APJ 5(4):15-24, Winter 2025

Arman Process Journal (APJ)

Homepage: https://www.armanprocessjournal.ir

Improving Security and Privacy in the Internet of Things Based on Blockchain Technology

R. Ghaffari[1]

[1] Department of Business Administration, Islamic Azad University, Arak Branch, Arak, Iran

ABSTRACT

RESEARCH PAPER

Received: 7 July 2024
Accepted: 18 November 2024

KEYWORDS:
Security,
Privacy,
Internet of Things,
Blockchain,

[1] **Corresponding author:**
r.ghaffarii @gmail.com.

As a smart and effective technology, the Internet of Things (IoT) plays a very important role in today's technology-driven world. This technology refers to a set of computer and technology-driven communications and interactions such as sensors, processing units, software and hardware with other devices and systems, that are connected and linked via the Internet or other communication networks. On the other hand, blockchain is a decentralized and distributed ledger that records transactions on many computers. This structure ensures that no single entity can access the entire chain to commit fraud. Each block in the chain contains a list of transactions, a time stamp and a cryptographic hash of the previous block, so each record created is unchangeable in a secure way. Blockchain technology, as one of the great innovations of the digital world, has been applied in many areas, including cybersecurity. Security is one of the fundamental challenges in the field of IoT, which can be enhanced and improved through blockchain. The purpose of this research is to analyze the solutions to improve security and privacy and to apply it in creating a privacy monitoring system in the Internet of Things based on blockchain technology. Finally, blockchain, with its unique features, can be an important tool in strengthening the security of the IoT against various threats and reducing risks. Using this technology in areas such as data protection, preventing information manipulation, and increasing the security of cloud systems can help reduce threats and improve digital security. Although there are challenges in the path of blockchain adoption and implementation, its benefits, especially in this area, are very significant.

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۴، زمستان ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

فصلنامه تخصصی فناوری اطلاعات و ارتباطات
شماره مجوز: ۸۷۰۹۰

ارتقای امنیت و حریم خصوصی در اینترنت اشیاء براساس تکنولوژی از بلاکچین

رضا غفاری[1]،
گروه مدیریت بازرگانی، دانشگاه آزاد اسلامی، واحد اراک، اراک، ایران

مقاله پژوهشی

تاریخ دریافت مقاله: ۱۴۰۳/۵/۱۲
تاریخ پذیرش: ۱۴۰۳ /۹/۶

واژگان کلیدی:
امنیت،
حریم خصوصی،
اینترنت اشیاء،
بلاکچین،

چکیده

اینترنت ا شیاء به عنوان یک تکنولوژی هو شمند و موثر، نقش ب سیار مهمی را در دنیای فناورمحور امروز ایفا می کند. این تکنولوژی به مجموعه ای از ارتباطات و تعاملات رایانه ای و فناور محور مانند حسگرها، واحدهای پردازش، نرم‌افزار و سخت‌افزار با دیگر د ستگاه‌ها و سامانه‌ها ا شاره دارد که از طریق اینترنت یا دیگر شبکه‌های ارتباطی متصل و مرتبط باشند.

از سوی دیگر بلاکچین یک دفتر کل غیرمتمرکز و توزیع شده است که تراکنش ها را در بسیاری از رایانه ها ثبت می کند. این ساختار تضمین می‌کند هیچ نهاد واحدی نمی‌تواند به کل زنجیره د ستر سی دا شته باشد تا بتواند کلاهبرداری کند. هر بلوک در زنجیره حاوی لیستی از تراکنش ها، یک مهر زمانی و یک هش رمزنگاری از بلوک قبلی است، بنابراین هر رکورد ایجاد شده به روشی امن غیرقابل تغییر است. فناوری بلاک‌چین به عنوان یکی از نوآوری‌های بزرگ دنیای دیجیتال، در بسیاری از حوزه‌ها از جمله امنیت سایبری به کار گرفته شده است. امنیت یکی از چالش های بنیادین در حوزه اینترنت اشیاء می‌باشد که از طریق بلاکچین قابل ارتقا و بهبود می باشد. هدف این تحقیق تحلیل راهکارهای ارتقای امنیت و حریم خصوصی و بکارگیری آن در ایجاد یک سیستم نظارت بر حفظ حریم خصوصی در اینترنت اشیاء بر اساس تکنولوژی بلاکچین می باشد. در نهایت، بلاک‌چین با ویژگی‌های بی نظیر خود می‌تواند به‌عنوان یک ابزار مهم در تقویت امنیت حوزه اینترنت ا شیا در برابر تهدیدات مختلف و کاهش ریسک ها مؤثر واقع شود. ا ستفاده از این فناوری در زمینه‌هایی همچون حفاظت از داده‌ها، جلوگیری از د ستکاری اطلاعات، و افزایش امنیت سیستم‌های ابری، می‌تواند به کاهش تهدیدات و ارتقای امنیت دیجیتال کمک کند. اگرچه چالش‌هایی در مسیر پذیرش و پیاده‌سازی بلاک‌چین وجود دارد، اما مزایای آن به‌ویژه در این حوزه بسیار چشمگیر است.

