ارائهٔ یک رویکرد مبتنی بر بلاک‌چین برای خودکارسازی تضمین صحت و محرمانگی داده‌های ثبت رخداد

فاطمه آملی[۱]، مصطفی بستام[۲*]، احسان عطائی[۳]

دانش‌آموختهٔ کارشناسی‌ارشد، گروه مهندسی کامپیوتر، دانشکدهٔ فناوری و مهندسی، دانشگاه مازندران، بابلسر، ایران[۱]

استادیار، گروه مهندسی کامپیوتر، دانشکدهٔ فناوری و مهندسی، دانشگاه مازندران، بابلسر، ایران[۲*]

دانشیار، گروه مهندسی کامپیوتر، دانشکدهٔ فناوری و مهندسی، دانشگاه مازندران، بابلسر، ایران[۳]

چکیده

با افزایش تهدیدات سایبری، داده‌های ثبت رخداد به‌عنوان منبعی کلیدی برای شناسایی و تحلیل حوادث امنیتی شناخته می‌شوند و بینش‌های ارزشمندی از فعالیت‌های سامانه ارائه می‌دهند؛ بااین‌حال، هرگونه دست‌کاری در این داده‌ها می‌تواند دقت تحلیل‌های امنیتی را کاهش داده و تصمیم‌گیری‌های مرتبط با امنیت را تحت تأثیر قرار دهد. فناوری بلاک‌چین با ویژگی‌هایی نظیر غیرمتمرکزبودن، شفافیت و تغییرناپذیری بستری قابل اعتماد برای تضمین صحت داده‌ها فراهم می‌کند. در این پژوهش، به جای ذخیره‌سازی مستقیم داده‌های خام که پرهزینه و محدودکننده‌است، چارچوبی خودکار معرفی شده‌است که از بلاک‌چین عمومی اتریوم و قراردادهای هوشمند برای ذخیرهٔ هش رمزنگاری‌شده داده‌های ثبت رخداد استفاده می‌کند. این روش با کاهش هزینه‌های ذخیره‌سازی، در عین حفظ محرمانگی و امکان راستی‌آزمایی داده‌ها، کارایی بالایی ارائه می‌دهد. فرایند تضمین صحت داده‌ها در دو مرحله انجام می‌شود: ثبت و مقایسهٔ دوره‌ای هش‌ها و اعتبارسنجی دسته‌ای در بازه‌های زمانی بلندتر برای کشف هرگونه دست‌کاری احتمالی. ارزیابی این مدل در شبکهٔ آزمایشی سپولیا نشان داده‌است که هزینه‌های عملیاتی و سربار پردازشی بهینه شده و امکان استفاده از این روش در مقیاس وسیع فراهم است. این پژوهش، روشی نوآورانه و عملی برای خودکارسازی تضمین صحت داده‌های ثبت رخداد ارائه می‌دهد و راه‌کاری قابل اتکا برای ارتقای امنیت اطلاعات در کاربردهای واقعی پیشنهاد می‌کند.

واژگان کلیدی: مدیریت داده‌های ثبت رخداد، صحت داده‌ها، بلاک‌چین، اتریوم، قرارداد هوشمند.

A Blockchain-Driven Approach to Automating Event Log Data Integrity and Confidentiality

Fatemeh Amoli[1], Mostafa Bastam[2]*, Ehsan Ataie[3]

M.Sc. Graduate, Department of Computer Engineering, Faculty of Engineering and Technology, University of Mazandaran, Babolsar, Iran[1]

Assistant Professor, Department of Computer Engineering, Faculty of Engineering and Technology, University of Mazandaran, Babolsar, Iran[2]*

Associate Professor, Department of Computer Engineering, Faculty of Engineering and Technology, University of Mazandaran, Babolsar, Iran[3]

Abstract

With the rapid rise of cybersecurity threats and the increasing complexity of digital security, event log data serves as a critical source for identifying and analyzing cyberattacks and threats. This data provide key insights into system activities, essential for detecting unauthorized intrusions, analyzing suspicious behaviors, and conducting security investigations. However, any alteration or tampering with the data can disrupt the analysis and detection processes, leading to incorrect security decisions.

* نویسندهٔ عهده‌دار مکاتبات

* Corresponding author

• تاریخ ارسال مقاله: ۱۴۰۳/۰۹/۲۶ • تاریخ پذیرش: ۱۴۰۴/۰۴/۲۹ • تاریخ انتشار: ۱۴۰۴/۶/۲۲ • نوع مطالعه: پژوهشی

[DOI: 10.61882/jsdp.22.2.65]

Blockchain technology, with its unique features such as decentralization, immutability, and transparency, has been recognized as a reliable and secure platform for storing and protecting data. This technology enables the storage of data hashes in a way that any changes can be easily detected. However, directly storing the vast volume of event log data on the blockchain faces challenges such as high costs and storage space limitations.

