینجا به بررسی کاربردی که اینترنت اشیا در ویتنام دارد: مانند ایمنی غذا، مدیریت ترافیک و مدیریت زباله‌ها و غیره پرداخته شده‌است، که این مشکلات نیازمند سرویس‌های اینترنت اشیا هستند. پژوهش‌گران در پژوهش‌های جدید سرویس‌های اینترنت اشیای خاصی را پیشنهاد می‌دهند تا با استفاده از این سرویس‌ها بتوان به شکل دقیقی این مشکلات را حل کرد.

در مقالهٔ [۳۴] پروتکلی با ویژگی مدیریت سه‌وجهی[1] و سلسله‌مراتبی اعتماد برای دستگاه‌های کلودلت[2] ابری به نام IoT-HiTrust برای شبکه‌های IoT در مقیاس بزرگ پیشنهاد و تحلیل کرده‌است. پروتکل مدیریت سلسله‌مراتبی سیار ابری اجازه می‌دهد دستگاه IoT اطلاعات مربوط به سرویس‌های خود را گزارش دهد و قابلیت اعتماد دستگاه IoT دیگر برای ترکیب و انتخاب خدمات را با پیروی از یک الگوی گزارش و پرس‌وجوی سادهٔ محلی، پرس‌وجو کند. در این پژوهش هم‌گرایی، دقت، و قابلیت انعطاف‌پذیری در برابر خود تبلیغی[3]، تبعیض[4]، بدگویی[5]، پرچین‌سازی[6] و حملات سرویس فرصت‌طلبانه[7] با وجود قطع متناوب شبکه به ابر بررسی شده‌است.

در مقالهٔ [۳۵]، خواص امنیت و اهداف مدیریت امنیت و اطمینان IoT مورد بررسی قرار گرفته، و یک بررسی در مورد پیشرفت‌های علمی کنونی در مورد اعتماد در شبکهٔ IoT انجام شده‌است؛ علاوه بر این، مسائل حل‌نشده را مورد بحث قرار داده، چالش‌های پژوهش مشخص شده و روند پژوهش‌های آینده را با

[1] 3-tier
[2] Cloudlet
[3] Self Promotion
[4] Discriminatory
[5] Bad Mouthing
[6] Ballot Stuffing
[7] Opportunistic Service Attacks

[DOI: 10.61186/jsdp.21.3.149]

پیشنهاد یک مدل پژوهش برای مدیریت امنیت جامع در IoT نشان داده‌است.

در مقالهٔ [۳۶] نویسندگان یک روش مدیریت امنیت نسبتا کارآمد و مقیاس‌پذیر برای اینترنت اشیا مبتنی بر مدیریت امنیت متمرکز محلی و توزیع‌شده سراسری با استفاده از زیرساخت‌های متن باز با نهادهای تأیید هویت و اعطای مجوز محلی بر روی دستگاه‌های لبه، ارائه می دهند. در این طرح در لبه سامانه‌های اینترنت اشیا یک دستگاه مجوزدهی وجود دارد که با یک دستگاه مجوزدهی در اینترنت نیز در ارتباط است.

مقاله [۳۷] یک مدل مدیریت اعتماد الهام‌گرفته از مغز مبتنی بر نوروفازی را برای ایمن‌سازی دستگاه‌های IoT و گره‌های رله و اطمینان از قابلیت اطمینان داده‌ها معرفی می‌کند. مسئله اطمینان از عملکرد شبکه در این مقاله به شکل مهمی مشخص شده‌است.

در مقالهٔ [۳۸]، طرح مدل‌سازی پایایی جدید برای محیط سرویس‌گرای IoT پیشنهاد شده‌است که هر دستگاه قابلیت‌های آن را به‌عنوان یک سرویس فراهم می‌کند و همچنین یک روتر می‌تواند داده‌ها را به سایر دستگاه‌ها منتقل کند. در این مقاله، IoT سرویس‌گرا به‌صورت سامانه متمرکز سرویس ناهمگون IoT[1] (CHISS) مدل‌سازی شده‌است.

مقالهٔ [۳۹] آن‌چه به معنای اطمینان از امنیت روترها توسط سازندگان شبکهٔ مرکز تجاری هوشمند[2] SBC است، تجزیه و تحلیل کرده و استفاده از مدل مارکوف را در دستور کار قرار داده‌است. برای حل مسئله معادلات دیفرانسیل Kolmogorov خطی، لازم است جمع‌آوری و تجزیه و تحلیل آمار در مورد خرابی نرم‌افزار و سخت‌افزار انجام شود و این نشان داد که لازم است از وسایل محافظت در برابر حملات هکرها با درجهٔ امنیت بالا استفاده شود؛ بااین‌حال، به‌دلیل آسیب‌پذیری نرم‌افزار دستگاه‌های شبکه، اغلب به نظر می‌رسد خرابی مدل مارکوف توسعه یافته، هم قابلیت اطمینان و هم امنیت شبکه SBC را درنظر می‌گیرد.

مقالهٔ [۴۰] یک چارچوب عمومی برای کاهش حملات صفر-روزه[3] در شبکهٔ IoT ارائه کرده‌است. رویکرد پیشنهادی مقاله از رفتارهای متداول دستگاه‌های IoT به‌عنوان مکانیسم شناسایی استفاده می‌کند و به دنبال آن یک پروتکل پیام هشدار و پروتکل به اشتراک‌گذاری داده‌های ضروری برای ارتباط قابل اطمینان را در هنگام حمله راه‌اندازی می‌کند.

در پژوهش [۴۲] چارچوبی به نام "PrivySharing" مطرح شد که چارچوبی مبتنی بر زنجیرهٔ بلوکی است. این روش حفظ حریم خصوصی و به اشتراک‌گذاری امن داده‌های اینترنت اشیا در یک محیط شهر هوشمند را در دستور کار قرار داده‌است. به ادعای نویسندگان طرح پیشنهادی آن‌ها از بسیاری جهات از استراتژی‌های موجود متمایز است. در این طرح سعی شده‌است با تقسیم شبکهٔ زنجیرهٔ بلوکی به کانال‌های مختلف، حریم خصوصی داده‌ها حفظ شود، جایی‌که هر کانال تعداد محدودی از سازمان‌های مجاز را شامل می‌شود و نوع خاصی از داده‌ها مانند سلامت، ماشین هوشمند، انرژی هوشمند یا جزئیات مالی را پردازش می‌کند؛ علاوه‌بر این، دسترسی به داده‌های کاربران در یک کانال با تعبیهٔ کنترلرهای دسترسی در قراردادهای هوشمند کنترل می‌شود. همچنین داده‌های درون کانال به ترتیب با استفاده از جمع‌آوری خصوصی اطلاعات و رمزگذاری، جدا و ایمن می‌شوند. به همین ترتیب، REST API که مشتریان را قادر به تعامل با شبکهٔ زنجیرهٔ بلوکی می‌کند و دارای امنیت دوگانه در قالب API Key و OAuth 2.0 است، به‌کار گرفته شده‌است. طرح پیشنهادی مقاله سعی کرده مطابق با برخی از الزامات قابل توجهی باشد که در مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا ذکر شده‌است؛ همچنین یک سامانه پاداش در قالب یک رمز دیجیتالی به نام "PrivyCoin" برای کاربران به اشتراک‌گذاری داده‌های خود با سهام‌داران / اشخاص ثالث ارائه داده‌است.

در مقالهٔ [۴۳] نویسندگان طرح حفظ حریم خصوصی اشتراک اطلاعات انعطاف‌پذیر (FPDS) در اینترنت اشیا را به کمک ابر پیشنهاد داده‌اند. با استفاده از طرح FPDS، یک کاربر اینترنت اشیا می‌تواند با استفاده از رمزگذاری مبتنی بر هویت، داده‌ها را در یک گیرنده رمزگذاری کند. از همه مهم‌تر، کاربر اینترنت اشیا می‌تواند خط‌مشی دسترسی دقیق را برای اعطای اعتبار تفویض[4] مشخص کند. پس از آن این کاربران اعتبار مذکور را به ابر ارسال می‌کنند تا بتواند تمام داده‌های رمزگذاری‌شده را که از سیاست دسترسی برآورده می‌کنند، به متن‌های رمزگذاری‌شدهٔ جدیدی که برای گیرندهٔ جدید قابل خواندن هستند، تبدیل کند؛ به این ترتیب، کاربران اینترنت اشیا می‌توانند داده‌های برون‌سپاری‌شده به ابر را به روشی انعطاف‌پذیر و حفظ حریم خصوصی به اشتراک بگذارند.

پژوهش [۴۴] کمک‌هایی برای غلبه بر محدودیت‌های امنیتی ردیابی تماس انجام داده‌است: نخست، یک معماری حفظ حریم خصوصی را برای ردیابی تماس پیشنهاد داده‌است که از زیرساخت ثابت فرستنده‌های راهنمای

[1] Centralized, Heterogeneous IoT Service System
[2] smart business center
[3] zero-day
[4] Delegation

[DOI: 10.61186/jsdp.21.3.149]

بلوتوث با انرژی پایین[1] (BLE) استفاده می‌کند. دوم، امکان استفاده از راهنماهای BLE برای مصرف انرژی بدون باتری ارزیابی می‌کند تا این معماری پایدارتر و سبزتر شود. سرانجام، چالش‌ها و فرصت‌های پژوهشی عملی برای آکادمی و صنعت را شناسایی و معماری ردیابی تماس پایدار با کمک به حفظ حریم خصوصی را تحلیل کرده‌است. از آنجا که زیرساخت این سامانه IoT است، روش حفظ حریم خصوصی در این پژوهش برای ما می‌تواند اهمیت داشته باشد.

پژوهش [۴۵] به تمام جنبه‌های مهم کسب درآمد از اینترنت اشیا با تمرکز بیشتر بر صنعت مراقبت‌های بهداشتی و چالش‌های مربوطه مانند مدیریت داده‌ها، مقیاس‌پذیری، مقررات، قابلیت همکاری، امنیت و حفظ حریم خصوصی می‌پردازد؛ علاوه‌براین، یک معماری مرجع جامع برای اقتصاد داده‌های مراقبت‌های بهداشتی با یک مطالعهٔ موردی عمیق درمورد تشخیص و پیش‌بینی ناهنجاری‌های قلبی با استفاده از محاسبات چندطرفهٔ (MPC) و یادگیری ماشین با حفظ حریم خصوصی (PPML) ارائه داده‌است.

در پژوهش [۴۶] یک چارچوب غیرمتمرکز مبتنی‌بر زنجیرهٔ بلوکی با طرح‌های احراز هویت و حفظ حریم خصوصی برای ارتباطات ایمن در شبکه‌های حس‌گر بی‌سیمی (WSN) که اینترنت اشیا را شکل می‌دهد، پیشنهاد شده‌است. فرایند ثبت، صدور گواهی‌نامه و لغو برای ارتباط با گره‌های حس‌گر و ایستگاه پایه (BS) در یک محیط رایانش ابری استفاده می‌شود. در این طرح، سرخوشهٔ گره‌ها اطلاعات جمع‌آوری‌شده از آن‌ها را به BS هدایت می‌کند. درنتیجه، BS تمام پارامترهای اصلی را بر روی زنجیرهٔ بلوکی توزیع‌شده نگهداری می‌کند و مابقی داده‌ها که حجم بالایی دارند برای ذخیره‌سازی به ابرها هدایت می‌شوند. گواهی‌های لغوشده که متعلق به گره‌های مخرب‌اند، توسط BS از زنجیرهٔ بلوکی حذف می‌شوند.

پژوهش [۴۷] یک رویکرد برای افزایش حفظ حریم خصوصی در برنامه‌های مراقبت بهداشتی مبتنی بر اینترنت اشیا با استفاده از تکنیک‌های رمزگذاری هومومورفیک همراه با فناوری زنجیرهٔ بلوکی پیشنهاد می‌کند. رمزگذاری هومومورفیک، انجام محاسبات روی داده‌های رمزگذاری‌شده را بدون نیاز به رمزگشایی تسهیل می‌کند که درنتیجه آن از حریم خصوصی داده‌ها در طول فرایند محاسباتی محافظت می‌کند. داده‌های رمزگذاری‌شده را می‌توان توسط اشخاص مجاز بدون افشای محتوای واقعی، پردازش و تجزیه و تحلیل کرد؛ علاوه‌براین، قراردادهای هوشمند را در شبکهٔ زنجیرهٔ بلوکی برای اعمال کنترل دسترسی و تعریف سیاست‌های اشتراک‌گذاری داده‌ها ترکیب می‌کند. قراردادهای هوشمند تنظیمات مجوز دقیقی را ارائه می‌دهند که تضمین می‌کند فقط نهادهای مجاز می‌توانند به داده‌های رمزگذاری‌شده دسترسی داشته باشند و از آن‌ها استفاده کنند. این تنظیمات از داده‌ها در برابر مشاهده توسط اشخاص غیرمجاز محافظت می‌کند؛ همچنین، طرح ذکرشده یک رکورد ممیزی از تمام تراکنش‌های داده ایجاد می‌کند که هم پاسخ‌گویی و هم شفافیت را بهبود می‌بخشد.

در [۴۸] یک طرح احراز هویت متقابل حفظ حریم خصوصی برای سامانه‌های مراقبت بهداشتی مجهز به اینترنت اشیا برای دستیابی به احراز هویت سبک و مؤثر دستگاه‌های شبکه پیشنهاد شده‌است. برای پشتیبانی از قابلیت‌های پردازش دستگاه‌های اینترنت اشیا، این طرح احراز هویت پیشنهادی با استفاده از رمزنگاری‌های اولیهٔ سبک وزن، یعنی عملیات الحاق و درهم‌سازی و XOR طراحی شده‌است. به ادعای نویسندگان این طرح می‌تواند یک جلسهٔ امن بین یک دستگاه مجاز و یک دروازه ایجاد کند و از دسترسی دستگاه‌های غیرمجاز به سامانه‌های مراقبت بهداشتی جلوگیری کند.