مقدمه

اینترنت اشیا به میلیاردها دستگاه فیزیکی در سراسر جهان گفته می‌شود که به اینترنت متصل هستند و اطلاعات را جمع‌آوری می‌کنند و با کاربر و سایر دستگاه‌های متصل به اشتراک می‌گذارند. تقریبا هر چیزی که بتواند به شبکه اینترنت متصل شود، بخشی از اینترنت اشیا است. در اینترنت اشیاء دستگاه‌ها اطلاعاتی را فرستاده و دستورهایی را دریافت می‌کنند، از این رو نفوذ هکر و سوءاستفاده آن چندان هم دور از انتظار نیست. اخیراً آزمایشگاه مکآفی اینتل گزارش امنیتی را ارائه کرده است که طی آن به خطراتی که دستگاه‌های اینترنت اشیاء را تهدید می‌کنند، اشاره کرده است. در این گزارش آمده که با افزایش دستگاه‌های متصل به هم در اینترنت اشیاء، خطر نفوذ هکرها نیز افزایش می‌یابد، شاید برخی دستگاه‌ها از امنیت کافی برخوردار نباشند [۱].

در حوزه امنیت اینترنت اشیاء، حملات مختلفی معرفی می‌شود که فضای این مفهوم و فناوری‌های مرتبط با آن را درگیر کرده است. این نشان می‌دهد که این فناوری به پرتگاه بسیار پیچیده‌ای نزدیک شده است و اقدامات متقابل اغلب صرفاً واکنشی است. مسئله امنیت در اینترنت اشیاء را می‌توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است ولی همچنان نیازمندی‌های امنیتی اینترنت اشیاء و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است [۲].

یکی از چالشهای عمده ای که باید به منظور وارد کردن اینترنت اشیا به جهان واقعی بر طرف شود مشکلات امنیتی در این حوزه است. تهدیداتی که می تواند بر نهادهای اینترنت اشیا تأثیر گذارد متعدد هستند، مانند حملات با هدف کانالهای ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیا که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف، می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری مکانیزمهای امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. از جمله دو چالش مهم و پیچیده در اینترنت اشیا عبارتند از :امنیت و حریم خصوصی. امنیت شامل دسترسی غیرقانونی به اطلاعات و حمله هایی است که موجب قطعی فیزیکی در قابلیت دسترسی به سرویس می گردد [۳].

امنیت و حریم شخصی در اینترنت اشیا

اخیرا بیشتر محققان در حال حاضر به دنبال افزایش و توسعه حریم خصوصی در برنامه های کاربردی حوزه اینترنت اشیا هستند، فناوریهای بهبود حریم می تواند به موضوع اشیا، تراکنش یا سیستم متمایل گردد و از آن برای محافظت از هویت در اینترنت خصوصی[1] (PET) استفاده شود. در محیط اینترنت اشیا، امنیت و حریم خصوصی برای تضمین یک تعامل قابل اعتماد بین دنیای فیزیکی و دنیای مجازی مهم هستند [۵].

اینترنت اشیا که از آن به عنوان "انقلاب صنعتی جدید" یاد می‌شود، به دلیل تغییری که در شیوه زندگی ایجاد کرده‌است، تعاملات بین دولت‌ها و دنیای پیرامونشان را با دنیای مجازی و تکنولوژی نیز دگرگون ساخته است. اینترنت اشیاء به زبان ساده، ارتباط حسگرها و دستگاه‌ها با شبکه‌ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند. امروزه اینترنت اشیا با رشد نمایی در حوزه صنعت و تحقیقات همراه بوده است. اینترنت اشیاء (IoT) اتصال میلیاردها دستگاه و سنسور کم مصرف از طریق اینترنت را فراهم آورده است که حجم وسیعی از داده ها را تولید می کند. به طور کلی ، دستگاه های IoT اطلاعات را از طریق شبکه های سیمی و بی سیم مختلف منتقل می کنند. به دلیل ماهیت باز شبکه ، دستگاه ها در برابر حملات آسیب پذیر هستند و امنیت در اینترنت اشیا تضمین نمی شود. علاوه بر آن اطلاعات منتقل شده بین دستگاه ها در برابر نفوذ و دستکاری آسیب پذیر هستند که منتج به حملات Dos و حملات Ddos می شود. علاوه بر این ، داده های تولید شده در این سیستم ها ، اگر به درستی حفظ نشوند ، می توانند حریم خصوصی کاربران زیادی را در معرض دید قرار دهند و نگرانی هایی را برای کاربران به همراه داشته باشند [۶]. امروزه استفاده از فناوری بلاکچین جهت تامین امنیت در اینترنت اشیا مورد توجه بسیاری از محققان قرار گرفته است. فناوری بلاکچین به یک پایگاه داده مشترک توزیع شده اطلاق می شود که در آن موجودیت ها در یک زنجیره با یکدیگر کار می کنند تا یک کتاب توزیع شده را حفظ کنند که سوابق داده آن نمی تواند دستکاری و یا جعل شود. از طرفی دیگر ، بلاکچین و IoT از نظر ویژگی های توزیع شده شباهت دارند. بلاکچین از شبکه معمولی نقطه به نقطه استفاده می کند. بنابر، این ویژگی ها، اگر از فن آوری های بلاکچین به طور موثر استفاده شود ، برنامه