In this research, an innovative model has been presented to automate the assurance of event log data integrity and confidentiality using the public Ethereum blockchain and smart contracts. Instead of storing event log data directly, only their hashes have been saved on the blockchain. This approach not only reduces storage costs but also ensures data confidentiality.

The automated data integrity assurance process in this model occurs in two stages:

1. **Stage One: Event log data hashes have been periodically stored on the blockchain and compared with previous hashes.**
2. **Stage Two: Over longer intervals, all stored hashes have been reviewed and validated to prevent any potential tampering.**

In this study, the costs associated with implementing this model on the Ethereum Sepolia test network had been precisely calculated. The analysis indicates that operational costs and computational overhead have been optimized across different time intervals, demonstrating the model's feasibility for large-scale deployment.

Ultimately, this research tries to introduce a novel and practical model, taking a significant step toward automating the assurance of event log data integrity and confidentiality, providing a reliable solution for real-world applications.

Keywords: Log management, Data integrity, Blockchain, Ethereum, Smart Contract.

۱-مقدمه

با گسترش روزافزون تهدیدات سایبری و پیچیدگی‌های امنیتی در دنیای دیجیتال امروزی، سازمان‌ها بیش‌ازپیش نیازمند ابزارهای مؤثر و قابل اعتماد برای حفاظت از داده‌های حساس خود هستند؛ در این راستا، داده‌های ثبت رخداد[1] به‌عنوان یکی از منابع کلیدی برای شناسایی و مقابله با تهدیدات نقش حیاتی دارند. این داده‌ها شامل جزئیاتی از فعالیت‌های سامانه‌ها هستند که می‌توانند اطلاعات مهمی در خصوص حملات سایبری، نقض‌های امنیتی و رفتارهای مشکوک ارائه دهند؛ بااین‌حال، دست‌کاری یا حذف این داده‌ها می‌تواند به‌راحتی منجر به ازبین‌رفتن شواهد ضروری و ایجاد چالش‌های جدی در فرایندهای پژوهش‌های امنیتی و قضایی شود[۱, ۲]؛ در این میان، فناوری بلاک‌چین[2] به‌دلیل ویژگی‌های منحصربه‌فرد خود مانند غیرمتمرکزبودن، شفافیت و تغییرناپذیری توجه بسیاری از پژوهش‌گران را به خود جلب کرده‌است. بلاک‌چین به‌عنوان یک بستر ذخیره‌سازی امن و قابل اعتماد می‌تواند فرایند ثبت و حفظ داده‌ها را به شکلی که امکان تغییر یا دست‌کاری آن‌ها وجود نداشته باشد، تضمین کند؛ به این ترتیب، این فناوری قادر است، نقش مهمی در محافظت از یک‌پارچگی داده‌های ثبت رخداد ایفا و از اعتبار این داده‌ها در فرایندهای تحلیل تهدیدات و حملات سایبری اطمینان حاصل کند[۳]؛ بااین‌حال، استفاده از بلاک‌چین در ذخیره‌سازی داده‌های ثبت رخداد با چالش‌های خاصی روبه‌رو است؛ حجم بالای داده‌های تولیدی و سرعت بالای ایجاد آن‌ها، به‌علاوه هزینه‌ها و محدودیت‌های ناشی از ذخیره‌سازی بر روی بلاک‌چین مشکلاتی را در استفادهٔ گسترده از این فناوری ایجاد کرده‌است[۴, ۵]. در بسیاری از پژوهش‌ها، راه‌حل‌هایی برای کاهش هزینه‌ها و بهینه‌سازی فرایند ذخیره‌سازی بلاک‌چین ارائه شده‌است؛ اما بیشتر این مطالعات به جنبه‌های خودکارسازی و خودکفاکردن فرایندهای ذخیره‌سازی و تضمین صحت داده‌ها توجه نکرده‌اند.

این پژوهش با هدف رفع این کمبود، مدلی نوآورانه برای تضمین صحت و یک‌پارچگی داده‌های ثبت رخداد ارائه می‌دهد که از ویژگی‌های بلاک‌چین عمومی اتریوم[3] و قراردادهای هوشمند[4] بهره می‌برد. این مدل فرایند ثبت هش[5] داده‌های رخداد را به‌صورت خودکار و غیرمتمرکز انجام داده و از این طریق، نه‌تنها صحت داده‌ها را به‌طور مؤثر تضمین می‌کند، بلکه هزینه‌های ذخیره‌سازی و زمان پردازش را نیز به کمینه می‌رساند. در این پژوهش، علاوه‌بر ارائهٔ مدل پیشنهادی، پیاده‌سازی این مدل و تحلیل هزینه‌های آن نیز مورد بررسی قرار می‌گیرد. مقالهٔ حاضر به شرح زیر ساختار یافته است: در بخش دوم، پژوهش‌های مرتبط بررسی می‌شود. بخش سوم به ارائهٔ مدل پیشنهادی و بخش چهارم به بررسی چگونگی پیاده‌سازی روش پیشنهادی و ارزیابی نتایج حاصله معطوف شده‌است؛ درنهایت، در بخش پنجم، نتیجه‌گیری و پیشنهادها برای پژوهش‌های آینده آورده شده‌است.