در [۴۹] یک استراتژی ارتقای تشخیص عیب همراه با حفظ حریم خصوصی، برای سکوهای سلامت الکترونیک مبتنی بر فناوری زنجیرهٔ بلوکی مطرح شده‌است. پژوهش، یک روال کنترل دسترسی را پیشنهاد می‌کند که به مسئولین و مالکان داده‌ها اجازه می‌دهد کنترل‌های دسترسی مدنظر خود را بر داده‌های پزشکی حساس به حریم خصوصی خود مشخص کنند. کاربران می‌توانند از تراکنش‌های کاربر خود برای تولید کلید برای لغو یا اضافه‌کردن پزشکان مجاز استفاده کنند.

در مقالهٔ [۵۰] پیشنهاد شده‌است که یکپارچگی ایمن و حفظ حریم خصوصی IoT با واحدهای مراقبت‌های بهداشتی برای تحقق یک چارچوب نظارت بر بیمار ازراه‌دور[2] RPM قابل اعتماد، در دسترس و امن ارائه شود. بنا به ادعای پژوهش این چارچوب احراز هویت امن مبتنی‌بر RFID، ارتباطات امن سراسری و حفاظت از حریم خصوصی را فراهم می‌کند. چارچوب ارائه‌شده شامل ساعت MOTO 360 (بیو'ps حسگر/ حس‌گر بدن) با سیستم‌عامل پوشیدنی اندروید، سرور با چارچوب REST و یک برنامهٔ تلفن هوشمند برای نظارت و تشخیص سقوط، فشارخون و ضربان

[1] Bluetooth Low Energy

[2] Remote Patient Monitoring

[DOI: 10.61186/jsdp.21.3.149]

قلب است. این سناریوی انگیزشی با امنیت و حریم خصوصی ارتقا یافته‌است.

در [۵۱] بیان شده‌است که امروزه شاهد گسترش خدمات مختلف اینترنت اشیا در حوزه‌های مختلف از قبیل نظارت و سلامت هستیم. این خدمات از طریق دستگاه‌های هوشمند در هر مکان و زمانی می‌تواند در دسترس کاربران قرار گیرند؛ این در حالی است که این دسترسی‌ها می‌تواند مسئلهٔ امنیت و حریم خصوصی را به امری حساس و حیاتی تبدیل کند. در این مقاله یک پروتکل احراز هویت دوطرفه دستگاه‌به‌دستگاه برای شبکه‌های خانگی هوشمند، ارائه شده‌است. این پروتکل بر اساس رمزنگاری نامتقارن برای احراز هویت دستگاه‌های موجود در شبکه طراحی شده‌است و در آن تمامی دستگاه‌ها یک کلید جلسهٔ خصوصی مشترک دارند. برای حصول اطمینان از امنیت ارتباط‌ها در هر جلسه، کلیدهای جلسه پس از هر جلسهٔ ارتباطی تغییر می‌کنند. برنامه‌نویسی طرح پیشنهادی به‌وسیلهٔ HLPSL، شبیه‌سازی و ارزیابی بهینگی با ابزار SPAN و AVISPA انجام شده‌است. تحلیل‌های امنیتی نشان می‌دهد که پروتکل پیشنهادی در مقابل حملات امنیتی، پایداری خود را حفظ می‌کند.

در [۵۱] عنوان شده‌است که در محاسبات چندسویهٔ امن، گروهی از کاربران، نتیجهٔ یک تابع ریاضی را بر روی دادهٔ محرمانه خود، با حفظ حریم خصوصی داده‌ها محاسبه می‌کنند. در این پژوهش، مسئلهٔ جمع چندسویهٔ امن با قابلیت تکرار، بدون افزایش هزینهٔ محاسباتی و ارتباطی مورد توجه قرار گرفته‌است؛ در این مسئله هر کاربر چندین مقدار محرمانه دارد و اعضا قصد دارند مجموع داده‌های محرمانهٔ خود را به‌صورت نظیربه‌نظیر محاسبه کنند؛ به‌طوری که محرمانگی داده‌های هر کاربر حفظ شود. در این مقاله یک پروتکل کارا جهت محاسبه جمع چندسویهٔ امن با قابلیت تکرار در مدل شبه‌درست‌کار ارائه شده‌است. راه‌کار پیشنهادی، بدون نیاز به کانال امن، محرمانگی داده‌های کاربران و نتایج حاصل جمع را تأمین می‌کند و در مقابل تبانی جزئی کاربران تا سطح نفر ایمن و نسبت به روش‌های موجود، از نظر هزینهٔ محاسبات و ارتباطات بسیار کاراست.

در جدول (۱) مقایسه‌ای بین برخی روش‌های پیشین در این زمینه انجام شده‌است.

۳-ساختار پیشنهادی

پژوهش حاضر به حفظ حریم خصوصی در سامانه اینترنت اشیا برای انتقال داده‌ها در حوزهٔ مراقبت سلامت می‌پردازد. از تفاوت پژوهش حاضر با کارهای پیشین می‌توان حداقل به چندین مورد اشاره کرد. ابتدا اینکه هدف برخی پژوهش‌ها متفاوت است. این روش‌ها هدف این پژوهش را به‌منظور حفظ حریم خصوصی اینترنت اشیا در داده‌های سلامت، حداقل در یکی از بخش‌ها دنبال نمی‌کنند (بدون درنظرگرفتن روش به‌کاررفته)؛ سپس ساختار ارائه‌شده در این پژوهش که متشکل از پنج قسمت (کاربران، دستگاه‌های IoT، دستگاه‌های لبه، سرویس‌دهندهٔ امنیتی و رایانش ابری) است که در پژوهش‌های گذشته به تعداد و شکلی متفاوت بوده و بخش‌های آن نیز کمابیش به گونه‌ای متفاوت است. در پژوهش حاضر استفاده از زنجیرهٔ بلوکی برروی ارتباطات درون شبکهٔ اینترنت اشیا بدون اضافه‌کردن ساختار نظیربه‌نظیر و شبکهٔ هم‌پوشان اضافه انجام شده‌است. نحوهٔ استفاده از زنجیرهٔ بلوکی می‌تواند در نتیجهٔ آن تعیین‌کننده باشد و علاوه بر این داده‌ای که بر روی آن قرار داده می‌شود نیز کاربرد آن را تغییر می‌دهد. همچنین استفاده از الگوریتم احراز هویت از طریق دریافت گواهی‌نامهٔ X.509 و سامانه زیرساخت کلید عمومی[1] PKI بر روی لبهٔ ابر یک نوآوری در این زمینه به‌ویژه در این کاربر خاص است. محل احراز هویت بر روی لبه و بر روی سرور مربوطه، حفظ محرمانگی از طریق زنجیرهٔ بلوکی در ترکیب با رمزنگاری نامتقارن PKI، حفظ ناشناسی از طریق الگوریتم دیفی-هلمن و روال‌های تعریف‌شده برای عملکرد احراز هویت، رمزگذاری، انتقال برروی بستر زنجیرهٔ بلوکی از جمله دیگر تفاوت‌هایی است که این پژوهش را از پژوهش‌های دیگر متمایز می‌کند.

همچنین ذکر این نکته ضروری است که درکل حوزهٔ این پژوهش گسترده بوده و عناصر متفاوتی می‌تواند داشته باشد درحالی‌که پوشش تمام عناصر در یک پژوهش واحد غیرممکن است؛ بنابراین در این پژوهش نیز نمی‌توان ادعا داشت که کل حوزهٔ سلامت و امنیت را در تمام ابعاد آن پوشش می‌دهد؛ بلکه سعی شده بخش‌های مهمی را در این حوزه به همراه پیشنهاد یک ساختار مناسب پوشش دهد. به‌هرحال پژوهش‌هایی برای بررسی و مقایسه انتخاب شده‌اند که حداقل در یک عنصر با ساختار پیشنهادی اشتراک داشته باشند.

در این پژوهش سعی بر این است که با یک روش مبتنی بر زنجیرهٔ بلوکی و احراز هویت مناسب و پردازش در ابر لبه که پردازش اطلاعات و ارتباطات را سریع‌تر می‌کند، حفظ محرمانگی در داده‌های سلامت با کارایی قابل ملاحظه‌ای حاصل شود. این روش دارای پردازش و ذخیره‌سازی در شبکهٔ نظیربه‌نظیر در بستر ابر لبه است که از بخش‌های مهم برای حفظ محرمانگی است.

[1] Public key infrastructure

[DOI: 10.61186/jsdp.21.3.149]

سامانه پیشنهادی که تعداد قسمت‌های آن پیش‌تر نیز ذکر شد دارای پنج قسمت است:

۱ -کاربران (شامل بیمار، پزشک، پرستار و...)

۲ -دستگاه¬های IoT (شامل دستگاه‌های پایش سلامت، تلفن همراه، رایانه یا لپ‌تاپ کاربران)

۳ -دستگاه‌های لبه (شامل مودم ارتباطی، دستگاه‌های مجهز به سرویس مربوطه)

۴ -سرور امنیتی (که البته بخش مهمی از لبه محسوب می‌شود)

۵ -رایانش ابری برای ذخیره‌سازی نهایی و دسترسی ازراه‌دورشکل (۲) ساختار مورد نظر در طرح پیشنهادی را نشان می‌دهد. در شکل (۲) قسمت الف مدل ابر لبه مشخص شده‌است که در آن دستگاه‌های پزشکی و حس‌گرها به‌عنوان دستگاه‌های IoT در بخش پایین قرار گرفته‌است،

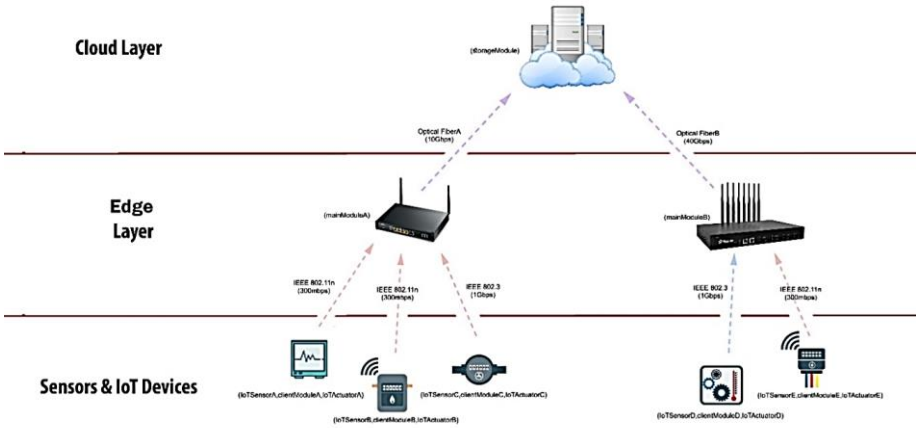
(جدول-۱): مقایسهٔ بین روش‌های پیشین

(Table-1): Comparision between before approaches

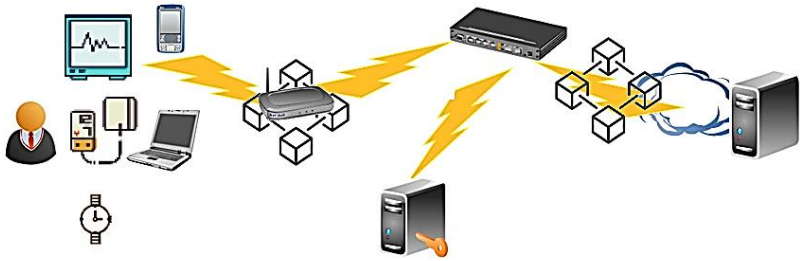
مرجع	هدف	ایده یا روش اجرایی	مزایا	معایب
[۵]	جریان‌یابی روان و مناسب داده از مدل اطلاعات به مدل RCPSP در برنامه‌ریزی ساخت+تطبیق با زمان‌بندی پروژه در وضعیت منابع محدود	مدل اطلاعاتی مبتنی بر بسته کاری- ادغام داده‌های چندمنظوره با یک روش نیمه‌خودکار+روش انتقال دادهٔ تطبیقی	یکپارچگی جریان داده-درنظرگرفتن محدودیت منابع	این روش با بهره‌گیری از رهیافت‌های هوشمند می‌تواند بهبود یابد. نیمه‌خودکاربودن موجب پیچیده‌شدن و سخت‌شدن پیاده‌سازی می‌شود
[۳۴]	افزایش قابلیت اعتماد در اینترنت اشیا مبتنی بر ابر	روشی سلسله‌مراتبی برای مدیریت دستگاه‌های سیار ابری به نام IoT-HiTrust با گزارش اطلاعات سرویس‌ها توسط دستگاه‌ها و انتخاب بر اساس پرس‌وجو	افزایش قابلیت اعتماد در برابر پدیده‌هایی مثل قطع ارتباط، خودتبلیغی، تبعیض، حملات سرویس فرصت‌طلبانه و غیره.	این روش با بهره‌گیری از رهیافت‌های هوشمند می‌تواند بهبود یابد. عدم توجه به امنیت پروتکل‌های به‌کارگرفته‌شده به‌ویژه گزارش‌دهی دستگاه‌ها.
[۳۷]	مدیریت اعتماد در دستگاه‌های IoT با اطمینان بالا از عملکرد شبکه	الهام از مغز به روش نوروفازی	ایمن‌سازی دستگاه‌های IoT و اطمینان از قابلیت اعتماد داده‌ها	عدم تأمین محرمانگی داده‌ها و حریم خصوصی
[۴۲]	حفظ حریم خصوصی داده‌ها (با دسته‌بندی‌های مختلف)	چارچوبی به نام PrivySharing با استفاده از زنجیرهٔ بلوکی، امنیت دوگانه در قالب API Key وOAuth 2.0 ، استفاده از رمز دیجیتالی برای اشتراک داده توسط کاربران	فراگیربودن، به‌کارگیری چندین مکانیزم در جهت پوشش وجوه مختلف مورد نیاز	کلی‌نگری و عدم توجه به داده‌های خاص و ویژگی‌های آن‌ها
[۴۳]	حفظ حریم خصوصی اینترنت اشیا برای داده‌های برون‌سپاری‌شده در ابر	رمزگذاری مبتنی بر هویت، مشخص‌کردن سیاست دسترسی برای اعطای اعتبار تفویض	انعطاف‌پذیری	عدم امکان اشتراک‌گذاری گروهی داده‌ها
[۴۴]	حفظ حریم خصوصی ردیابی تماس در اینترنت اشیا (بر روی گوشی‌های هوشمند) در مقابله با حملات استراق سمع	استقرار متراکم دستگاه‌های IoT بدون باتری که بسته‌های BLE را مداوم همه‌پخشی می‌کند.	هزینهٔ نگهداری کم، کاهش مصرف انرژی کاربر، بهبود دقت تخمین فاصله	هزینهٔ استقرار بالا، تک‌منظوره‌بودن، همه‌پخشی موجب ازدحام بالا در شبکه است و با افزایش تعداد دستگاه‌ها موجب اختلال زیاد می‌شود
[۴۷]	حفظ حریم خصوصی اینترنت اشیا در برنامه‌های پایش سلامت	استفاده از زنجیرهٔ بلوکی، رمزنگاری هومومورفیک	بهبود پاسخ‌گویی و شفافیت، کاهش زمان و برخی هزینه‌ها نسبت به روش‌های مورد مقایسه	کندبودن و پیچیدگی زیاد محاسبات رمزنگاری هومومورفیک، مقیاس‌پذیری پایین و حجم کم داده‌ها و تراکنش‌ها
[۴۸]	ایجاد امنیت در برابر برخی حملات و خطرات در مراقبت بهداشتی هوشمند با احراز هویت بر روی دستگاه‌های IoT، جلوگیری از دسترسی غیرمجاز بر روی	استفاده از احراز هویت متقابل، رمزنگاری سبک از طریق عملیات الحاق، درهم‌سازی و XOR	سادگی و سبکی، تنوع حملات مورد تقابل	مشکل ثبت کاربر ناشناس، سادگی عملیات رمز آن را در برابر هکرها ریسک‌پذیر می-کند