[1] Privacy-enhancing technologies

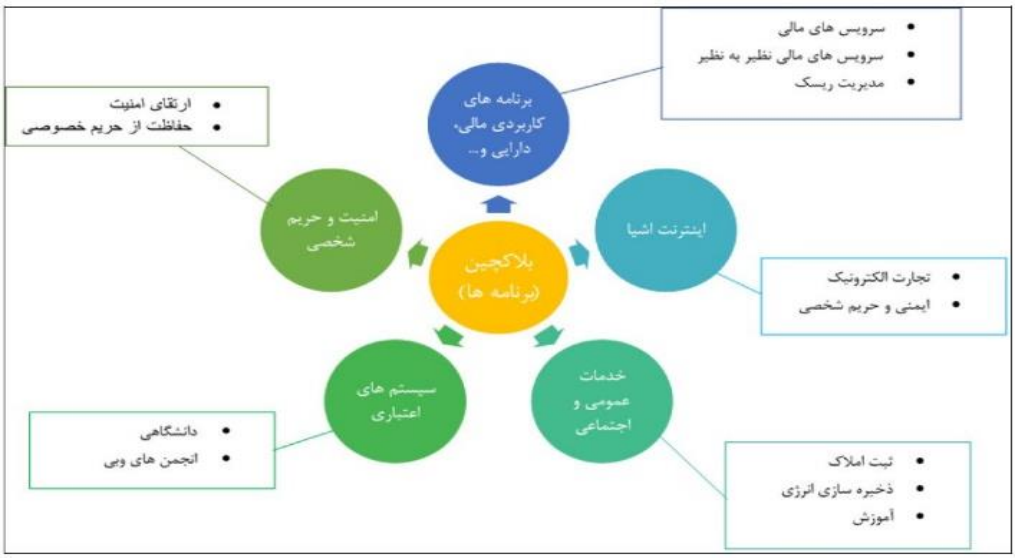
IoT می تواند به بسیاری از ویژگی های امنیتی شبکه مانند حفاظت از حریم خصوصی دستگاه ، تأیید اعتبار اطلاعات ، کنترل دسترسی و رمزگذاری داده ها دست یابد. در واقع به منظور حفظ امنیت در اینترنت اشیا، بلاکچین یک راه حل مطلوب است. در این تحقیق ما چارچوبی را پیشنهاد می کنیم که بلاکچین را در یک سیستم IoT ادغام کند و و راه حلی برای حفظ امنیت در اینترنت اشیا و حریم خصوصی آن فراهم آورد [۹-۷].

اینترنت اشیاء (IoT) یکی از امیدوارکننده ترین فناوری های پیشرو در آینده است. با این حال ، امنیت IoT محدودیت های آشکاری دارد، که هنوز راه حل قانع کننده ای برای آن ارائه نشده. اما کاربرد IoT همچنان در حال گسترش است. بر این اساس ، خطرات امنیتی و آسیب پذیری ها به طور مداوم در حال افزایش است. برای مثال ویروس بات نت به نام "mirar" با کنترل دستگاه های IoT توانست نیمی از اینترنت در ایالات متحده فلج کند که یکی از گسترده ترین حمله ویروسی در تاریخ نامیده می شود [۱۰].

با توجه به ماهیت اینترنت اشیا که در آن داده‌ها بین افراد و اشیا به اشتراک گذاشته می‌شود ، امنیت داده ها ، حریم خصوصی و قابلیت اطمینان سه چالش اصلی در حوزه امنیتی IoT است و یافتن یک راه‌حل امنیتی ضروری است. تکنولوژی‌های بلاکچین فرصتی را فراهم می‌آورند که سطح لازم اعتماد بین اعضای یک شبکه فراهم شود . در حال حاضر ، بلاکچین به دلیل ماهیت غیرقابل انکار و مزایای آن در مورد امنیت و حفظ حریم خصوصی ، مورد توجه چشمگیری قرار گرفته است ، بلاکچین این توانایی را دارد که محدودیت های اینترنت اشیاء (IoT) مانند محافظت از داده ها و حریم خصوصی را برطرف کند. این تکنولوژی از سیستم‌های نظیر به نظیر و توزیع شده که شامل زنجیره‌ای از بلاک‌هاست برای ذخیره تراکنش‌ها استفاده می‌کند. به عنوان یک سیستم غیرمتمرکز، سیستم‌های بلاکچین به یک شخص ثالث مورد اعتماد نیاز ندارند. در عوض، برای تضمین قابلیت اعتماد و ثبات داده‌ها و معاملات، بلاکچین مکانیسم اجماع غیرمتمرکز را اتخاذ می‌کند. ساختار آن مانند یک فایل لاگ دیجیتال است که به صورت گروهی از لینک‌های متصل به نام بلاک ذخیره می‌شوند. هر بلاکی با بلاک قبلی قفل می‌شود. هنگامی که بلاکی به این زنجیره اضافه شود دیگر قابل تغییر نیست [۱۲-۱۱]. بلاکچین یک بستر برای انجام معاملات مورد اعتماد و بدون شخص ثالث را فراهم می کند ، که در آن هر انتقال وجه ، هر کار و هر درخواستی دارای رکوردی در زنجیره با امضای دیجیتال برای تأیید عمومی است. با توجه به مطالب، در این پژوهش مدلی برای حفظ امنیت و حریم خصوصی در اینترنت اشیا با استفاده از بلاکچین ارائه می شود.