۲- کارهای مرتبط

مطالعات پیشین به‌طور گسترده‌ای به ارائهٔ راه‌کارهای مختلف برای استفاده از بلاک‌چین به‌منظور تضمین صحت داده‌های

[1] Log Files
[2] Blockchain
[3] ETHEREUM
[4] Smart Contract
[5] Hashing

[DOI: 10.61882/jsdp.22.2.65]

مختلف پرداخته‌اند و هر یک سعی داشته‌اند چالش‌های مربوط به حجم بالای داده‌ها و هزینه‌های ذخیره‌سازی در بلاک‌چین را برطرف کنند؛ بااین‌حال، پژوهش‌های موجود بیشتر بر جنبه‌های نظری و فنی تمرکز داشته‌اند و به‌طور محدود به موضوع خودکارسازی فرایند تضمین امنیت داده‌ها و تحلیل هزینه‌های آن پرداخته‌اند. بسیاری از پژوهش‌گران به ترکیب بلاک‌چین با فناوری‌های مکمل مانند IPFS [1] پرداخته‌اند تا چالش‌های مقیاس‌پذیری و هزینه‌های ناشی از ذخیره‌سازی داده‌ها در بلاک‌چین را کاهش دهند. **IPFS** یک پروتکل ذخیره‌سازی و اشتراک‌گذاری فایل غیرمتمرکز است که از آدرس‌دهی محتوا[2] برای شناسایی داده‌ها استفاده می‌کند. این سامانه به‌صورت همتابه‌همتا عمل می‌کند و داده‌ها را به‌صورت توزیع‌شده بین گره‌ها ذخیره می‌کند که باعث افزایش کارایی، امنیت می‌شود[۴]. مطالعات [۶-۸] با ذخیرهٔ داده‌های حجیم در **IPFS** و ثبت هش آن‌ها در بلاک‌چین، به کاهش قابل توجه هزینه‌های ذخیره‌سازی دست یافته‌اند.

در حوزهٔ محاسبات ابری، بلاک‌چین به‌عنوان یک لایهٔ امنیتی برای حفاظت از داده‌ها مطرح شده‌است. مطالعات [۹, ۱۰] راه‌کارهایی برای استفاده از بلاک‌چین در تأمین امنیت و یک‌پارچگی داده‌های ثبت رخداد در محیط‌های ابری[3] ارائه داده‌اند؛ همچنین تاگوچی و همکاران [۱۱] طراحی مبتنی بر بلاک‌چین برای ذخیره‌سازی داده‌های ثبت رخداد در ابرهای عمومی[4] را پیشنهاد کرده‌اند. آوسون دیوید و همکاران [۱۲]، چهارچوبی برای کاهش چالش‌های پیش‌روی بازرسان در به‌دست‌آوردن شواهد قابل‌قبول از اکوسامانه‌های ابری ارائه کرده‌اند که از بلاک‌چین برای ذخیره‌سازی این شواهد استفاده می‌کند؛ علاوه‌بر این، تیان و همکاران [۱۳] یک طرح حسابرسی عمومی برای گزارش رفتار کاربران در محیط‌های ابری مشترک پیشنهاد داده‌اند که بر پایهٔ بلاک‌چین بنا شده‌است.

ترکیب بلاک‌چین با سایر فناوری‌ها مانند یادگیری ماشین[5] و اینترنت اشیا[6] نیز مورد توجه پژوهش‌گران قرار گرفته است. آلتولیان و همکاران [۱۴] با استفاده از قراردادهای هوشمند، امنیت و یک‌پارچگی داده‌های تولیدشده به‌وسیلهٔ اینترنت اشیا را بهبود بخشیده‌اند؛ همچنین لی و همکارانش [۱۵] یک سامانه ذخیره‌سازی توزیع‌شده برای داده‌های آتش‌نشانی اینترنت اشیا ارائه داده‌اند که بر پایهٔ بلاک‌چین و **IPFS** ساخته شده‌است. در حوزهٔ سلامت، جاوید و همکارانش [۱۶] یک سامانه امنیتی مبتنی بر بلاک‌چین برای جلوگیری از دست‌کاری داده‌های پزشکی پیشنهاد داده‌اند و همچنین خور و همکارانش [۱۷] روشی برای تأیید امنیت داده‌های دستگاه‌های اینترنت اشیا کم‌مصرف ارائه کرده‌اند.