[DOI: 10.61186/jsdp.21.3.149]

مرجع	هدف	ایده یا روش اجرایی	مزایا	معایب
	سامانه مراقبت بهداشتی			
[۴۹]	حفظ حریم خصوصی در تشخیص عیب بر روی سکوی سلامت الکترونیک	استفاده از زنجیرهٔ بلوکی، کنترل دسترسی داده، محدودیت در حذف و تغییر داده	بهبود زمان و محاسبات نسبت به روش‌های پیشین، قوی‌بودن زنجیرهٔ بلوکی در حفظ محرمانگی	عدم تعیین بستر مناسب انتقال داده و ساختار ذخیره و بازیابی، عدم مقاومت در برابر برخی حملات از جمله حملات کوانتومی
[۵۰]	احراز هویت و حفظ حریم خصوصی در سامانه پایش الکترونیک و در زمان نظارت بر سلامتی بیماران	احراز هویت متقابل مبتنی بر RFID، رمزنگاری متقارن	عدم ردیابی کاربر، جلوگیری از حملهٔ پاسخ[1]، محرمانگی روبه‌جلو و روبه‌عقب	مشخص‌نبودن جزئیات بستر ذخیره‌سازی داده و تأمین امنیت آن، افزایش زمان انتقال داده به‌دلیل تعدد احراز هویت، هزینهٔ محاسباتی بالا
[۵۱]	احراز هویت کاربران در اینترنت اشیا به یکی از حساس‌ترین مفاهیم امنیتی تبدیل شده‌است.	طرح پیشنهادی به‌وسیلهٔ HLPSL، شبیه‌سازی و ارزیابی بهینگی با ابزار SPANو AVISPAانجام شده‌است.	حفظ پایداری در مقابل حملات امنیتی	زمان‌بر و هزینه‌بربودن پروتکل پیشنهادی
[۵۲]	از موارد پرکاربرد محاسبات چندسویهٔ امن، جمع چندسویهٔ امن است که هدف آن انجام عملیات جمع بر روی دادهٔ محرمانه کاربران است. در برخی کاربردها ممکن است، هر عضو چندین مقدارِ محرمانه داشته و هدف، محاسبهٔ مجموعِ داده‌های متناظر باشد؛ در این صورت لازم است پروتکلِ جمعِ چندسویهٔ امن، چندین‌بار برای محاسبهٔ مجموع داده‌های گروه تکرار شود.	پروتکل کارا جهت محاسبهٔ جمع چندسویهٔ امن با قابلیت تکرار در مدل شبه‌درست‌کار	تأمین محرمانگی بدون نیاز به کانال امن، هزینهٔ محاسبات و ارتباطات	مدل استفاده شده محدود است.



(الف)



(ب)

(شکل-۲): مدل مورد نظر و پیشنهادی الف) مدل رایانش لبه ب) ساختار کلی پیشنهادی

(Figure-2): A) Edge Computing Model. B) Proposed general structure

[1] Reply Attack

[DOI: 10.61186/jsdp.21.3.149]

در بخش بعدی به معرفی اجزای ساختار پیشنهادی پرداخته می‌شود. سپس فناوری به‌کار رفته در بخش‌های مختلف و روال‌های طرح مورد نظر معرفی می‌شود.

۳-۱-اجزای طرح پیشنهادی

پیش‌تر اجزای طرح پیشنهادی به صورت کلی بیان شد. در این بخش هر کدام از اجزا به شکل جداگانه معرفی می‌شود.

۱- کاربران

کاربران به‌طور معمول بخش مهمی از سامانه‌های کامپیوتری محسوب می‌شوند که این سامانه‌ها را کنترل می‌کنند و یا از آن‌ها برای رفع نیاز کاربر استفاده می‌شود. در طرح‌های پایش سلامت کاربران می‌توانند شامل بیماران (برای رفع نیاز نظارت و درمان آن‌ها)، پزشکان، پرستاران و یا پرسنل درمانگاه‌ها و مراکز پزشکی و بهداشتی (برای کنترل بیمار و دستگاه‌ها) باشند. نقش هر کدام از کاربران مجزا در سامانه تعریف می‌شود و دسترسی‌های خاص خود را خواهند داشت. در این بین بیماران در سامانه، دسترسی اصلی را برای اعمال محدودیت به اطلاعات ارسالی دارند؛ زیرا صاحبان اصلی داده‌ها هستند و مدیران مراکز پزشکی پس از آن دارای بالاترین دسترسی‌ها هستند. این دسترسی‌ها به‌وسیلهٔ یک سیستم کنترل دسترسی مانند Active Directory یا لیست‌های کنترل دسترسی[1] (ACL) قابل اعطا و کنترل است.

۲- دستگاه‌های IoT

دستگاه‌های IoT در طرح پایش سلامت شامل یک‌سری لوازم پزشکی به‌طور معمول مجهز به فرستنده/گیرنده رادیویی که به کاربر متصل می‌شوند، به همراه دستگاه‌های رایانه‌ای همچون لپ‌تاپ، گوشی هوشمند و تبلت می‌شود. این دستگاه‌ها در وهلهٔ نخست وظیفهٔ ارسال و دریافت اطلاعات را برای اطلاع‌رسانی و کنترل شرایط بیمار دارا هستند. در وهلهٔ بعدی به‌ویژه برای رایانه‌های کاربران، این دستگاه‌ها قابلیت مشاهده، کنترل و اعمال محدودیت بر روی اطلاعات توسط کاربران را فراهم می‌سازند.

۳- دستگاه‌های لبه

طرحیی که در این پژوهش برای پردازش اولیهٔ اطلاعات استفاده شده، استفاده از دستگاه‌های لبه است. ابتدا یک نکتهٔ حائز اهمیت است که در استفاده از پردازش لبه می‌توان دو نوع کاربر در سامانه تعریف کرد. ۱- کاربر منفرد و ۲- کاربر گروهی. کاربران منفرد، به‌طورمعمول بیماران خانگی تحت مراقبت در منزل هستند. برای این کاربران دستگاه‌های لبه نیازمند پیچیدگی خاصی نیست و می‌توان از دستگاه‌های اتصال به اینترنت مانند کامپیوتر یا مودم به‌عنوان سرور پردازش لبه استفاده کرد. درکل سعی بر این است که کاربران چندان درگیر پیکربندی سامانه نشوند و درنتیجه مثلاً تنها با نصب یک واسط و ماژول نرم‌افزاری بر روی یک سامانه یا استفاده از یک مودم با قابلیت مورد نظر، این امکان برای کاربران خانگی فراهم می‌شود، اما کاربران گروهی کاربران مستقر در مراکز درمانی و بیمارستان‌ها هستند که این کاربران به‌علت پیچیدگی بیشتر دسترسی به سامانه، نیازمند بهره‌مندی از دستگاه‌های مجهزتر با قابلیت بالاترند. همچنین پردازش‌های سنگین‌تری در این سامانه وجود دارد که در نتیجهٔ استفاده از یک طرح معمولی پاسخ‌گوی نیازمندی نخواهد بود.

۴- سرویس‌دهندهٔ امنیتی

سرویس‌دهندهٔ امنیتی با اینکه جزئی از لبه به‌شمار می‌آید، اما به‌دلیل اهمیت آن و وظیفهٔ مهمی که دارد جداگانه و به‌عنوان یک بخش مستقل از سامانه مورد بررسی است. این سرویس‌دهنده در کاربران منفرد می‌تواند به‌صورت ماژول نرم‌افزاری یا سخت‌افزاری به سامانه الحاق شوند، اما در کاربران گروهی سرویس‌دهندهٔ جداگانه دارد و البته همان سرویس‌دهنده نیز با روش‌های قابلیت اطمینان مانند افزونگی و پشتیبان‌گیری محافظت می‌شود. این سرویس‌دهنده صدور گواهی امنیتی و کنترل فرایندهای احراز هویت و ارتباطات را در سامانه با فناوری زنجیرهٔ بلوکی بر عهده دارد.

۵- رایانش ابری

رایانش ابری در سامانه پیشنهادی وظیفه ذخیره‌سازی نهایی داده‌ها به‌صورت زنجیرهٔ بلوکی را برعهده دارد. همچنین کنترل نهایی صحت داده‌ها برعهدهٔ آن خواهد بود. رایانش ابری به سامانه امکان دستیابی و گسترش هر چه بیشتر می‌دهد؛ یعنی برای مثال می‌توان چندین مرکز را هم‌زمان در سامانه داشت و به‌صورت مشترک، اما امن از داده‌ها استفاده کرد؛ همچنین موجب می‌شود که یک

[1] Access Control List

[DOI: 10.61186/jsdp.21.3.149]

کنترل مناسب و سطح بالا بر روی داده‌ها اعمال شود و از طرفی امکان دستیابی به قابلیت نظارت بر روی سامانه از دید بالاتر را اضافه می‌کند. به‌هر صورت استفاده از رایانش ابری در سامانه، منافع بالایی به‌همراه خواد داشت و البته برخی چالش‌ها را نیز ایجاد می‌کند که تا حد زیادی می‌توان با تکنیک‌ها و فرایندهای به‌کار گرفته‌شده، رفع و رجوع شوند.

۲-۳-فرایند زنجیرهٔ بلوکی

ارتباطات و داده‌ها دو مفهوم مهم در یک سامانه رایانه‌ای-شبکه‌ای هستند و نیاز به بهره‌گیری از روش‌هایی برای امن‌کردن آن‌ها وجود دارد. از آنجا که در این پژوهش به‌ویژه بر روی محرمانگی تأکید بسیاری شده‌است؛ بنابراین؛ روالی برای تأمین آن درنظر گرفته شده‌است که بتواند پاسخ‌گوی نیازمندی‌های پایش سلامت پزشکی الکترونیک باشد. در حوزهٔ سلامت داده‌ها باید در اختیار خود بیمار، پزشک معالج و پرستار شخص و همچنین پرسنل مراکز درمانی قرار بگیرد. تمام این جابه‌جایی اطلاعات از دستگاه‌های متصل به بیمار تا فرد مورد نظر در ساختار پزشکی یا از طریق شبکهٔ داخلی یا بر بستر اینترنت صورت می‌گیرد که در هر حالت نیاز به بهره‌گیری از فرایند احراز هویت و رمزنگاری وجود دارد.

در این پژوهش زنجیرهٔ بلوکی روشی عمده برای امن‌سازی ارتباطات و داده‌ها محسوب می‌شود که در کنار آن نیازمند عملیاتی همچون احراز هویت و رمزنگاری هستیم. در فرایند زنجیرهٔ بلوکی داده‌ها در ساختار بلوکی و در قالب بلوک‌های داده جابه‌جا می‌شوند. هر گره در شبکه مجهز به گواهی اعتباری است که به‌وسیلهٔ سرور امنیتی اعطا می‌شود. از طرفی هر بلوک از داده نیز به یک رشته کاراکتری به نام درهم‌سازی نیاز دارد تا بتوان صحت و امنیت آن را مشخص کرد. این درهم‌سازی توسط توابع درهم‌سازی در هر گره و برای هر بلوک از داده تولید می‌شود. روش مورد استفاده برای درهم‌سازی در این سامانه چنان‌چه پیش‌تر نیز اشاره شد روش SHA2 است.

هنگامی که یک بیمار یا دستگاه‌های متصل به بدن او به‌عنوان مبدأ نیاز به ارسال داده به مرکز پزشکی یا یک پزشک خاص به عنوان مقصد را داشته باشد، لازم است که ابتدا فرایند احراز هویت صورت پذیرد که در بخش بعد بیان می‌شود. در نتیجهٔ این فرایند یک نشست بین مبدأ و مقصد شکل می‌گیرد؛ البته این فرایند می‌تواند از سمت پزشک یا مرکز درمانی (به مقصد بیمار) نیز آغاز شود و در اصل قضیه تفاوتی نمی‌کند. سپس داده‌ها از طریق فرایند زنجیرهٔ بلوکی و با توجه به رمزنگاری از طریق کلید خصوصی کاربر ارسال می‌شود. هر بلوک از داده‌ها دارای یک درهم‌سازی و یک امضا از طریق رمزنگاری با کلید خصوصی است که گره‌ها می‌توانند پس از رمزگشایی از پیام با کلید عمومی گره، آن را مشاهده کرده و پس از محاسبهٔ درهم‌سازی پیام، آن دو را با هم مقایسه کنند و از صحت اطلاعات ارسالی باخبر شوند. در طول نشست پیام‌ها در غالب بلوک‌های داده ارسال می‌شوند و زنجیرهٔ بلوکی را تشکیل می‌دهند. هر زنجیرهٔ بلوکی شامل درهم‌سازی بلوک‌های قبل از خود است که می‌تواند تضمین‌کنندهٔ مبدأ درست و نیز صحت پیام‌های ارسالی باشد. همچنین صحت توالی پیام‌ها نیز بدین ترتیب چک می‌شود تا داده‌ها مطابق با زمان تولید آن‌ها در مقصد بازیابی شوند.