دیدگاه ارتقای امنیت اینترنت اشیا براساس بلاکچین

اساسا کاربرد ها و نرم افزار های مختلفی برای فناوری بلاک چین وجود دارد که در این تحقیق به بررسی خلاصه ی چند برنامه ی کاربردی می پردازیم :برنامه های کاربردی (دارایی، مالی و سرمایه گذاری) بلاک چین اینترنت اشیا خدمات عمومی و اجتماعی سیستم اعتباری امنیت در شکل ۱ دامنه ی کاربردهای بلاک چین با تاکید بر بعد امنیت را بررسی نموده و نمایش داده ایم:

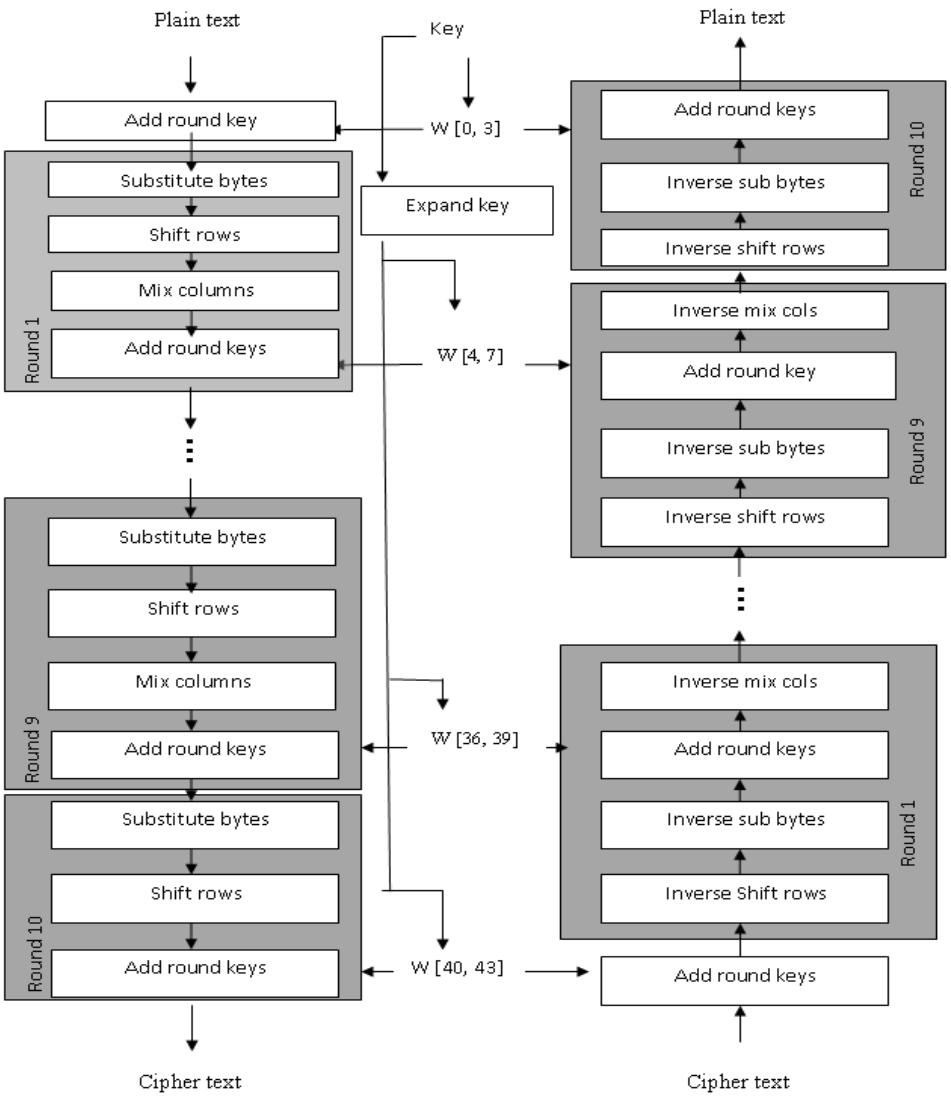


شکل ۱. دامنه کاربرد بلاکچین

در طول دهه گذشته، اینترنت اشیا به واسطه در دسترس بودن سیستم های ارتباطی بی سیم (به عنوان مثال، RFID، WiFi، G۴، IEEE، x۱۵,۸۰۲)، برای برنامه های نظارت و کنترل بسیار هوشمند وارد زندگی ما شده است. امروزه مفهوم اینترنت اشیا چندگانه است و فناوری‌ها، خدمات و استانداردهای مختلفی را در بر می‌گیرد و به طور گسترده‌ای به عنوان پایه و اساس بازار فناوری اطلاعات و ارتباطات حداقل برای ده سال آینده در نظر گرفته می‌شود. تحولات ناشی از انقلاب در زیرساخت های ناشی از اینترنت، امکان برقراری ارتباط افراد و اطلاعات را در هر مکان و در هر زمان ممکن ساخته است. اینترنت اشیاء (IoT) یکی از امیدوارکننده ترین فناوری های پیشرو در آینده است. با این حال ، امنیت IoT محدودیت های آشکاری دارد ، که هنوز راه حل قانع کننده ای برای آن ارائه نشده. اما کاربرد IoT همچنان در حال گسترش است. بر این اساس ، خطرات امنیتی و آسیب پذیری ها به طور مداوم در حال افزایش است. برای مثال ویروس بات نت به نام "mirar" با کنترل دستگاه های IoT توانست نیمی از اینترنت در ایالات متحده فلج کند که یکی از گسترده ترین حمله ویروسی در تاریخ نامیده می شود [۱۳].