به‌طور خاص، پژوهش‌های [۱۸, ۱۹] رویکردهای مختلفی را برای ذخیره‌سازی ایمن و کارآمد داده‌های ثبت رخداد بر روی بلاک‌چین پیشنهاد داده‌اند. همهٔ این مقالات بر افزایش امنیت داده‌ها و جلوگیری از دست‌کاری آن‌ها تمرکز دارند و از روش‌های مختلفی مانند قراردادهای هوشمند، درخت مرکل[7]، **IPFS** و یادگیری ماشین برای بهبود عملکرد سامانه استفاده می‌کنند. به طور خاص، پوتز و همکارانش [۱۸] بر عملکرد بالا و مقاومت در برابر حملات تأکید دارند. علی و همکارانش [۲۰] از **Elasticsearch** برای ذخیرهٔ اسناد **JSON** استفاده کرده‌اند و از یادگیری ماشین برای شناسایی تهدیدات بهره برده‌اند. لی و همکارانش [۲۱] از قراردادهای هوشمند **ABAC** [8] برای کنترل دسترسی به داده‌ها استفاده کرده‌اند و بر جست‌وجوی سریع داده‌ها متمرکز شده‌اند. جین و همکاران [۷] از **IPFS** برای ذخیرهٔ داده‌های خام و بلاک‌چین برای ذخیرهٔ هش‌ها استفاده کرده‌اند و بر کاهش هزینه‌های تراکنش متمرکز شده‌اند؛ همچنین، جیانگ و همکاران [۲۲] از درخت مرکل چهارگانه برای تأیید یک‌پارچگی داده‌ها استفاده کرده‌اند و به کاهش هزینه‌های ذخیره‌سازی در بلاک‌چین پرداخته‌اند. همهٔ این مطالعات نشان می‌دهند که بلاک‌چین می‌تواند به‌عنوان یک فناوری کلیدی برای ایجاد سامانه‌های ذخیره‌سازی داده‌های امن و قابل اعتماد عمل کند.

در این پژوهش، روشی نوآورانه برای تضمین امنیت داده‌های ثبت رخداد با استفاده از بلاک‌چین اتریوم و قراردادهای هوشمند ارائه شده‌است. این روش با خودکارسازی فرایند ثبت هش داده‌های ثبت رخداد از هرگونه دست‌کاری در داده‌ها جلوگیری می‌کند و به طور قابل اعتماد، صحت و اصالت آن‌ها را تأیید می‌کند؛ علاوه‌بر این، با تحلیل دقیق هزینه‌ها، کارایی و مقرون‌به‌صرفه‌بودن این روش بررسی شده‌است. در مقایسه با مطالعات پیشین روش پیشنهادی با ارائهٔ یک راه‌کار عملی و قابل اجرا برای محیط‌های واقعی، گامی مهم در جهت کاربردی‌سازی فناوری بلاک‌چین در حوزهٔ امنیت اطلاعات برداشته‌است. جدول (۱) مقایسه‌ای بین کارهای انجام‌شده و روش پیشنهادی را نشان می‌دهد.

از دیگر امتیازات برجستهٔ این پژوهش می‌توان به پیاده‌سازی عملی مدل پیشنهادی و ارزیابی دقیق نتایج حاصل از آن اشاره کرد که اعتبار و قابلیت اطمینان نتایج پژوهش را به‌طور قابل توجهی افزایش داده‌است.

[1] InterPlanetary File System
[2] Content Addressing
[3] Cloud
[4] Public Cloud
[5] Machine Learning
[6] Internet of Things
[7] Merkle tree
[8] Attribute-Based Access Control contract

[DOI: 10.61882/jsdp.22.2.65]

(جدول-۱): مقایسهٔ کارهای مرتبط

(Table-1): Work comparison table

پشتیبانی خودکار	پلتفرم بلاک‌چین	قرارداد هوشمند	الگوریتم هش	نوع بلاک‌چین	محرمانگی لاگ	صحت لاگ	مرجع
خیر	اتریوم	بله	SHA256-Keccak256	عمومی	بله	بله	[۱۶]
خیر	Fabric	بله	CID of IPFS	خصوصی	بله	بله	[۱۷]
خیر	EXONUM	بله	SHA256	مجاز	بله	بله	[۲۰]
خیر	Multichain	بله	SHA256	خصوصی	بله	بله	[۲۱]
خیر	اتریوم	بله	SHA256	عمومی	بله	بله	[۷]
خیر	اتریوم	بله	CID of IPFS	عمومی	خیر	بله	[۲۲]
بله	سپولیا اتریوم	بله	SHA256	عمومی	بله	بله	روش پیشنهادی