کلید عمومی کلیهٔ گره‌ها در یک شبکهٔ محلی در لبه ذخیره‌سازی می‌شود و به‌راحتی قابل بازیابی است، اما کلید عمومی اگر مربوط به شبکهٔ دیگر باشد، از سمت لبه قابل پیگیری است که درخواست به ابر داده می‌شود. در ابر تمام کلیدهای عمومی ذخیره شده و قابل دستیابی است. همچنین تمام بلاک‌های داده و درهم‌سازی آن‌ها نیز به‌وسیلهٔ لبه به ابر ارسال می‌شود تا در ابر ذخیره‌سازی شود و در صورت نیاز به داده‌های بیمار، بازیابی شود.

۳-۳-احراز هویت در لبه

هرگاه در شبکه‌ای بتوان کلیدهای عمومی افراد را به روشی امن به‌دست آورد می‌توان احراز هویت را به روشی ساده‌تر مبتنی بر «رمزنگاری کلید عمومی» پیاده‌سازی کرد. برای مثال فرض کنید مؤسسه‌ای (مثل دانشگاه یا بانک) برای کاربران خود گواهی‌نامه X.509 صادر و ساختار PKI[1] خود را راه اندازی کرده باشد و این مؤسسه دستگاه‌های اینترنت اشیا را مورد استفاده قرار دهد. بدین‌ترتیب در شبکهٔ یک یا چند سرویس‌دهندهٔ مشخص برای توزیع کلید عمومی یا گواهی‌نامهٔ دیجیتالی وجود دارد؛ در چنین شرایطی می‌توان از الگوی شکل (۳) برای احراز هویت کاربران یا دستگاه‌ها بهره گرفت. در این شکل فرض کنید «کاربر یا دستگاه A» (برای مثال آلیس یا یک حس‌گر دما) برای انتقال داده می‌خواهد نشستی را با «دستگاه B» با کاربری باب به عنوان سرویس‌دهنده ترتیب بدهد که این سرویس‌دهنده می‌تواند روی ابر باشد و یا به‌صورت محلی وجود داشته باشد. صدور گواهی و کنترل در این بخش برعهدهٔ سرویس‌دهندهٔ امنیتی بر روی لبه است.

روال کار به شرح زیر خواهد بود که در آن نوآوری در نحوه و محل به‌کارگیری این روش است:

[1] Public Key Infrastructure

[DOI: 10.61186/jsdp.21.3.149]

۱. در نخستین گام، «کاربر یا دستگاه A» باید از سرویس‌دهندهٔ توزیع کلید عمومی، تقاضای دریافت کلید دستگاه B را بدهد. هرگاه ساختار، مبتنی بر PKI بنا نهاده شده باشد او می‌تواند با دریافت گواهی‌نامهٔ دیجیتالی صادره برای دستگاه B (کاربر باب)، آن را اعتبارسنجی کند، سپس کلید عمومی دستگاه B (کاربر باب) را از درون گواهی‌نامه به‌دست آورد.

۲. در این مرحله نیز فرض شده که کاربر A به روشی مطمئن، کلید عمومی مندرج در گواهی‌نامهٔ دیجیتالی باب را به‌دست آورده و قادر است به کمک آن اطلاعاتی را رمز کند و برای دستگاه B بفرستد.

۳. در پیام سوم، کاربر A شناسهٔ کاربری خود (A) و عدد تصادفی RA را در یک ساختمان دادهٔ مشخص قرار داده‌است و آن را به کمک کلید عمومی دستگاه B (EB) رمزنگاری و ارسال می‌کند. بدیهی است که هیچ کسی جز خود کاربر B (باب) قادر به رمزگشایی این پیام نیست.

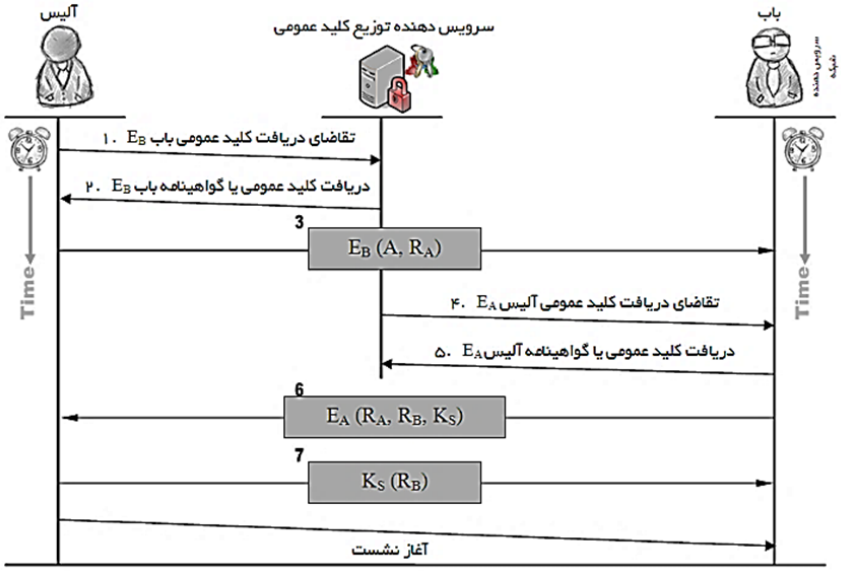
۴. باب پس از رمزگشایی پیام سوم با کلید خصوصی خود، شناسهٔ کاربر A و رشته چالش او را استخراج می‌کند و چون برای پاسخ به کاربر A، کلید عمومی او را نیاز دارد؛ به همین دلیل او نیز در پیام چهارم از سرویس‌دهندهٔ توزیع کلید، کلید عمومی یا گواهی‌نامهٔ کاربر A را تقاضا می‌کند.

۵. پس از دریافت کلید عمومی یا گواهی‌نامهٔ کاربر A، شرایط برای ارسال اطلاعات رمزنگاری‌شده مهیاست.

۶. در این پیام، باب سه آیتم: RA (رشته چالش ارسالی توسط کاربر A)، RB (رشته چالش خودش) و KS (کلید نشست برای استفاده از آن در رمزنگاری متقارن داده‌ها) را در یک ساختمان دادهٔ مشخص قرار می‌دهد و حاصل را به کمک کلید عمومی کاربر A، رمزنگاری می‌کند و آن را برای او پس می‌فرستد. به‌طور طبیعی تنها کسی که قادر به رمزگشایی و بازخوانی این آیتم‌ها خواهد بود، شخص کاربر A (آلیس) است.

کاربر A پس از رمزگشایی داده‌ها، ابتدا با بررسی R_A و مقایسهٔ آن با رشته چالش ارسالی به این نتیجه می‌رسد که این پاسخ با درخواست او تطابق دقیق دارد یا خیر؟ بدین ترتیب تازه‌بودن پیام اثبات و از حملهٔ تکرار جلوگیری می‌شود. حال باید با ارسال R_B که با کلید نشست K_S رمزنگاری شده، به دستگاه B ثابت کند که او نیز یک کاربر فعال و واقعی است و پیام سوم، پیامی تکراری نبوده‌است. بدین ترتیب نشست بین باب و آلیس با کلید نشست K_S آغاز خواهد شد.

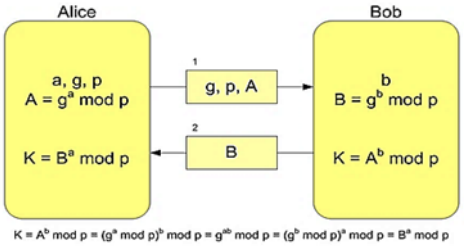
تنها کاری که یک فریب‌کار می‌تواند انجام بدهد آن است که پیام سوم را استراق سمع کند و سپس آن را از طرف کاربر A برای دستگاه B بفرستد، اما از آنجا که کلید خصوصی کاربر A را نمی‌داند قادر به رمزگشایی پاسخ دستگاه B نیست و نمی‌تواند در مرحلهٔ هفتم نشست را تکمیل کند. از طرفی فرض شده‌است که کاربر A و دستگاه B کلید عمومی یکدیگر را به روشی به‌دست آورده‌ان؛ لذا هرگونه تقلب در جعل کلید عمومی کامل بی‌ثمر خواهد بود.



(شکل-۳): احراز هویت در روش پیشنهادی با دریافت گواهی‌نامهٔ X.509 و ساختار PKI

(Figure-3): Authentication in the proposed method with X.509 certificate and PKI structure

[DOI: 10.61186/jsdp.21.3.149]



(شکل-۴): نحوهٔ اشتراک کلیدها در شبکه به روش دیفی هلمن

(Figure-4): How to share keys on the network using the Diffie Hellman method

طرف اول		
پنهان	محاسبه	ارسال
	g ،p	
a		
		g^a mod p
	...	
	$(g^b \bmod p)^a \bmod p$	

طرف دوم		
پنهان	محاسبه	ارسال
	g ،p	
b		
	...	
		g^b mod p
	$(g^a \bmod p)^b \bmod p$	

(شکل-۵): نحوهٔ رمزنگاری کلید و مبادلهٔ کلید در دو طرف

(Figur- 5): How to encrypt the key and exchange the key on both sides

۴-۳-تبادل کلید با روش دیفی-هلمن

در روش پیشنهادی در این پژوهش از تبادل کلید دیفی-هلمن[1]، در فرایند احراز هویت به منظور رسیدن به هدف تطبیق اساسی در برآورده‌کردن امنیت استفاده شده‌است؛ این روش یک پروتکل رمزنگاری است که با استفاده از آن، دو نفر یا دو سازمان می‌توانند بدون نیاز به هرگونه آشنایی قبلی، یک کلید رمز مشترک ایجاد و آن را از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل کنند. این پروتکل، نخستین روش عملی مطرح‌شده برای تبادل کلید رمز در مسیرهای ارتباطی غیر امن است و مشکل تبادل کلید رمز در رمزنگاری کلید متقارن آسان می‌سازد. در فرمول‌های پیشنهادی اولیهٔ این پروتکل، از گروه هم‌نهشتی اعداد صحیح با پیمانهٔ عدد اول p و عمل‌گر ضرب اعداد صحیح استفاده شده‌است. در این گروه عددی، یک ریشه محاسبهٔ اولیه می‌شود که آن را با g نشان می‌دهد.

مقدار عدد اول به نام p (پیمانهٔ عمل ضرب) است و برای محاسبهٔ مقدار g میان دو طرف ردوبدل می‌شود. هر یک از دو طرف با استفاده از عمل توان پیمانه‌ای و مقادیر قبلی p و g و مقدار پنهانی یک مقدار جدید محاسبه (A)و برای طرف مقابل (B) ارسال می‌کند. طرف اول با استفاده از مقادیر p و g و a و B و طرف دوم با استفاده از مقادیر p و g و b و A و با همان عمل توان پیمانه‌ای مقدار جدیدی را محاسبه می‌کنند. مقدار جدید محاسبه‌شده چنان‌که فرمول نشان می‌دهد در دو طرف یکسان و همان کلید رمز مشترک است. مقادیر a و b و مقدار مشترک محاسبه‌شده، هرگز مستقیم از کانال ارتباط عبور نمی‌کنند. بقیه یعنی مقادیر p و g و A و B ازکانال ارتباطی عبور می‌کنند و برای دیگران قابل دسترسی‌اند. دشواری حل مسئلهٔ لگاریتم گسسته تضمین می‌کند که مقادیر a و b و مقدار کلید رمز مشترک، با داشتن مقدار اعداد دیگر در عمل قابل محاسبه نباشد.

۵-۳-روال‌ها

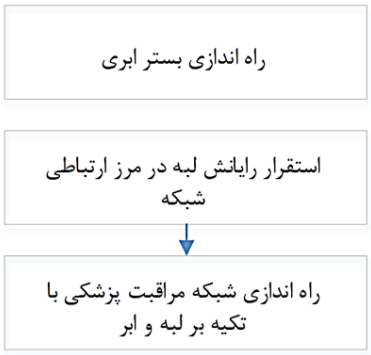
در بخش‌های قبلی بخشی از روال‌های موجود در روش پیشنهادی به‌صورت شماتیک بیان شدند. در ادامه ابتدا طرح کلی روش پیشنهادی به شکل نمودار مشخص و سپس مهم‌ترین الگوریتم‌های مربوطه بیان می‌شوند. در شکل (۶ الف) مراحل راه‌اندازی سامانه مشاهده می‌شود که ابتدا بستر ابری فراهم، سپس لبهٔ ابری و در انتها شبکهٔ مراقبت پزشکی با تکیه بر ابر و لبه راه‌اندازی می‌شود؛ به این دلیل که در هر مرحلهٔ پایین‌تر نیاز به احراز هویت است.