در این پژوهش روش تحقیق مورد نظر کتابخانه ای می باشد. در این پژوهش نخست تحقیقاتی درزمینه‌ی اینترنت اشیا و همچنین ساختار امنیت و حریم خصوصی و استفاده از بلاک چین انجام شده است. پس‌ازآن به بررسی راه حل های ارائه شده در زمینه افزایش امنیت در اینترنت اشیا پرداخته ایم. روش جمع آوری داده، - مقالات علمی معتبر که در پایگاه‌های علمی معتبری همچون google scholar و سایر پایگاه‌ها و نشریات علمی معتبر، منتشرشده‌اند. استفاده از کتب علمی منتشرشده درزمینه‌ی بلاک چین و کاربرد آن در امنیت و حریم خصوصی اینترنت اشیا - مطالعه پایان‌نامه‌ها و تحقیقات سایر دانشجویان و اساتید بین المللی در زمینه‌ی اینترنت اشیا، بلاک چین و روش های حفظ امینت در اینترنت اشیا. در این تحقیق به‌منظور حفظ حریم خصوصی و تامین امنیت در اینترنت اشیا، ابتدا ویژگی هایی از دستگاه ها و ارتباطات بین دستگاه ها که در معرض نفوذ و دستکاری هستند در نظر گرفته می‌شود. سپس با در نظر گرفتن ساختار بلاک چین و استفاده از ویژگی آن، دستگاه ها و ارتباطات بین آنها در برابر نفوذ و دستکاری مصون می شوند . تجزیه و تحلیل این اطلاعات در نرم‌افزار متلب پیاده‌سازی شده و نتایج حاصل از این تحقیق در نرم‌افزار متلب مورد تحلیل و ارزیابی قرار می‌گیرد. به منظور افزایش امنیت تبادل اطلاعات در سیستم سلامت هوشمند، از الگوریتم های رمزنگاری در بستر تلفیقی مه- اینترنت اشیا استفاده می گردد.

رمز نگاری AES یک الگوریتم رمزنگاری متقارن است. رمزگشایی متن رمزگذاری شده تنها در صورتی امکان پذیر است که رمز عبور درست را بدانیم. الگوریتم AES یک الگوریتم تکراری است. هر تکرار یک دور نامیده می شود. و تعداد کل دورها ۱۲ ،۱۰ و یا ۱۴ دور است. ورودی الگوریتم یک قالب ۱۲۸ بیتی اطلاعات است که به ۱۶ بایت تقسیم می شود. همه ی عملیات های مختلف الگور یتم AES از قبیل جمع با کلید دور، جانشینی بایت ها، شیفت سطری و مخلوط کردن ستونها بر روی همین آرایه انجام میگیرد. هر دور الگوریتم AES شامل چهار عملیات است. در الگوریتم AESهم گیرنده و هم فرستنده از یک کلید مشابه برای رمزگذاری و رمزگشایی استفاده میکنند. طول متن اصلی ۱۲۸ بیت ثابت است، درحالیکه طول کلید میتوانید ۱۹۲، ۱۲۸ و یا ۲۵۶ بیت باشد. همان طور که گفته شد ورودی الگوریتم که ۱۲۸ بیت اطلاعات است که به ۱۶ بایت تقسیم شده و این بایت ها وارد آرایه ها ی 4×4 می شوند، که state نامیده می شوند. هر عضو این آرایه عنصری از میدان محدود $GF(28)$ است که بر چند جمله ای اولیه $m(x) = x^8 + x^4 + x^3 + x + 1$ بنا نهاده شده است. هر دور الگوریتم AES شامل چهار عملیات است. که دور آخر شامل سه عملیات است. این الگوریتم شامل یک سری از عملیات مرتبط است، بعضی از آنها شامل جایگزینی ورودی ها با خروجی های خاص (جایگزینی) و بعضی دیگر شامل جایگزینی بیت هایی که در اطراف آنها قرار دارد است [۱۵-۱۴]. دیدگاه پیشنهادی این پژوهش از این الگوریتم استفاده نموده و روال انجام کار را به شکل زیر مکانیزه می نماید:



شکل ۲. مراحل عملیات رمزگذاری و رمزگشایی

لذا براساس مقادیر پارامترهای ارزیابی استخراج شده از خروجی شبیه سازی ، متوسط پارامترهای ارزیابی برای دو روش امنیت در این پژوهش و SAP در بستر ابر [۱۷-۱۶]. بصورت جدول ۱. محاسبه شده است.

جدول ۱. مقایسه میانگین مقادیر پارامترهای ارزیابی طرح های احراز هویت مبتنی بر رمزگذاری

روش های امنیت	محاسبات سرویس گیرنده(ms)	محاسبات سرویس دهنده (ms)	ارتباطات (kb)	زمانبندی (ms)
دیدگاه پیشنهادی	۳۵	۱۸۹	۱۵۲۴	۴۶۹
SAP	220	276	5052	879

همانطور که در جدول ۲-۱ نشان داده شده است متوسط مقادیر تمامی پارامترهای ارزیابی در روش پیشنهادی کمتر از پروتکل SAP می باشد. در ادامه به تحلیل این مقادیر می پردازیم.