۳- روش پیشنهادی

در شکل (۱) نمای کلی از روش پیشنهادی آورده شده‌است. مدل پیشنهادی این مقاله برای تضمین خودکار صحت داده‌های ثبت رخداد از فناوری بلاک‌چین و قراردادهای هوشمند استفاده می‌کند. این مدل با ذخیره‌سازی هش داده‌ها در بلاک‌چین از یک‌پارچگی داده‌ها محافظت می‌کند و در عین حال، محرمانگی آن‌ها را حفظ کرده و امکان تأیید صحت داده‌ها را فراهم می‌آورد؛ علاوه‌براین، در این مدل تلاش شده‌است تا هزینه‌های عملیاتی مرتبط با ذخیره‌سازی داده‌ها و پردازش محاسباتی به‌دقت محاسبه شود. در ادامه، جزئیات این روش شرح داده خواهد شد؛ با این حال، پیش از پرداختن به این جزئیات ضروری است که برخی از مفاهیم و ابزارهای مورد استفاده در این پژوهش تعریف و توضیح داده شوند.

۳-۱-تعاریف

در این بخش برخی از مفاهیم کلیدی و اساسی که در مدل پیشنهادی استفاده شده‌اند، توضیح داده شده‌است.

بلاک‌چین: یک فناوری غیرمتمرکز برای ذخیره‌سازی داده‌ها است که به‌طور عمده در ارزهای دیجیتال استفاده می‌شود. این فناوری از زنجیره‌ای از بلوک‌ها تشکیل شده که هر بلوک شامل مجموعه‌ای از تراکنش‌ها یا داده‌ها است. بلاک‌چین به‌دلیل ویژگی‌های امنیتی خود مانند تغییرناپذیری، شفافیت و توزیع داده‌ها در میان گره‌های مختلف شبکه برای بسیاری از کاربردهای امنیتی و ذخیره‌سازی داده‌ها مناسب است.

قرارداد هوشمند: یک برنامهٔ رایانه‌ای است که بر روی بلاک‌چین اجرا می‌شود[۲۲] و به‌طور خودکار شرایط قرارداد را بر اساس ورودی‌های داده‌شده اجرا می‌کند. این قراردادها به طور معمول به زبان‌های برنامه‌نویسی خاص مانند سالیدیتی نوشته می‌شوند و برای انجام تراکنش‌ها یا پردازش اطلاعات در بلاک‌چین بدون نیاز به واسطه یا شخص ثالث طراحی شده‌اند[۲۳].

هش: فرایندی است که در آن داده‌های ورودی از هر اندازه به یک مقدار ثابت و کوتاه به نام «هش» تبدیل می‌شوند. هش‌ها برای تضمین یک‌پارچگی داده‌ها استفاده می‌شوند؛ به این معنی که اگر داده‌های ورودی تغییر کنند، هش خروجی به‌طور قابل توجهی تغییر خواهد کرد. الگوریتم‌هایی مانند **SHA-256** برای تولید هش‌ها استفاده می‌شوند. در این مقاله برای تضمین صحت داده‌های ثبت رخداد از هش داده‌ها استفاده شده‌است.

ذخیره‌سازی داده‌ها در بلاک‌چین: بر حسب معمول به‌دلیل هزینه‌های بالا و محدودیت‌های فضایی صورت نمی‌گیرد. در این مقاله تنها هش داده‌های ثبت رخداد در بلاک‌چین ذخیره می‌شود تا ضمن حفظ محرمانگی داده‌ها از صحت آن‌ها نیز اطمینان حاصل شود. این روش از ذخیره‌سازی داده‌های خام جلوگیری می‌کند و در عین حال امکان تأیید صحت داده‌ها را فراهم می‌آورد.

سپولیا:[1] یکی از شبکه‌های آزمایشی[2] اتریوم است که برای آزمایش و ارزیابی قراردادهای هوشمند استفاده می‌شود. این شبکه مشابه شبکهٔ اصلی اتریوم عمل می‌کند، اما تراکنش‌ها و هزینه‌ها در آن به‌صورت آزمایشی انجام می‌شود. سپولیا به توسعه‌دهندگان این امکان را می‌دهد که پیش از استقرار قراردادهای هوشمند در شبکهٔ اصلی اتریوم آن‌ها را آزمایش کنند.

[1] Sepolia
[2] Testnet

[DOI: 10.61882/jsdp.22.2.65]

متامسک:[1] یک کیف پول دیجیتال برای تعامل با بلاک‌چین‌های اتریوم و سایر بلاک‌چین‌هاست. این کیف پول به کاربران این امکان را می‌دهد که به‌راحتی از طریق مرورگر یا اپلیکیشن موبایل خود، به بلاک‌چین متصل شوند و تراکنش‌ها را انجام دهند؛ همچنین متامسک ابزار مناسبی برای ارتباط با شبکه‌های آزمایشی مانند سپولیا فراهم می‌آورد و برای توسعه‌دهندگان به‌عنوان یک ابزار مفید برای استقرار و مدیریت قراردادهای هوشمند عمل می‌کند.