در شکل (۶ ب) روال کلی روش پیشنهادی برای تأمین امنیت انتقال داده‌های مراقبت پزشکی مشخص شده‌است؛ در این روال در مراحل اولیه احراز هویت قرار دارد که در ابر برای معرفی دستگاه‌های لبه و ایجاد اعتماد لازم است. در لبه نیز

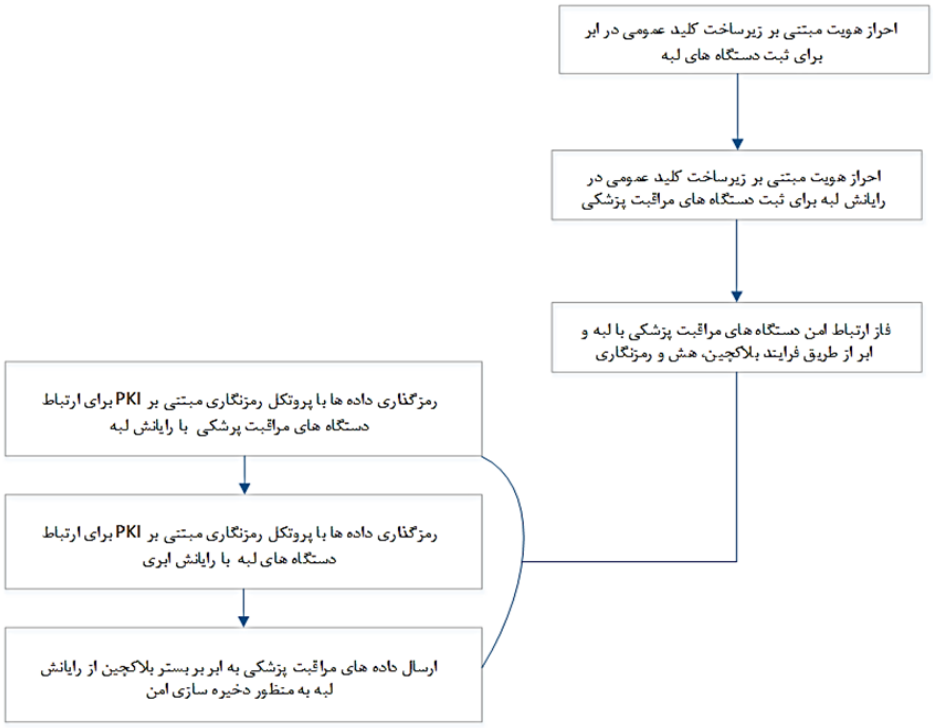
[1] Diffie-helman

[DOI: 10.61186/jsdp.21.3.149]

احراز هویت برای ثبت دستگاه‌های پزشکی صورت می‌گیرد که با استفاده از سرویس‌دهندهٔ امنیتی مستقر در لبه این امر انجام می‌شود. سپس وارد فاز ارتباط دستگاه‌های مراقبت پزشکی با لبه و ابر می‌شویم که از طریق فرایند زنجیرهٔ بلوکی و با استفاده از عملیات درهم‌سازی و رمزنگاری صورت می‌گیرد. این بخش از روال خود متشکل از سه بخش است. بخش نخست رمزگذاری داده‌های مراقبت پزشکی به‌دست‌آمده از این دستگاه‌ها برای ارسال بر روی لبه است؛ همچنین داده‌های ارسالی از سمت لبه نیز برای ارسال به ابر نیاز به رمزگذاری دارد و در انتها داده‌های رمزگذاری‌شدهٔ مراقبت پزشکی بر بستر زنجیرهٔ بلوکی از دستگاه‌ها و با واسطه لبه به سمت ابر ارسال می‌شوند؛ البته بستر زنجیرهٔ بلوکی کل این فرایند را پوشش می‌دهد و انتقال داده‌ها از طریق فرایند زنجیرهٔ بلوکی است. درکل مرحلهٔ سوم دربرگیرنده و کامل‌کنندهٔ دو مرحلهٔ قبلی است.



(شکل-۶ الف): مراحل راه‌اندازی سامانه
(Figure-1 A): System initialization steps



(شکل-۶ ب): روال کلی روش پیشنهادی در تأمین امنیت انتقال داده‌های مراقبت پزشکی
(Figure-1 B): The general procedure of the proposed method in securing the medical care data transmission

الگوریتم‌های زیر مشخص‌کنندهٔ برخی جزئیات روش پیشنهادی هستند. در بخش رمزگذاری پیام‌ها اگر کاربر بخواهد ناشناس باشد و برای مثال سؤالی را از پزشک بپرسد ابتدا باید از لبه، مجوز درخواست کند. درواقع تمام کاربران برای اینکه بتوانند ناشناس در سامانه فعالیت کنند این مجوز را نیاز دارند که در هر زمانی می‌توانند آن را با درخواست از لبه به‌دست بیاورند؛ سپس کاربر از تولید رمز نامتقارن و تبادل کلید دیفی-هلمن برای برقراری ارتباط امن و رمزگذاری‌شده استفاده می‌کند و در این مرحله کاربر مبدأ باید مجوز خود را ارائه کند و در غیر این

[DOI: 10.61186/jsdp.21.3.149]

صورت درخواست پذیرفته نمی‌شود. در صورت عدم تمایل به ناشناس‌بودن، کاربر (یا دستگاه مبدأ) کلید عمومی مخصوص خود را برای رمزگذاری پیام‌ها به‌کار می‌برد؛ بنابراین، الگوریتم رمزگذاری و ارسال داده به صورت زیر است:

```
Algorithm1 Enc_Data (Dta, BBH)
(1) If User select Anonimity
(2)    If User hasn't (Anonymus License AL)
         Request from Edge
         Get (AL)
         If it fails Return (Error!);
       End of If (2)
       Generate new asymmetric public-private key pair (Puk, Prk)
    Share the public key Puk with receiver via Diffie-Helman algorithm along with Anonymus License providing
    End of If (1)
        HashD ←Hash (Dta+BBH)
        SDta  ← Sign Dta with Puk and HashD
     End of If
    Return SDta

Algorithm2 Send_Data (i)
Hash (B0) = 0
If User isn't Authenticated (its not for Anonymus cummunication)
    Authenticate via Edge
    If it fails Return (Error!);
End of If

While (there is any data) and (Bli not Full)
 (1) If there is before Block Bli not send
       Data + Bli→ Bli
     Else
       Create new Bli
       Data → Bli
   End of If (1)
 End of While
 (2) If Hash (Bli-1) is not available
          Request from Edge
    End of If (2)
SData←Enc_Data (Bli, Hash (Bli-1))
Send (SData)
```

الگوریتم (۱) رمزگذاری داده را نشان می دهد و الگوریتم (۲) ارسال داده را که در آن قبل از ارسال تابع رمزگذاری فراخوانی می‌شود. برای استفاده از امکان ناشناس‌بودن اگر کاربر تاکنون مجوز نگرفته باشد، ابتدا درخواست مجوز ارسال می‌شود. اگر موفقیت‌آمیز بود یا مجوز داشت اقدام به تولید جفت رمز غیرمتقارن می‌کند. در هر صورت برای رمزگذاری داده ابتدا درهم‌سازی آن تولید و با کلید خصوصی به همراه درهم‌سازی تولیدشده رمز می‌شود؛ برای ارسال داده ابتدا کاربر باید احراز هویت شده باشد و اگر نتواند احراز هویت شود خطا برمی‌گرداند. سپس تا زمانی که داده‌ای وجود داشته باشد و بلوک حاضر ظرفیت کافی داشته باشد، داده به آن اضافه می‌شود. اگر بلوکی وجود نداشته باشد یا پر باشد، بلوک جدید ایجاد و داده به آن اضافه می‌شود. در انتها قبل از ارسال باید درهم‌سازی بلوک قبلی اگر موجود بود به داده اضافه شود و اگر نبود درخواست شود. بلوک و درهم‌سازی بلوک قبلی رمزگذاری شده و در پیغام قرار گرفته، ارسال می‌شود.

۴-ارزیابی روش پیشنهادی

برای ارزیابی عملکرد روش پیشنهادشده در مقایسه با روش‌های معمول در گذشته از شبیه‌سازی استفاده شده‌است. اجرای کامل روش پیشنهادی در محیط‌های واقعی نیازمند همگون‌سازی و هماهنگی بین نرم‌افزارهای گوناگون است که به‌دلیل نبود هماهنگی مناسب بین نرم‌افزارها و وجود ناسازگاری بین آن‌ها، پیاده‌سازی کامل آن در محیط‌های واقعی به‌سادگی میسر نیست[۱۶]، به این علت برای ارزیابی، روش شبیه‌سازی را انتخاب کرده‌ایم. در این بخش ابتدا داده‌ها و چارچوب محیط شبیه‌سازی توضیح داده خواهد شد؛ سپس به ارزیابی و مقایسهٔ روش پیشنهادی با روش‌های مطرح‌شده در پژوهش پیشین (مقالهٔ [۴۱] و [۴۹]) پرداخته می‌شود.

۴-۱-داده‌ها

در این پژوهش از داده‌های حس‌شده به‌وسیلهٔ حس‌گرهای شبکهٔ IoT در کنار داده‌های پزشکی برای بارگذاری در شبکهٔ شبیه‌سازی‌شدهٔ اینترنت اشیا و ابر استفاده شده که داده‌های پزشکی مورد استفاده بوده‌است. این داده‌ها مربوط به پایش افراد مبتلا به عوارض قلبی بوده و بر روی سیصد نفر نمونه‌گیری شده‌است. برای استانداردبودن، نرمال‌سازی یک روش مؤثر در این زمینه است. نمونه‌گیری در خود مؤسسه انجام شده‌است و از تمام نمونه‌های موجود که در اختیار قرار داده شده، بهره‌برداری شده‌است. همچنین این داده‌های بیماری قلبی شامل سیزده ویژگی مطابق جدول (۲) است. مجموعه‌دادگانی که در این پژوهش استفاده شده‌است متعلق به بنیاد درمانی کلیولند آمریکا و به نام مجموعه‌دادگان قلبی بنیاد درمانی کلیولند[1] [۵۳] شهرت دارد.

۴-۱-۱-نرمال‌سازی داده‌ها

چنان‌چه ذکر شد از نرمال‌سازی و محدودکردن داده‌ها برای استانداردکردن آن‌ها بهره گرفته شده‌است. ازآنجا که مقیاس داده‌های عددی با هم متفاوت است می‌توانیم آن‌ها را به فرم استاندارد تبدیل کنیم (در نرمال‌سازی استاندارد مقادیر کلی داده‌ها باید بین دو عدد مشخص انتخاب شوند). فرم استاندارد به این صورت است که تمام داده‌ها را با استفاده از فرمول زیر بین بازه d1 تا d2 قرار دهیم:

$$\overline{x} = \frac{(x - xmin)(d2 - d1)}{xmax - xmin} + d1 \qquad (۱)$$

[1] Cleveland Clinic Fundation Heart Disease Dataset (https://archive.ics.uci.edu/ml/datasets/heart+Disease)

[DOI: 10.61186/jsdp.21.3.149]

(جدول-۲): مشخصه‌های مجموعه‌دادگان قلبی کلیولند[۵۳]

(Table-2): Characteristics of the Cleveland Cardiac Data Collection [53]

شماره	نام	نوع	توضیحات
۱	Age	پیوسته	به سال
۲	SEX	گسسته	مرد= ۱ & زن= ۰
۳	Cp نوع درد قفسهٔ سینه	گسسته	آنژین صدری معمولی= ۱ & آنژین صدری غیرمعمول= ۲ قفسهٔ سینه بدون درد= ۳ & بدون علامت= ۴
۴	Trestbps	پیوسته	فشار خون در حال استراحت (mm Hg)
۵	Chol	پیوسته	میزان کلسترول (mg/dl)
۶	Fbs میزان قند خون بیش از ۱۲۰ (mg/dl)	گسسته	دارد= ۱ ندارد= ۰
۷	Restecg نتایج کاردیوگرافی در حال استراحت	گسسته	نرمال= ۰ & دارای اختلال موج ST-T = ۱ نشان از وجود احتمالی هیپرتروفی بطن چپ = ۲
۸	Thalach	پیوسته	حداکثر ضربان قلب
۹	Exang آنژین صدری ناشی از ورزش	گسسته	بله = ۱ خیر = ۰
۱۰	Old peak ST	پیوسته	فرورفتگی موج ST ناشی از ورزش نسبت به حالت استراحت
۱۱	Slope شیب اوج قسمت ورزش	گسسته	۱ -upsloping ۲ – flat - downsloping ۳
۱۲	Ca	گسسته	تعداد عروقی که توسط فلوروسکوپی علامت گذاشته شده‌اند، که بین ۰ تا ۳ متغیر است
۱۳	Thal حداکثر ضربان قلب در حالت ورزش	گسسته	نرمال = ۳ نقص ثابت = ۶ نقص برگشت پذیر = ۷

به‌طور معمول با توجه به استاندارد داده‌های نرمال d1=0 و d2=1 انتخاب می‌شود. در برخی از داده‌ها مانند داده‌های متنی، نرمال‌سازی نیاز نیست و امری غیرمعمول محسوب می‌شود؛ زیرا متن می‌تواند نامحدود باشد، اما درکل نرمال‌سازی (و محدودسازی داده‌های متنی) می‌تواند به عملکرد داده‌کاوی و بالابردن کارایی و دقت آن کمک کند؛ بدین‌ترتیب در مورد داده‌های متنی به‌طور معمول سعی می‌شود چند مقدار مشخص و محدود تعریف و در هر رکورد یکی از مقادیر انتخاب شود؛ همچنین برای چنین داده‌هایی از اعداد صحیح نیز به‌جای متن می‌توان استفاده کرد؛ باوجوداین، برخی داده‌های متنی مانند نام افراد و توضیحات از هیچ مقدار مشخصی تبعیت نمی‌کنند که بتوان محدودسازی کرد و فقط می‌توان برای آن‌ها برخی قوانین و قالب خاص تعریف کرد؛ برای مثال این‌که بیشتر از ده نویسه برای نام قرار داده نشود و در صورت بیشتربودن نویسه‌های انتهایی حذف شود. مجموعه‌دادهٔ مورد استفاده در این پژوهش با توجه به منبع آن نرمال است و داده‌های متنی آن نیز مطابق جدول با اعداد محدود نشان داده شده‌است.

۴-۲-محیط شبیه‌سازی

نرم‌افزار شبیه‌سازی که در این پژوهش مورد استفاده قرار گرفته‌است، نرم‌افزار شبیه‌ساز ns نسخهٔ ۲.۳۵ است که در آن از زبان‌های برنامه‌نویسی c++ و tcl استفاده شده‌است.

[DOI: 10.61186/jsdp.21.3.149]

سامانه iot، پردازش ابر و زنجیرهٔ بلوکی شبیه‌سازی‌شده در این پژوهش با استفاده از کدهای c++ است و همچنین سامانه امنیت مکمل شامل احراز هویت و رمزنگاری با دیفی-هلمن نیز همگی با این کدها اجرا و ارزیابی شده‌اند.