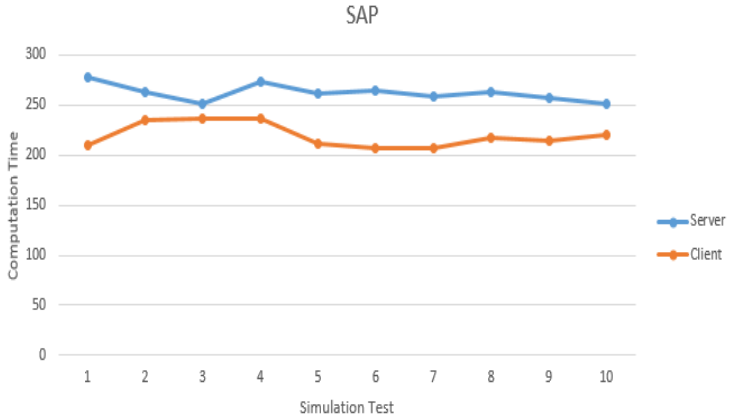
- زمان محاسبات سرویس گیرنده متوسط زمان محاسبات سرویس گیرنده در روش پیشنهادی تقریبا ۳۵ میلی ثانیه است در حالیکه این زمان برای SAP تقریبا ۲۲۰ میلی ثانیه می باشد و این بدین معناست که زمان محاسبات سرویس گیرنده در روش پیشنهادی ۱۸٪ زمان محاسبات سرویس گیرنده در SAP می باشد. لازم به ذکر است در روش پیشنهادی ، سرویس گیرنده تنها محاسبه یک امضاء و یک رمز گذاری متن رمزی را انجام می دهند، اما در SAP علاوه بر این دو محاسبه، تصدیق سرویس دهنده نیز باید صورت گیرد. به همین دلیل محاسبات سرویس گیرنده در روش پیشنهادی بسیار کمتر از SAP می باشد.

- زمان محاسبات سرویس دهنده: متوسط زمان محاسبات سرویس دهنده در روش پیشنهادی تقریبا ۱۸۹ میلی ثانیه است در حالیکه این زمان برای SAP، ۲۷۶ میلی ثانیه می باشد و این نشان دهنده این است که در روش AES-ECC زمان محاسبات سرویس دهنده ، ۷۰٪ این زمان درSAP می باشد. در روش پیشنهادی سرویس دهنده تنها محاسبه یک تأیید امضاء و بک رمز گشایی متن رمزی را انجام می دهد، اما در SAP علاوه بر این دو محاسبه، تصدیق سرویس گیرنده نیز باید صورت گیرد. به همین دلیل محاسبات سرویس دهنده در روش پیشنهادی کمتر از SAP می باشد.

- هزینه ارتباطات متوسط هزینه ارتباطات در روش پیشنهادی تقریبا ۱۵۲۴ بایت می باشد در حالیکه برای SAP، این مقدار تقریبا ۵۰۵۲ بایت می باشد. مقایسه این مقدار نشان می دهد هزینه ارتباطات در روش پیشنهادی ،۳۰٪ هزینه ارتباطات SAP می باشد. عمده ترین دلیل کاهش هزینه ارتباطات در پیشنهادی در مقایسه با SAP این است که در SAP دو گواهینامه کلید عمومی و دو امضاء RSA بین سرویس گیرنده و سرویس دهنده در شبکه منتقل می شود در حالیکه در پیشنهادی تنها یک امضاء IBS و یک متن رمزی IBE از سوی سرویس گیرنده به سرویس دهنده ارسال می شود و سرویس دهنده هیچ اطلاعات امضاء یا متن رمزی را به سرویس گیرنده نمی فرستد. بنابراین در روش پیشنهادی نسبت به SAP اطلاعات کمتری مبادله می شود که منجر به کاهش هزینه ارتباطات و در نتیجه کاهش مصرف پهنای باند شبکه می شود.

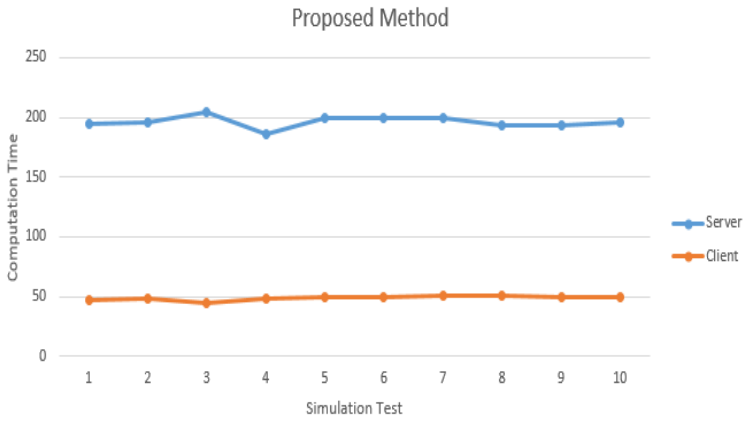
- زمان تصدیق: این پارامتر زمان صرف شده برای فرآیند اشتراک گذاری امن اطلاعات بیمار را نشان می دهد. متوسط زمان تصدیق روش پیشنهادی بصورت تقریبی ۴۶۹ میلی ثانیه است، در حالیکه این زمان برای SAP، ۸۷۹ میلی ثانیه می باشد. این امر نشاندهنده این است که در روش پیشنهادی زمان تصدیق ، تقریبا ۵۹٪ این زمان در SAP می باشد.