۳-۲-شرح روش پیشنهادی

روش پیشنهادی به‌گونه‌ای طراحی شده‌است که صحت داده‌های ثبت رخداد را به‌صورت خودکار و در دو مرحله به کاربر اطلاع می‌دهد. در این روش از بلاک‌چین به‌عنوان یک پایگاه دادهٔ امن برای ذخیرهٔ داده‌های ثبت رخداد استفاده شده‌است؛ بااین‌حال، باید توجه داشت که ذخیره‌سازی داده‌ها روی بلاک‌چین هزینه‌بر است؛ همچنین به‌دلیل ویژگی‌های مشخص بلاک‌چین، این روش با هدف تضمین صحت داده‌های ثبت رخداد از طریق ذخیره‌سازی آن‌ها بر روی بلاک‌چین طراحی شده‌است. داده‌های ثبت رخداد که به‌عنوان اطلاعات اصلی فعالیت‌ها در سطح شبکه محسوب می‌شوند، نیازمند حفظ محرمانگی‌اند، اما از آنجا که داده‌های ذخیره‌شده در بلاک‌چین برای تمامی اعضای شبکه قابل مشاهده‌اند، این مسئله با لزوم حفظ محرمانگی این داده‌ها تناقض دارد؛ بنابراین با درنظرگرفتن دو عامل مهم، یعنی هزینهٔ بالای ذخیره‌سازی داده در بلاک‌چین و ضرورت حفظ محرمانگی داده‌های ثبت رخداد پیشنهاد می‌شود به جای ذخیرهٔ مستقیم این داده‌ها تنها هش آن‌ها روی بلاک‌چین ذخیره شود.

در این روش از یک تابع که بر روی یک سرور در حال اجرا است استفاده می‌شود. این تابع از داده‌های ثبت رخداد سامانه در بازه‌های زمانی مشخص هش می‌گیرد و هش‌ها با استفاده از توابع قرارداد هوشمند در یک آرایه روی بلاک‌چین ذخیره می‌شوند.

برای تضمین خودکار صحت داده‌ها، تابع مورد نظر در بازه‌های زمانی مشخص اجرا شده و با فراخوانی توابع قرارداد هوشمند، هش جدید محاسبه‌شده از داده‌های ثبت رخداد بر روی شبکهٔ بلاک‌چین ذخیره می‌شود. در زمان ذخیرهٔ هش جدید آخرین هش پیشین با هش مجددی که از داده‌های ثبت رخداد در بازه پیشین گرفته شده‌است، مقایسه می‌شود. درصورت مغایرت، به کاربر اطلاع داده می‌شود و به این ترتیب، به‌صورت خودکار از تغییرات صورت‌گرفته در داده‌های ثبت رخداد آگاه می‌شود. از طرفی، آرایهٔ مورد نظر در بازهٔ طولانی‌تری (که در ارزیابی‌ها یک روز در نظر گرفته شده‌است) بازنشانی می‌شود. در زمان بازنشانی، دوباره از داده‌های ثبت رخداد سامانه در همان بازه‌ها هش گرفته‌شده و با هش‌های ذخیره‌شده در بلاک‌چین مقایسه می‌شود و درصورت مغایرت به کاربر اطلاع داده می‌شود با استفاده از این روش دو مرحله‌ای، اطمینان بیشتری از صحت داده‌ها به‌دست می‌آید. این رویکرد به‌ویژه در برابر نفوذگرانی مؤثر است که امکان دارد، پس از انجام اقدامات مخرب، تنها داده‌های ثبت رخداد مربوط به بازه زمانی ورود خود را حذف کنند؛ داده‌هایی که ممکن است متعلق به بازه‌های زمانی متعددی پیش از بازه زمانی فعلی باشند. درصورتی‌که صحت‌سنجی تنها به‌صورت یک‌مرحله‌ای و محدود به داده‌های ثبت رخداد بازه زمانی قبلی انجام شود، روش پیشنهادی در چنین مواردی عملکرد مطلوبی نخواهد داشت؛ به همین دلیل، صحت‌سنجی باید طی دو مرحله انجام شود. در مرحلهٔ نخست، داده‌های ثبت رخداد مربوط به بازه زمانی پیشین مورد صحت‌سنجی قرار می‌گیرند؛ سپس در انتهای بازه زمانی دوم، صحت داده‌های ثبت رخداد متعلق به چندین بازه زمانی به‌صورت هم‌زمان بررسی می‌شود. این رویکرد باعث افزایش دقت و اطمینان در تضمین صحت داده‌ها می‌شود. انتخاب این بازه‌های زمانی، شامل: ۱) بازه زمانی کوتاه‌تر و مشخص برای ذخیرهٔ هش داده‌های ثبت رخداد روی بلاک‌چین و ۲) زمان بازنشانی آرایهٔ حاوی هش‌ها بسیار حائز اهمیت است. این انتخاب باید به‌گونه‌ای باشد که هم هزینهٔ مالی کمتری به همراه داشته باشد و هم از هدف خود، یعنی تضمین صحت داده‌های ثبت رخداد دور نشود.