کلیات روش به‌کارگرفته‌شده در این پژوهش به این صورت است که در ابتدا با استفاده از نرم‌افزار سیگوین در ویندوز، ns2 به اجرا درآمده و با توجه به جریان‌های پیشنهادی افزایش امنیت، محیط با عملکرد این جریان به انتهای شبیه‌سازی رسیده و سپس مقادیر به‌دست‌آمده برای انجام محاسبات به‌وسیلهٔ دستورهای awk ارائه شده‌است.

۴-۳-پارامترهای شبیه‌سازی

سناریوی شبیه‌سازی عبارت است از مدل انرژی معمول شبکه‌های اینترنت اشیا پوشیدنی و در آن گره‌هایی که شعاع ارسال و دریافت آن‌ها حدود ۵m تا ۱۰m است و در فضای ۰.۵m * ۲m پخش شده‌اند. این گره‌ها با توان انتقال ۰.۰۳۶ وات با پهنای باند در کانال‌ها برابر بیست مگاهرتز قرار دارند. در مدل پخش گره‌ها در شبکه این کار یکنواخت درکل شبکه صورت می‌پذیرد و گره‌ها تصادفی در کل شبکه پخش می‌شوند.

برای نشان‌دادن میزان تأثیر روش پیشنهادی، مطالعهٔ نمونه برای ارزیابی بازدهی در محیط شبکه‌های سلسله‌مراتبی و خوشه‌بندی‌شدهٔ حس‌گر بی‌سیم را انجام دادیم. برای مدل‌سازی مدل انرژی به‌طور واقع‌بینانه از مدل انرژی که در شبیه‌ساز ns تعریف شده‌است، در شبیه‌سازی خود استفاده کردیم. گره‌های شبکهٔ حس‌گر در بدنهٔ اینترنت اشیا از نوع ذرات mica با تغییر در نرخ ارسال‌ها و دریافت‌ها برای شبیه‌سازی محیط ناهمگون هستند. جدول (۳) پارامترهای به‌کار رفته را در شبیه‌سازی نشان می‌دهد. این پارامترها به‌گونه‌ای به‌کار رفته‌اند که دیگر روش‌های قبلی که برای حمله در شبکه‌های اینترنت اشیا به‌کار رفته‌اند و در مقالات مربوطه گزارش شده‌اند، نیز قابل مقایسه باشند. در جدول (۴) نیز پارامترهای سخت‌افزاری به‌کارگرفته‌شده برای اجرای شبیه‌سازی مشخص شده‌است.

۴-۳-۱-معیارهای کارایی

• درصد دست‌یابی به اطلاعات مفید

نرخ دسترسی گره‌های غیرمجاز و مهاجم به اطلاعات موجود در یک شبکه یا رسانهٔ ذخیره‌سازی را گوییم.

$$UIAp = \frac{Info\ Accessed\ (by\ attackers)}{Whole\ Info} \quad (۲)$$

• گذردهی

$$Throughput = \frac{\mu}{t} \quad (۳)$$

μ: تعداد بیت‌های دریافت‌شده در t واحد زمان

برای کل شبکه برابر با میانگین گذردهی کل گره‌ها خواهد بود.

• تأخیر انتها به انتها[1]

$$D = T_d - T_S \quad (۴)$$

D: زمان تأخیر یک بسته

Td: زمان دریافت بسته در مقصد

Ts: زمان ارسال بسته در مبدأ

(جدول-۳): پارامترهای نرم‌افزاری شبیه‌سازی

(Table-3): Simulation software parameters

row	Parameter	Value
1	ناحیهٔ شبیه‌سازی	2 x 0.5 m^2
2	دامنهٔ انتقال گره‌های معمولی حس‌گر	5-10 m^2
3	پروتکل MAC	CSMA-CA
4	پهنای باند	20 Mhz
5	نیروی انتقال گره‌های معمول	0.036 W
6	نیروی دریافت گره‌های معمول	0.024 W
7	نیروی بیکاری	0.00006 W
8	تعداد گره‌ها	50-100
9	نوع لایهٔ پیوند (MAC)	802.11
10	پروتکل مسیریابی شبکه	LEACH
11	تعداد مهاجمان	10

(جدول-۴): پارامترهای سخت‌افزاری

(Table-4): Hardware parameters

#	نام سخت‌افزار	مدل
1	CPU	intel core i7 2.20Ghz
2	RAM	16G DDR3
3	HDD	1TB

۴-۴-تحلیل کارایی

پس از انجام شبیه‌سازی در خروجی نرم‌افزار علاوه بر اینکه هزینهٔ بهینه‌ترین برای تمام حالت‌ها محاسبه می‌شود، نتایج محاسبات، تعداد مهاجرت ماشین‌های مجازی، تعداد نقض SLA[2]، درصد نقض SLA و میانگین نقص SLA را مشخص می‌کنیم. در جدول ۵ کارایی روش پیشنهادی در برابر یک حمله DoS مشهود است.

دلیل مقایسه با روش‌های موجود DVFS[3] و DNS[4] مقایسهٔ کارایی در هنگام وجود یک حمله است که در صورت چنین شرایطی روش پیشنهادی چه عملکردی می‌تواند داشته باشد؛ درحالی‌که در شرایط مشابه کارایی حتی وجود طرح‌های کارآمد نیز نمی‌تواند شرایط مناسبی را در سامانه، لبه و محاسبات ابری در زمینهٔ سرویس‌های

[1] End-to-end Delay
[2] Service level agreement
[3] Dynamic Voltage and Frequency Scaling
[4] Dynamic Network Shutdown

[DOI: 10.61186/jsdp.21.3.149]

دریافتی ایجاد کند. در طرح DVFS زمانی که یک افزایش بار در سامانه ایجاد می‌شود (برای مثال زمان یک حمله) ولتاژ و فرکانس عملیاتی سرور یا سوئیچ افزایش پیدا می‌کند. درنتیجه در حد امکان سعی می‌شود از نقض SLA جلوگیری شود. در طرح DNS هنگامی که شبکه با افت بسیار زیادی روبه‌رو شود، به‌صورت موقت و خودکار عملیات آن خاموش می‌شود و سپس با افزایش درخواست‌ها و نیاز به افزایش منابع این امر صورت می‌پذیرد. درنتیجه در زمان حمله منابع بیشتری در اختیار قرار می‌گیرد تا نقض SLA وجود نداشته باشد.

(جدول-۵): مقایسهٔ طرح‌های کارآمد با روش پیشنهادی در رابطه با نقض SLA

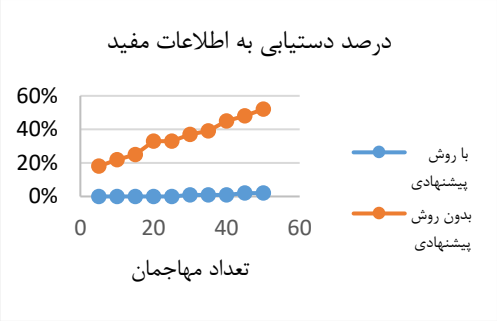
(Table-5): Comparison of efficient schemes with the proposed method in relation to SLA violations

پارامتر	مرکز	سرویس	سوئیچ
بدون ذخیره‌سازی	٪۱۰۰	٪۱۰۰	٪۱۰۰
DVFS	٪۹۶	٪۹۷	٪۹۵
DNS	٪۳۷	٪۳۹	٪۳۲
DVFS+DNS	٪۳۵	٪۳۷	٪۳۱
Proposed	٪۰.۳۰	-	-

در بخش دوم و در یک سناریو میزان جلوگیری از دسترسی به داده‌ها از طرف هکرها با استفاده از روش پیشنهادی مشخص می‌شود. بدین ترتیب که هکرهایی که قصد دسترسی به داده‌های مهم و رمزگشایی آن‌ها را داشته باشند، با این روش نمی‌توانند به دادهٔ واقعی دست پیدا کنند؛ درنتیجهٔ این حملات که حملات شنود هستند، باید دید که چند درصد از داده‌های به‌دست‌آورده‌شده توسط هکرها شناسایی خواهد شد. با توجه به استفاده از رهیافت زنجیرهٔ بلوکی برای حفظ محرمانگی با اطمینان می‌توان گفت این آزمایش اهمیت بالایی برای تحلیل کارایی روش پیشنهادی دارد.

حال در این سناریو یک تعداد گره مهاجم داریم که تعداد آن‌ها افزایش می‌یابد. با افزایش گره‌های مهاجم درصد دستیابی موفق گره‌های مهاجم به اطلاعات گره‌های دیگر مشخص شده‌است؛ حالتی که زنجیرهٔ بلوکی اعمال شود و حالتی که نشود در شکل بعد مورد مقایسه قرار گرفته‌است. نرخ ارسال صد کیلوبایت در ثانیه و تعداد کل گره‌ها صد گره در نظر گرفته شده‌است.

چنان‌چه در شکل (۶) مشاهده می‌شود هنگامی که هیچ روشی برای رمزنگاری داده وجود نداشته باشد، بسیاری از داده‌ها در معرض افشا خواهند بود و این میزان در تعداد پنجاه مهاجم به پنجاه‌درصد می‌رسد. با رمزنگاری با روش پیشنهادی درصد داده‌های افشاشده بسیار ناچیز است که با وجود احتمال حدس رمز یا داده از سمت مهاجمان، معادل صفر خواهد بود.

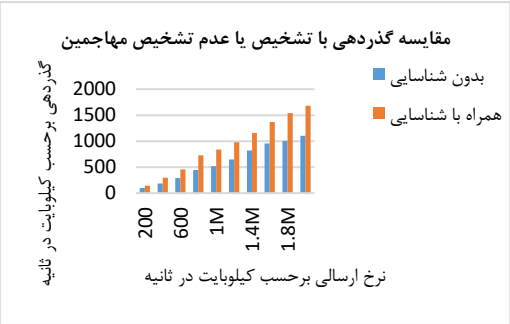


(شکل-۶): درصد دست‌یابی به اطلاعات

(Figure-6): Percentage of access to information

۴-۴-۱-سناریوی جلوگیری از ورود گره‌های مخرب

در سناریویی دیگر تأثیر افزایش ترافیک بر کارایی روش پیشنهادی هنگامی که عامل جلوگیری از دسترسی گره‌های مخرب بر روی ابر و لبه فعال شده‌باشد (یعنی احراز هویت) در برابر زمانی که فعال نشده‌باشد، بررسی می‌شود. در این سناریو قصد بر این است که مشخص شود اجرای روش پیشنهادی برای ورود به قسمت لبه در شبکه، بر روی کارایی شبکه هنگام افزایش ترافیک و شلوغی شبکه چیست و چه میزان از گذردهی شبکه هنگام حملات کم می‌شود؛ بدین ترتیب میزان ارسال گره‌ها از دویست کیلوبایت در ثانیه به دو مگابایت در ثانیه رسیده و اثر آن بر روی گذردهی شبکه بررسی می‌شود. تعداد گره‌ها سیصد گره در نظر گرفته شده‌است.



(شکل-۷): مقایسهٔ گذردهی در سناریوی شناسایی گره‌های مخرب

(Figure-7): Transition comparison in the destructive node identification scenario

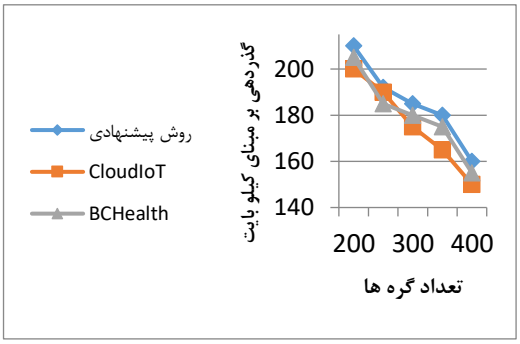
با توجه به شکل (۷) با افزایش ترافیک شبکه، ابتدا اختلاف نرخ گذردهی بین روش بدون جلوگیری از ورود و همراه با جلوگیری از ورود افزایش پیدا می‌کند. این نشان از این موضوع است که با جلوگیری از ورود گره‌های مهاجم، ترافیک شبکه تأثیر گره‌های مهاجم با تشخیص و جلوگیری از فعالیت آن‌ها تأثیر چندان مخربی نخواهد داشت، درحالی‌که هنگامی که از ورود این گره‌ها جلوگیری

[DOI: 10.61186/jsdp.21.3.149]

نمی‌شوند، تأثیر تخریب بسیار زیاد است و ترافیک شبکه رشد کمی خواهد داشت؛ مطابق با این مشاهدات حذف بسته‌ها در هر دو حالت کم‌ترافیک و پرترافیک اتفاق می‌افتد و این مسئله‌ای است که به‌هرحال وجود دارد. درنتیجه ترافیک دریافتی از شبکه کامل نخواهد بود و بخشی از داده‌ها از بین می‌رود.

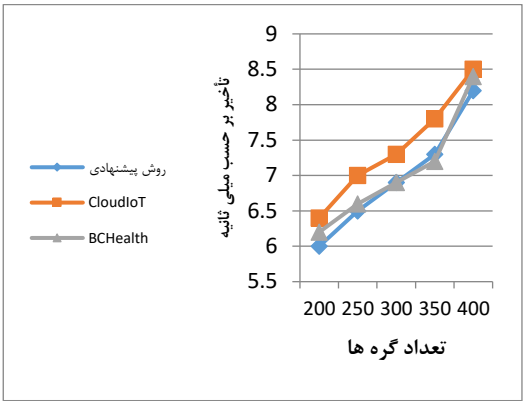
۴-۵-مقایسه با روش دیگر

در این بخش از مقاله برخی از نتایج به‌دست‌آمده از روش پیشنهادی را با روش‌های دیگری که پیش‌ازاین در تأمین محرمانگی اینترنت اشیا در بستر رایانش ابری مطرح شده‌اند، مقایسه می‌شود[۴۱] و [۴۹]. پژوهش [۴۱] کمابیش جدید است که مسئلهٔ مدیریت امنیت، تولید کلید و رمزنگاری را در شبکه‌های iot با یک روش مبتنی بر ابر مورد نظر قرار داده و ارزیابی خود را با محاسبهٔ میزان عملکرد با حالت بدون اجماع ارائه داده‌است. در این روش از الگوریتم متقارن AES و نامتقارن RSA برای رمزگذاری استفاده شده‌است. همچنین در ارتباط با پژوهش [۴۹] که پیشتر نیز تا حدی معرفی شد یک روش جدید برای بهره‌گیری از قابلیت زنجیرهٔ بلوکی بر روی سامانه سلامت به نام BCHealth[1] پیشنهاد می‌دهد که از الگوریتم‌های رمزنگاری AES و شبکه مبتنی بر یک دستگاه مدیریت مرکزی اینترنت اشیا با نام IHM[2] استفاده می‌کند که با دستگاه‌های اینترنت اشیا همچون PDA بیمار برای بررسی‌های امنیتی ارتباط برقرار می‌کند و همچنین با روال زنجیرهٔ بلوکی مجتمع شده‌است؛ اگرچه در این روش از محل دقیق ذخیره‌سازی سخن به میان نیاورده، اما درکل از ابر به‌عنوان یک موجودیت برای ارتباط با زنجیرهٔ بلوکی سخن گفته شده‌است. باوجوداین، برای مقایسهٔ بهتر میان روش پیشنهادی و BCHealth فرض می‌شود که IHM برای ذخیره‌سازی اطلاعات مورد استفاده قرار می‌گیرد که یک موجودیت محلی است. سپس روال معرفی‌شده در پژوهش برای کنترل دسترسی بر اساس ساختار پیشنهادی آن اجرا شده‌است.