در شکل 2-2 نمودارهای زمان محاسبات برای الگوریتم پیشنهادی و الگوریتم SAP ترسیم شده است. همانطور که در این شکل مشاهده می شود، نمودارهای زمان محاسبات سرویس گیرنده و سرویس دهنده در SAP نزدیک به هم می باشند. براین اساس متوسط زمان سرویس گیرنده ۲۴۱ میلی ثانیه و متوسط زمان سرویس دهنده ۲۵۹ میلی ثانیه می باشد. بعبارت دیگر در روش SAP سرویس گیرنده با وجود محدودیت منابع، به اندازه ۷۵ درصد محاسبات سرویس دهنده، متحمل سربار محاسباتی می شود.



شکل ۳. نمودار زمان محاسبات SAP

از طرف دیگر، در شکل 3-2 نمودارهای زمان محاسبات سرویس گیرنده و سرویس دهنده در الگوریتم AES-ECC ارائه شده است. همانطور که مشخص است بین نمودار زمان محاسبات سرویس گیرنده با نمودار زمان محاسبات سرویس دهنده فاصله عمودی زیادی وجود دارد بطوریکه متوسط زمان محاسبات سرویس گیرنده ۵۰ میلی ثانیه و متوسط زمان محاسبات سرویس دهنده ۲۰۴ میلی ثانیه می باشد و این نشان می دهد که در الگوریتم پیشنهادی، سربار محاسباتی سرویس گیرنده حدود ۲۵ درصد سربار محاسباتی سرویس دهنده می باشد.



شکل ۴. زمان محاسبات دیدگاه پیشنهادی

با توجه به اینکه سربار محاسباتی سرویس گیرنده نسبت به سرویس دهنده در دیدگاه پیشنهادی در مقایسه با SAP بسیار کمتر می باشد، بنابراین می توان گفت که الگوریتم پیشنهادی در مقایسه با SAP به نحو بهتری با ماهیت محاسبات مه مبتنی بر اینترنت اشیا منطبق می شود. همچنین به منظور مقایسه دقیق تر، می توان الگوریتم پیشنهادی رااز نقطه نظر زمان شکست کلید رمزگذاری شده باالگوریتم های مبتنی بر لگاریتم گسسته، مبتنی بر منحنی های بیضوی، مبتنی بر امضای دیجیتال مقایسه نمود. در الگوریتم پیشنهادی، توانسته ایم میزان عملکرد امنیت شبکه با استفاده از بلاکچین را نسبت به شکسته شدن کلید افزایش دهیم از این رو می توان استدلال نمود که الگوریتم پیشنهادی در حدود ۲۸,۵۷ درصد بهتر از AES معمولی، ۱۵ درصد بهتر از DSA، ۱۸,۰۱ درصد بهتر از الگوریتم ECC و در نهایت حدود ۷,۷۶ درصد بهتر از RSA عمل می کند. به عبارت دیگر با استفاده از این مدل پیشنهادی موفق شدیم داده های رمزگذاری شده را که بعضاً اطلاعات محرمانه صاحبان حساب هستند را تا مدت بیشتری در برابر حملات ضد امنیتی افزایش دهیم و با امنیت و اطمینان بیشتری ارسال نماییم.

نتیجه‌گیری و راهکارهای آتی

همانطور که بیان شد، تعداد د ستگاه های اینترنت ا شیا علاوه بر مقدار اطلاعاتی که تولید می شـــود به طور قابل توجهی در حال افزایش اســت، بنابراین اهداف اصــلی تضــمین ایمنی دســتگاه ها، داده ها و کاربران اینترنت ا شیا ا ست. انتخاب الگوریتمی که تمام محرمانه بودن، حریم خ صو صی و در د سترس بودن را فراهم می ک ند، نقشـــی ح یاتی در ح فا ظت از کاربران و داده ها دارد. رمزگذاری و رمزگشایی رمزنگاری کلید عمومی (رمزنگاری با کلید نامتقارن) با اعمال دو کلید مختلف انجام می شـــود. این دو کلید در چنین جفت کلیدی به عنوان کلید خصوصی و عمومی شناخته می شـــوند. در رمزنگاری کلید عمومی، هر یک از طرفین نگران ارتباطات ایمن در طول انت شار کلید عمومی خود ه ستند. در این پژوهش از مدل رمزنگاری جهت سرویس های امنیتی و به عنوان یک ابزار اســاســی در امنیت شــبکه اســتفاده نمودیم. پس برای ارســـال اطلاعات حســـاب در راســـتای برقراری تراکنش مالی و محافظت آن از د ستبرد د شمن و اطمینان گیرنده از صحت پیام، لازم اســت که پیام دارای امنیت و اعتبار باشـــد. برای این منظور قبل از ارســـال پیام، آن را رمز می کنند. امروزه به منظور ارتباط امن در مکالمات تلفنی و بیســـیم های رادیویی از تکنولوژی های پی شرفته ی رمز نگاری ا ستفاده می گردد. از این رو نتایج بد ست

آمده در این پژوهش نشان می دهد که دیدگاه پیشنهادی توانسته معایب و کاستی های الگوریتم های رمزگذاری پیشین نظیر RSAT ، ECC و AES را پو شش دهد و در را ستای رمزنگاری، به نحو قابل توجهی عمل نماید. همچنین استفاده این الگوریتم در پیاده سازی بعد امنیت سخت افزاری قابلیت کاربرد دارد.