۳-۳- پارامترهای مهم در روش پیشنهادی

در روش پیشنهادی برای تضمین صحت داده‌های ثبت رخداد به‌صورت خودکار در دو مرحله چندین پارامتر وجود دارد که تأثیر مستقیمی بر دست‌یابی به اهداف این روش دارند. این پارامترها در ادامه توضیح داده می‌شوند:

نوع الگوریتم هش: یکی از پارامترهای کلیدی است. این پارامتر هم بر مدت زمان مورد نیاز برای هش‌گرفتن از داده‌ها تأثیر دارد و هم بر طول رشتهٔ هش. از آنجا که طول رشتهٔ هش بر میزان هزینهٔ ذخیره‌سازی آن در بلاک‌چین تأثیر می‌گذارد، نوع الگوریتم تأثیر زیادی بر دو جنبهٔ هزینه، یعنی سربار زمانی و هزینهٔ مالی خواهد داشت.

[1] MetaMask

[DOI: 10.61882/jsdp.22.2.65]

حجم داده‌های ثبت رخداد: در مدت زمان مشخص‌شده برای هش‌گرفتن از این داده‌ها به‌وسیلهٔ سرور تأثیر مستقیم دارد؛ به عبارت دیگر حجم بیشتر داده‌ها باعث افزایش سربار زمانی برای هش‌گرفتن از آن‌ها خواهد شد؛ بنابراین هرچه حجم داده‌ها بزرگ‌تر باشد، زمان بیشتری برای پردازش و هش‌گرفتن از آن‌ها نیاز است.

طول رشته‌های هش: که از هش‌گرفتن از داده‌های ثبت رخداد در بازه‌های زمانی مشخص به‌دست می‌آید، بر هزینهٔ ذخیره‌سازی داده‌ها در بلاک‌چین تأثیر زیادی دارد. هر الگوریتم هش خروجی با طول متفاوتی تولید می‌کند؛ برای مثال خروجی الگوریتم SHA-256 یک رشتهٔ ۳۲ بایتی است. این تفاوت طول رشته‌های هش می‌تواند تأثیر زیادی بر هزینهٔ ذخیره‌سازی در بلاک‌چین داشته باشد.

بازه زمانی برای هش‌گرفتن از داده‌ها: یکی دیگر از پارامترهای تأثیرگذار است؛ هرچه این بازه زمانی کوتاه‌تر باشد، فرایند تضمین صحت داده‌ها مؤثرتر خواهد بود، اما هزینهٔ ذخیره‌سازی هش‌ها در بلاک‌چین بیشتر می‌شود؛ بنابراین انتخاب بازه زمانی بر عملکرد و هزینه‌گذاری سامانه تأثیر مستقیم دارد. هزینهٔ استقرار قراردادهای هوشمند: که تنها یک بار انجام می‌شود، نیز جزو پارامترهای مهم است. این هزینه بستگی به نحوهٔ نوشتن قرارداد هوشمند دارد. در این مدل، تلاش شده‌است تا قرارداد هوشمند به بهینه‌ترین شکل ممکن نوشته شود تا هزینه‌ها به حداقل برسد.

هزینهٔ خواندن داده از بلاک‌چین: که در پایان هر دورهٔ زمانی تعیین‌شده باید محاسبه شود، پارامتر دیگری است که باید در نظر گرفته شود. این هزینه به‌ویژه زمانی که نیاز به دسترسی به داده‌ها برای بررسی وضعیت هش‌ها وجود دارد، مهم است.

طول آرایهٔ هش‌ها: هر چه بیشتر باشد، هزینهٔ بازنشانی آن نیز افزایش خواهد یافت. این پارامتر باید در طراحی سامانه دقیق مورد توجه قرار گیرد تا از افزایش بی‌مورد هزینه‌ها جلوگیری شود.