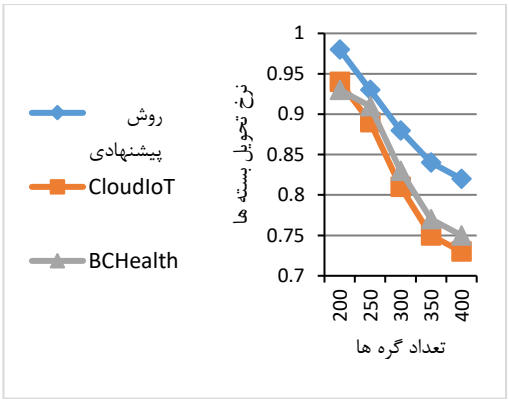
(شکل-۸): مقایسهٔ گذردهی روش‌ها با تغییر تعداد گره‌های شبکه

(Figure-8): Comparison of throughput of the methods by changing the number of network nodes



(شکل-۹): مقایسهٔ تأخیر روش‌ها با تغییر تعداد گره‌های شبکه

(Figur-9): Comparison of delay of the methods by changing the number of network nodes



(شکل-۱۰): مقایسهٔ نرخ تحویل بسته‌های روش‌ها با تغییر تعداد گره‌های شبکه

(Figure-10): Comparison of packet delivery rate of the methods by changing the number of network nodes

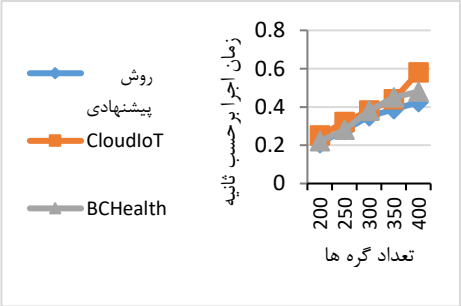
این سه مقایسه نشان می‌دهند عملکرد روش پیشنهادی در تشخیص و خنثی‌کردن حملات تا حد زیادی مؤثرتر از روش CloudIoT و BCHealth بوده‌است؛ ضمن اینکه در برابر این کارایی هزینهٔ بسیار زیادی نیز پرداخت نمی‌شود. در زمینهٔ گذردهی درکل روش پیشنهادی در بالای روش CloudIoT و BCHealth به چشم می‌خورد. این نشان‌دهندهٔ حذف تعداد کمتری از بسته‌هاست که به‌واسطهٔ حملات در شبکه حذف شده‌اند. البته برخی از بسته‌ها نیز به دلیل ماهیت پویای شبکه و شرایط آن ممکن است حذف شده باشد که ربطی به جلوگیری از حملات در شبکه ندارد. در زمینهٔ تأخیر نیز در برخی تعداد گره‌ها روش BCHealth عملکرد پایاپایی از خود نشان داده و یا کمی بهتر عمل کرده‌است در حالی که در بقیه تعداد گره‌ها عملکرد روش پیشنهادی نسبت به این روش به‌طور کامل برتر بوده‌است؛ همچنین در تمام حالت‌ها روش پیشنهادی نسبت به CloudIoT عملکرد بهتری از خود نشان داده‌است که استفاده از پردازش لبه به‌جای ابر این مورد را کامل موجه می‌سازد؛ همچنین در ارتباط با نرخ تحویل بسته‌ها مطابق انتظار که بسته‌های

[1] BlockChain Heathcare
[2] IoT Health Manager

[DOI: 10.61186/jsdp.21.3.149]

کمتری در اثر حملات حذف می‌شوند نرخ تحویل بسته برای روش پیشنهادی به‌طور کامل برتر از دو روش دیگر مورد مقایسه است. درکل نتایج نشان می‌دهد که جلوگیری از حمله به‌وسیلهٔ روش پیشنهادی می‌تواند در زمینهٔ گذردهی و نرخ تحویل بسته تأثیر بسزایی داشته باشد و آن‌ها را به شدت افزایش دهد؛ اگرچه تغییرات آن در زمینهٔ تأخیر چندان هم زیاد نخواهد بود.

زمان اجرای روش‌ها برای اتمام ارسال بسته‌ها و اتمام شبیه‌سازی یک معیار دیگر است که می‌تواند نشان‌دهندهٔ پیچیدگی اجرا و نیازمندی‌های محاسباتی در روش‌ها باشد؛ بدین ترتیب برای این منظور زمان اجرا در شبیه‌سازی محاسبه شده‌است که در شکل (۱۱) مشاهده می‌شود.



(شکل-۱۱): مقایسهٔ زمان اجرای روش‌ها با تغییر تعداد گره‌های شبکه

(Figure-11): Comparison of run time of the methods by changing the number of network nodes

همان‌طور که در شکل (۱۱) مشخص است، زمان اجرای روش پیشنهادی برای تعداد گره‌های پایین کمابیش برابر با روش BCHealth و کمی پایین‌تر از CloudIoT است، اما برای تعداد گره‌های بالا اختلاف زمانی بیشتری را با روش‌های دیگر نشان می‌دهد و در زمان کمتری اجرا می‌شود. دلیل این موضوع بیشتر به پیچیدگی کمتر روش در اجرا برمی‌گردد. در رابطه با پیچیدگی روش پیشنهادی و مرتبهٔ آن در بخش ۴-۶ بحث می‌شود.

در جدول (۶) یک مقایسهٔ عملکردی کارایی بر روی میانگین پارامترهای مختلف روش‌ها انجام شده‌است.

در این جدول برای هر یک از پارامترها مقدار میانگین به‌عنوان یک عدد مجزا در بالای هر خانه نوشته شده‌است. اعداد پایین، دو عدد هستند که عدد اول مشخص‌کنندهٔ بدترین و عدد دوم نشان‌دهندهٔ بهترین عملکرد هر روش در آن پارامتر کارایی است. چنانچه مشخص است روش پیشنهادی در هر سه زمینهٔ تأخیر، گذردهی و نرخ تحویل بسته‌ها دارای عملکردی بهتر است، به‌ویژه در زمینهٔ نرخ تحویل بسته که مشخص‌کنندهٔ میزان غلبه بر حملات است، بیش از ۵ درصد بهبود مشاهده می‌شود.

در جدول (۷) مقایسهٔ کلی روش پیشنهادی با روش CloudIoT و BCHealth برای تأمین امنیت و دسترسی‌پذیری در مراقبت بهداشتی الکترونیک مبتنی بر ابر و اینترنت اشیا آورده شده‌است؛ فرض بر این است که این روش به بهترین شکل اجرایی شده و جوانب مختلف امنیت در ابر را درنظر بگیرد.

(جدول-۶): مقایسهٔ عملکردی روش پیشنهادی و روش‌های پیشین

(Table-6): Operational comparison of the proposed method and before approaches

پارامتر / روش	تأخیر	گذردهی	نرخ تحویل بسته‌ها
CloudIoT	۷.۴ ۸.۵/۶.۴	۱۷۶ ۱۵۰/۲۰۰	۰.۸۲۴ ۰.۷۳/۰.۹۴
BCHealth	۷.۰۶ ۸.۴/۶.۲	۱۸۰ ۱۵۵/۲۰۵	۰.۸۳۸ ۰.۷۵/۰.۹۳
Proposed	۶.۹۸ ۸.۲/۶	۱۸۶ ۱۶۰/۲۱۰	۰.۸۹ ۰.۸۲/۰.۹۸

چنانچه در جدول (۷) مورد بررسی قرار گرفته‌است، روش‌هایی همچون CloudIoT در مقایسه با طرح پیشنهادی این پژوهش عملکرد ضعیف‌تری خواهند داشت که درنتیجه نیاز به پردازش اضافی ایجاد می‌شود. در طرح پیشنهادی این پژوهش پردازش‌ها بسیار ساده است و سربار پردازش کمابیش پایینی وجود خواهد داشت؛ ضمن اینکه مراحل به‌گونه‌ای است که کلیهٔ نیازمندی‌های مورد نیاز برای مراکز دادهٔ ابری و اینترنت اشیا در کاربرد پزشکی را پوشش می‌دهد. همچنین ازآنجا که روش BCHealth نحوه و محل ذخیره‌سازی داده را مشخص نکرده‌است این دو عامل در جدول برای این روش مشخص نشده‌است. در بقیهٔ فاکتورها روش پیشنهادی با BCHealt که همچون روش پیشنهادی از زنجیرهٔ بلوکی استفاده کرده‌است به‌صورت کلی تفاوت زیادی را نمی‌توان قائل شد و تفاوت آن در جزئیات طرح‌هاست که موجب عملکرد بهتر در روش پیشنهادی شده‌است.

۴-۶-پیچیدگی اجرا

پیچیدگی اجرای یک روش را می‌توان به‌صورت نظری تخمین زد؛ اگرچه در پدیده‌های پیچیده‌ای همچون شبکه‌های کامپیوتری و اینترنت اشیا از آنجا که عوامل بسیاری دخیل‌اند، این تخمین شاید چندان دقیق نباشد. به‌هرصورت برای مشخص‌کردن پیچیدگی اجرا نیاز است که برخی ساده¬سازی¬ها و مختصرسازی‌ها انجام شود.

[DOI: 10.61186/jsdp.21.3.149]

(جدول-۷): مقایسهٔ کلی روش پیشنهادی و روش‌های پیشین

(Table-7): Overall comparison of the proposed method and before approaches

روش به‌کار گرفته‌شده / معیارهای مقایسه	BCHealth	CloudIoT	Proposed
مقاوم‌بودن	بالا	پایین	بالا
انعطاف‌پذیری	N/A	پایین	بالا
مقیاس‌پذیری	N/A	پایین	بالا
مصرف منابع	متوسط	متوسط	متوسط
دقت عملکرد	بالا	بالا	بالا
قابلیت اطمینان	بالا	بالا	بالا
ایجاد محرمانگی	بالا	بالا	بالا
سرعت	متوسط	متوسط	متوسط
دسترسی‌پذیری	بالا	بالا	بالا
صحت داده‌ها	بالا	بالا	بالا

فرض می‌شود که تعداد گره‌ها (کاربران، دستگاه‌های IoT، گوشی‌های هوشمند و ...) برابر با n باشد و هر گره به صورت متوسط m پیام ارسال می‌کند، ابتدا هر گره برای ارسال پیام باید احراز هویت کند که در لبهٔ ابر این موضوع انجام می‌شود.

در شکل (۳) مشخص است که برای آغاز یک نشست تعداد هفت پیام ردوبدل می‌شود. این یک تابع خطی از n است. تمام n گره باید احراز هویت شوند که برای احراز هویت هر گره هفت پیام ارسال می‌شود (7n). هر گره متوسط m پیام ارسال می‌کند یعنی (m*n). درنتیجه می‌توان گفت اگر n گره بخواهند هرکدام m پیام بفرستند 7n+n*m پیام ارسال می‌شود. با فاکتور گرفتن از n جواب واضح‌تری به‌دست می‌آید به‌صورت n*(7+m).

با ساختار بلوکی در نظر گرفته شده برای ارسال داده‌ها این تعداد ارسالی می‌تواند دستخوش تغییر شود؛ زیرا پیغام‌ها به بلوک‌ها اضافه می‌شوند و پس از پرشدن هر بلوک ارسال صورت می‌گیرد. یعنی در واقع n*(7+[m/B]) پیام در شبکه ارسال می‌شود که B اندازهٔ هر بلوک است و [m/B] حد بالای تقسیم تعداد پیام بر اندازهٔ بلوک را نشان می‌دهد. با توجه به محاسبات صورت‌گرفته، این روش پیچیدگی متناسب

با تعداد گره‌ها و پیامها دارد و مرتبهٔ خطی است و استفاده از بلوک‌بندی پیام‌ها به کاهش این پیچیدگی کمک می‌کند. درنتیجه پیچیدگی نسبت به حالت عادی افزایش خاصی پیدا نمی‌کند و موجب مقیاس‌پذیری هرچه بیشتر این روش می‌شود.