پروتکل WPA2 به عنوان آخرین و بهترین پروتکل امنیتی شبکه های بی سیم که با استفاده از محیط بلاکچین ذکر شد و همانطور که مشاهده شد در این پروتکل از الگوریتم رمزگذاری AES استفاده شده است. این الگوریتم یکی از قوی ترین و بهترین الگوریتم های رمزنگاری شناخته شده است که از نظر حافظه و سرعت با امنیت بالا نیز مطلوب است اما همانطور که دیدیم این الگوریتم به شدت در برابر حمله DPA آسیب پذیر است. از سوی دیگر، الگوریتم رمزگذاری DEA که مبتنی بر عملگرهای جبری قراردادها است، در برابر این حمله شکست ناپذیر است. در نتیجه، یک الگوریتم رمزنگاری جدید مبتنی بر فیلدهای Galva، الگوریتم رمزنگاری AES و عملگرهای جبر DEA در فصل ارائه شد. بنابراین در برابر حملات معروف شبکه های اینترنت اشیا آسیب پذیر نیست. علاوه بر این، الگوریتم پیشنهادی جداول S-Box که در الگوریتم‌های رمزگذاری بلوک قبلی رایج است، ندارد. برای ذخیره مقادیر S-Boxها نیازی به فضای حافظه ندارد. در نتیجه پیشرفت خوبی از نظر حافظه حاصل شد که یکی از نقاط قوت این الگوریتم محسوب می شود، زیرا نیاز به حافظه از نوع ROM را در پیاده سازی سخت افزاری آن کاهش می دهد و با حداقل مدار منطقی قابل پیاده سازی است. از طرفی با حذف روال های ناوبری و جستجوی مربوط به این جداول، سرعت نیز افزایش یافت.

مراجع

[1] Hassen, Hafedh Ben, Nadia Ayari, and Belgacem Hamdi. "A home hospitalization system based on the Internet of things, Fog computing and cloud computing." Informatics in Medicine Unlocked, vol. 20, pp. 136-148, 2020.

[2] Tuli, Shreshth, Nipam Basumatary, Sukhpal Singh Gill, Mohsen Kahani, Rajesh Chand Arya, Gurpreet Singh Wander, and Rajkumar Buyya. "HealthFog: An ensemble deep learning based Smart Healthcare System for Automatic Diagnosis of Heart Diseases in integrated IoT and fog computing environments." Future Generation Computer Systems, vol. 104, pp. 187-200, 2020.

[3] Karthika, P., R. Ganesh Babu, and P. A. Karthik. "Fog computing using interoperability and IoT security issues in health care." In Springer Micro-Electronics and Telecommunication Engineering, pp. 97-105., 2020.

[4] Rincon, Jaime A., Solanye Guerra-Ojeda, Carlos Carrascosa, and Vicente Julian. "An IoT and Fog Computing-Based Monitoring System for Cardiovascular Patients with Automatic ECG Classification Using Deep Neural Networks." Sensors, vol. 20, no. 24, pp. 735-746, 2020.

[5] Bradley, D., Russell, D., Ferguson, I., Isaacs, J., MacLeod, A., & White, R. (2015). The Internet of Things–The future or the end of mechatronics. Mechatronics, 27, 57-74.

[6] Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). Fog computing: A platform for internet of things and analytics. In Big data and internet of things: A roadmap for smart environments (pp. 169-186). Springer, Cham.

[7] Shammar EA, Zahary AT, Al-Shargabi AA. A survey of IoT and blockchain integration: Security perspective. IEEE Access. 2021 Nov 19;9:156114-50.

[8] Sultan A, Mushtaq MA, Abubakar M. IOT security issues via blockchain: a review paper. InProceedings of the 2019 international conference on blockchain technology 2019 Mar 15 (pp. 60-65).

[9] Shammar EA, Zahary AT, Al-Shargabi AA. A survey of IoT and blockchain integration: Security perspective. IEEE Access. 2021 Nov 19;9:156114-50.

[10] Uckelmann, D., Harrison, M., & Michahelles, F. (Eds.). (2011). Architecting the internet of things. Springer Science & Business Media.

[11] Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.

[12] Banerjee M, Lee J, Choo KK. A blockchain future for internet of things security: a position paper. Digital Communications and Networks. 2018 Aug 1;4(3):149-60.

[13] Hafsa A, Sghaier A, Malek J, Machhout M. Image encryption method based on improved ECC and modified AES

[16] Smith J, Fathima SA. Securing IoT Networks in Smart Homes: Advanced Encryption Techniques and Authentication Protocols.

[17] Ugbedeojo M, Adebiyi MO, Aroba OJ, Adebiyi AA. RSA and Elliptic Curve Encryption System: A Systematic Literature Review. International Journal of Information Security and Privacy (IJISP). 2024 Jan 1;18(1):1-27.

algorithm. Multimedia Tools and Applications. 2021 May;80:19769-801.

[14] Hafsa A, Sghaier A, Zeghid M, Malek J, Machhout M. An improved co-designed AES-ECC cryptosystem for secure data transmission. International Journal of Information and Computer Security. 2020;13(1):118-40.

[15] JR MN, Lutimath NM. AN ENHANCED AES-ECC MODEL FOR THE SECURITY OF MOBILE APPLICATIONS USING CLOUD COMPUTING. Computer Integrated Manufacturing Systems. 2023 Apr 16;29(4):116-27.