۵- نتیجه‌گیری و کارهای آینده

در این مقاله سعی شد ابتدا نیاز سوابق پزشکی به محرمانگی تبیین شود و پس از بررسی این نیاز در حالت کلی مسئلهٔ محرمانگی در ارتباط با رایانش ابری به‌عنوان نیاز خاص امنیتی این دسته از داده‌ها در Cloud-IoT مورد بررسی قرارگرفت. با توجه به روش پیشنهادی مقاله برای تأمین محرمانگی در سامانه پزشکی مبتنی بر cloud-IoT که این روش مبتنی‌بر زنجیرهٔ بلوکی است، ساختار زنجیرهٔ بلوکی مورد بحث قرارگرفت و نقاط قوت و ضعف این سامانه‌ها بررسی شد. در ادامه با استفاده از زنجیرهٔ بلوکی به همراه ابزارهای امنیتی همچون احراز هویت بر روی لبهٔ ابر با زیرساخت کلید عمومی و رمزنگاری دیفی-هلمن یک طرح امنیتی برای مراقبت پزشکی و سوابق مبتنی بر Cloud-IoT پیشنهاد شد که بتواند محرمانگی را تا حد مطلوبی فراهم کند و تأخیر نیز نسبت به ابر کاهش یابد. با شبیه‌سازی این روش مشخص شد که این سامانه دارای محرمانگی مطلوب بوده و از طرف دیگر از نظر کارایی نسبت به روش‌های پیشین CloudIoT و BCHeath حداقل ۵درصد بهبود دارد. همچنین از چند نقطه‌نظر همچون مقاوم‌بودن، انعطاف‌پذیری و مقیاس-پذیری نسبت به روش CloudIoT دارای برتری است. از آنجا که روش BCHeath مکانیزم دقیق ذخیره و بازیابی و محل ذخیره‌سازی را مشخص نکرده‌است در ارتباط با مقایسهٔ برخی عوامل همچون انعطاف‌پذیری و مقیاس-پذیری با روش پیشنهادی نمی‌توان نظر دقیق داد، اما مزیت روش پیشنهادی نسبت به این روش، از نظر معیار عملکردی قابل توجه است؛ همچنین مزیتی همچون مرتبهٔ اجرایی خطی نیز از دیگر مزایای این روش است که می-

[DOI: 10.61186/jsdp.21.3.149]

تواند به مقیاس‌پذیری و حفظ کارایی آن کمک بیشتری کند.

در ادامهٔ این کار می‌توان ساختار ارائه‌شده را بیش‌ازپیش بهینه کرد. می‌توان نحوهٔ سرویس‌دهی‌ها را دقیق‌تر مشخص کرد و از انواع حملات در شبکه برای اجرا و ارزیابی استفاده و روش را برای هر حمله به‌صورت ویژه بهینه کرد. دامنهٔ حملات گسترده بوده و برای هر حمله مکانیزم خاصی لازم است که در هر روش گنجانده شود؛ بنابراین لازم است دامنهٔ زنجیرهٔ بلوکی با توجه به پشتیبانی از دفاع در برابر حملات مختلف بسط داده شود و داده‌های سوابق پزشکی بر اساس اهمیت محرمانگی آن سطح‌بندی و همچنین سوابق پزشکان و پرستاران را نیز شامل شود و در زمینهٔ مدیریت بهینهٔ منابع در این روش بحث‌وبررسی صورت گیرد.

6-Reference ۶- مراجع

[1] X. Wang, L. Bai, Q. Yang, L. Wang, and F. Jiang, "A dual privacy-preservation scheme for cloud-based eHealth systems," Journal of Information Security and Applications, vol. 47, pp. 132-138, 2019.

[2] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain leveraged decentralized IoT eHealth framework," Internet of Things, vol. 9, p. 100159, 2020.

[3] R. Duan, M. R. Boland, Z. Liu, Y. Liu, H. H. Chang, H. Xu, H. Chu, et al., "Learning from electronic health records across multiple sites: A communication-efficient and privacy-preserving distributed algorithm," Journal of the American Medical Informatics Association, vol. 27, no. 3, pp. 376-385, 2020.

[4] A. Majeed, "Attribute-centric anonymization scheme for improving user privacy and utility of publishing e-health data," Journal of King Saud University-Computer and Information Sciences, vol. 31, no. 4, pp. 426-435, 2019.

[5] A. Donawa, I. Orukari, and C. E. Baker, "Scaling blockchains to support electronic health record systems for hospitals," arXiv preprint arXiv:2001.05525, 2020.

[6] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of Medical Systems, vol. 42, no. 8, p. 140, 2018.

[7] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: A survey," Future Generation Computer Systems, vol. 56, pp. 684-700, 2016.

[8] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," Transactions on Emerging Telecommunications Technologies, vol. 25, no. 1, pp. 81-93, 2014.

[9] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782-147795, 2019.

[10] D. Gachet, M. de Buenaga, F. Aparicio, and V. Padrón, "Integrating internet of things and cloud computing for health services provisioning: The virtual cloud carer project," in 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 918-921. IEEE, 2012.

[11] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," IEEE Systems Journal, vol. 11, no. 1, pp. 88-95, 2015.

[12] N. Alharbe, A. S. Atkins, and J. Champion, "Use of cloud computing with wireless sensor networks in an Internet of Things environment for a smart hospital network," in Proceedings of the Seventh International Conference on eHealth, Telemedicine, and Social Medicine, Lisbon, Portugal, pp. 22-27, 2015.

[13] J. Zhou, T. Leppanen, E. Harjula, M. Ylianttila, T. Ojala, C. Yu, H. Jin, and L. T. Yang, "Cloudthings: A common architecture for integrating the internet of things with cloud computing," in Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 651-657. IEEE, 2013.

[14] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: A comprehensive survey," IEEE Access, vol. 3, pp. 678-708, 2015.

[15] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.

[16] F. Hussain and U. Qamar, "Identification and correction of misspelled drugs' names in electronic medical records (EMR)," in International Conference on Enterprise Information Systems, vol. 3, pp. 333-338. SCITEPRESS, 2016.

[17] S. I. Goldberg, M. Shubina, A. Niemierko, and A. Turchin, "A weighty problem: Identification, characteristics and risk factors for errors in EMR data," in AMIA Annual Symposium Proceedings, vol. 2010, p. 251. American Medical Informatics Association, 2010.

[18] E. A. Mohammed, B. H. Far, and C. Naugler, "Applications of the MapReduce programming framework to clinical big data analysis: Current landscape and future trends," BioData Mining, vol. 7, no. 1, pp. 1-23, 2014.

[19] Y. Liang and A. Kelemen, "Big Data science and its applications in health and medical research: Challenges and opportunities," J Biom Biostat, vol. 7, no. 307, 2016.

[DOI: 10.61186/jsdp.21.3.149]

Applications (iTAP), 2011 International Conference on, pp. 1-4. IEEE, 2011.
[33] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Information Systems Frontiers, pp. 1-14, 2014.
[34] J. Guo, R. Chen, and J. J. P. Tsai, "A mobile cloud hierarchical trust management protocol for IoT systems," in Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2017 5th IEEE International Conference on, IEEE, 2017.
[35] Y. Liu, J. E. Fieldsend, and G. Min, "A framework of fog computing: Architecture, challenges, and optimization," IEEE Access, vol. 5, pp. 25445-25454, 2017.
[36] H. Kim and E. A. Lee, "Authentication and authorization for the Internet of Things," IT Professional, vol. 19, no. 5, pp. 27-33, 2017.
[37] M. Mahmud, et al., "A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications," arXiv preprint arXiv:1801.03984, 2018.
[38] R. K. Behera, K. H. K. Reddy, and D. S. Roy, "Reliability modelling of service oriented Internet of Things," in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), IEEE, 2015.
[39] V. Kharchenko, et al., "Reliability and security issues for IoT-based smart business center: Architecture and Markov model," in 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), IEEE, 2016.
[40] V. Sharma, et al., "A consensus framework for reliability and mitigation of zero-day attacks in IoT," Security and Communication Networks, 2017.
[41] C. Stergiou, et al., "Secure integration of IoT and cloud computing," Future Generation Computer Systems, vol. 78, pp. 964-975, 2018.
[42] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," Computers & Security, vol. 88, p. 101653, 2020.
[43] H. Deng, Z. Qin, L. Sha, and H. Yin, "A flexible privacy-preserving data sharing scheme in cloud-assisted IoT," IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11601-11611, 2020.
[44] P. Tedeschi, K. E. Jeon, J. She, S. Wong, S. Bakiras, and R. Di Pietro, "Privacy-preserving and sustainable contact tracing using batteryless BLE beacons," arXiv preprint arXiv:2103.06221, 2021.
[45] F. Firouzi, B. Farahani, M. Barzegari, and M. Daneshmand, "AI-driven data monetization: The other face of data in IoT-based smart and
[20] W. J. Gordon and C. Catalini, "Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability," Computational and Structural Biotechnology Journal, vol. 16, pp. 224-230, 2018.
[21] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of ehealth data in Europe," International ISCIS Security Workshop. Springer, Cham, 2018.
[22] D. C. Nguyen, et al., "Blockchain for secure EHRs sharing of mobile cloud based e-Health systems," IEEE Access, vol. 7, pp. 66792-66806, 2019.
[23] M. Qazi, D. Kulkarni, and M. Nagori, "Proof of authenticity-based electronic medical records storage on blockchain," in Smart Trends in Computing and Communications, Springer, Singapore, pp. 297-306, 2020.
[24] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of Medical Systems, vol. 42, no. 8, p. 140, 2018.
[25] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," Journal of Information Security and Applications, vol. 50, p. 102407, 2020.
[26] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," Healthcare, Elsevier, 2019.
[27] E. Gorelik, "Cloud computing models," Doctoral dissertation, Massachusetts Institute of Technology, 2013.
[28] C. Choi, J.-H. Park, M. Na, and S. Jo, "Low-latency 5G architectures for mission-critical Internet of Things (IoT) services," Information and Communications Magazine, vol. 32, no. 9, pp. 17-23, 2015.
[29] H. Wu, K. Yue, C.-H. Hsu, Y. Zhao, B. Zhang, and G. Zhang, "Deviation-based neighborhood model for context-aware QoS prediction of cloud and IoT services," Future Generation Computer Systems, vol. 76, pp. 550-560, 2017.
[30] P. Bonte, F. Ongenae, F. De Backere, J. Schaballie, D. Arndt, S. Verstichel, E. Mannens, R. Van de Walle, and F. De Turck, "The MASSIF platform: A modular and semantic platform for the development of flexible IoT services," Knowledge and Information Systems, vol. 51, no. 1, pp. 89-126, 2017.
[31] T. D. Cao, H. H. Hoang, H. X. Huynh, B. M. Nguyen, T. V. Pham, Q. Tran-Minh, ... and H. L. Truong, "IoT services for solving critical problems in Vietnam: A research landscape and directions," IEEE Internet Computing, vol. 20, no. 5, pp. 76-81, 2016.
[32] G. Gang, Z. L., and J. Jun, "Internet of things security analysis," in Internet Technology and

[DOI: 10.61186/jsdp.21.3.149]

connected health," IEEE Internet of Things Journal, 2020.
[46] R. Goyat, G. Kumar, R. Saha, M. Conti, M. K. Rai, R. Thomas, M. Alazab, and T. H.-K. Kim, "Blockchain-based data storage with privacy and authentication in Internet-of-Things," IEEE Internet of Things Journal, 2020.
[47] A. Ali, et al., "HealthLock: Blockchain-based privacy preservation using homomorphic encryption in Internet of Things healthcare applications," Sensors, vol. 23, no. 15, p. 6762, 2023.
[48] S. Das and S. Namasudra, "Lightweight and efficient privacy-preserving mutual authentication scheme to secure Internet of Things-based smart healthcare," Transactions on Emerging Telecommunications Technologies, 2023, e4716.
[49] H. N. Alsuqaih, et al., "An efficient privacy-preserving control mechanism based on blockchain for E-health applications," Alexandria Engineering Journal, vol. 73, pp. 159-172, 2023.
[50] M. I. Ahmed and G. Kannan, "Secure and lightweight privacy-preserving Internet of Things integration for remote patient monitoring," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 9, pp. 6895-6908, 2022.
[51] M. P. Mahmoudi-Nasr and K. H. Kimia, "A mutual authentication method for Internet of Things", Signal and Data Processing, vol. 19, no. 2, pp. 6, 2022. [Online]. Available: http://jsdp.rcisp.ac.ir/article-1-1134-fa.html
[52] S. Azizi, M. Ashouri-Talouki, and H. Mala, "An efficient and secure frequent multiparty summation protocol", Signal and Data Processing, vol. 15, no. 4, pp. 31-40, 2019. [Online]. Available: http://jsdp.rcisp.ac.ir/article-1-649-fa.html
[53] A. Janosi, W. Steinbrunn, M. Pfisterer, and R. Detrano, "Heart Disease," UCI Machine Learning Repository [Online]. Available: https://archive.ics.uci.edu/dataset/45/heart+disease. [Accessed: Mar. 15, 2024].

عباس حسن پور عسکری دانش‌نامهٔ کارشناسی و کارشناسی‌ارشد را از دانشگاه آزاد رشتهٔ مهندسی کامپیوتر گرایش نرم‌افزار دریافت کرد و در حال حاضر دانشجوی دکترای تخصصی مهندسی کامپیوتر- نرم‌افزار دانشگاه علوم و تحقیقات- پردیس مرکز آموزش بین‌المللی قشم است. زمینه‌های پژوهشی مورد علاقهٔ وی اینترنت اشیا، داده‌کاوی، رایانش ابری و امنیت داده است.
نشانی رایانامهٔ ایشان عبارت‌است از:
Abbas.Hassanpouraskari@yahoo.com

عمید خطیبی بردسیری دارای مدرک دکترای تخصصی کامپیوتر (گرایش نرم‌افزار) و در حال حاضر عضو هیئت علمی تمام وقت دانشگاه آزاد اسلامی است. حوزه‌های پژوهشی مورد علاقهٔ ایشان شامل داده‌کاوی، مهندسی و اندازه‌گیری نرم‌افزار، رایانش ابری و الگوریتم‌های هوشمند است. ایشان بیش از صد مقالهٔ علمی و هفت جلد کتاب آموزشی تألیف کرده‌است.
نشانی رایانامهٔ ایشان عبارت‌است از:
a.khatibi@srbiau.ac.ir

مختار محمدی قنات غستانی استادیار گروه کامپیوتر دانشگاه آزاد اسلامی واحد بم است. بیش از بیست مقالهٔ پژوهشی ایشان در کنفرانس‌ها و نشریات معتبر دنیا منتشر شده و زمینه‌های تخصصی و علاقه‌مندی ایشان معماری کامپیوتر، شبکه‌های حس‌گر بی‌سیم و اینترنت اشیا است.
نشانی رایانامهٔ ایشان عبارت‌است از:
mokhtarmohamadi@srbiau.ac.ir

[DOI: 10.61186/jsdp.21.3.149]