بازه زمانی برای بازنشانی آرایهٔ هش‌ها: نیز تأثیر زیادی بر هزینهٔ حذف داده‌ها از بلاک‌چین دارد؛ هرچه این بازه زمانی طولانی‌تر باشد، تعداد هش‌هایی که باید ذخیره شوند، بیشتر خواهد بود و درنتیجه آرایه بزرگ‌تر می‌شود. این افزایش اندازهٔ آرایه هزینه‌های اضافی برای بازنشانی و حذف داده‌ها از بلاک‌چین را به همراه خواهد داشت.

۳-۴-رویهٔ اجرای مدل پیشنهادی

روش پیشنهادی با هدف بررسی خودکار تغییرات در داده‌های ثبت رخداد طراحی شده‌است. در این روش، هش این داده‌ها در فواصل زمانی معین محاسبه شده و در بلاک‌چین ذخیره می‌شوند تا امکان تشخیص هرگونه تغییر فراهم شود. این پروتکل شامل دو بازه زمانی مجزا است:

بازه زمانی کوتاه‌مدت: اجرا در فواصل پانزده دقیقه‌ای

بازه زمانی بلندمدت: اجرا در انتهای هر دورهٔ ۲۴ ساعته

در ابتدا، قرارداد هوشمند مستقرشده بر بستر بلاک‌چین، همچنین آرایه‌ای به نام logHashes به‌منظور ذخیره‌سازی هش‌ها مقداردهی اولیه می‌شود؛ سپس داده‌های ثبت رخداد به‌طور دوره‌ای هش شده و به‌صورت ایمن در بلاک‌چین ذخیره می‌شوند. در هر بازه زمانی کوتاه‌مدت، تابع (StoreHash) اجرا می‌شود. مراحل آن به‌صورت زیر است:

۱. دریافت داده‌های ثبت رخداد مربوط به پانزده دقیقهٔ گذشته
۲. محاسبهٔ هش جدید از داده‌ها
۳. بازیابی هش پیشین ذخیره‌شده در بلاک‌چین و مقایسه با هش جدید
۴. در صورت مغایرت هش‌ها، صدور هشدار تغییر غیرمجاز داده
۵. در صورت یکسان‌بودن هش‌ها بررسی تکراری‌بودن هش برای جلوگیری از حملات Replay Attack
۶. ذخیرهٔ هش جدید در آرایهٔ logHashes در بلاک‌چین

در انتهای هر بازه بلندمدت (۲۴ ساعته)، تابع (ResetAndVerifyHashes) اجرا می‌شود که مراحل آن به قرار زیر است:

۱. محاسبهٔ مجدد هش‌ها از داده‌های ثبت رخداد ۲۴ ساعت گذشته
۲. مقایسهٔ هش‌های جدید با هش‌های ذخیره‌شده
۳. هشدار در صورت تشخیص مغایرت (نشانه‌ای از دست‌کاری داده‌های تاریخی)
۴. در صورت تطابق کامل، پاک‌سازی آرایهٔ logHashes برای دورهٔ بعدی

این ساختار با تلفیق قابلیت‌های تغییرناپذیری بلاک‌چین و منطق بررسی چندمرحله‌ای تضمین می‌کند که هیچ‌گونه تغییر یا دست‌کاری در داده‌های ثبت رخداد بدون شناسایی باقی نماند؛ همچنین با طراحی دقیق توابع و زمان‌بندی اجرا حملاتی مانند Replay، Reentrancy و Front-running به‌طور مؤثری کنترل می‌شوند و امکان تأثیرگذاری آن‌ها بر عملکرد سامانه از بین می‌رود.

۳-۵-تضمین صحت و محرمانگی در مدل

هدف اصلی این مدل تضمین صحت و تضمین محرمانگی داده‌های ثبت رخداد است. به طور جزئی‌تر:

تضمین صحت: برای اطمینان از صحت داده‌های ثبت رخداد از ویژگی تغییرناپذیری بلاک‌چین استفاده می‌شود. با ذخیرهٔ هش داده‌ها بر روی بلاک‌چین هرگونه تغییر در داده‌های اصلی قابل شناسایی خواهد بود؛ همچنین بررسی صحت داده‌ها در دو بازه زمانی متفاوت (کوتاه‌تر و بلندتر) احتمال خطا را کاهش می‌دهد.

[DOI: 10.61882/jsdp.22.2.65]

تضمین محرمانگی: به‌دلیل ماهیت عمومی بلاک‌چین، ذخیرهٔ مستقیم داده‌های خام (داده‌های ثبت رخداد) بر روی آن امن نیست؛ بنابراین برای ایجاد اثر انگشتی منحصر به فرد از داده‌ها، از الگوریتم هش استفاده می‌شود. این اثر انگشت (هش) به جای داده‌های اصلی بر روی بلاک‌چین ذخیره می‌شود؛ به این ترتیب محرمانگی داده‌ها حفظ می‌شود و تنها صحت آن‌ها قابل تأیید خواهد بود.

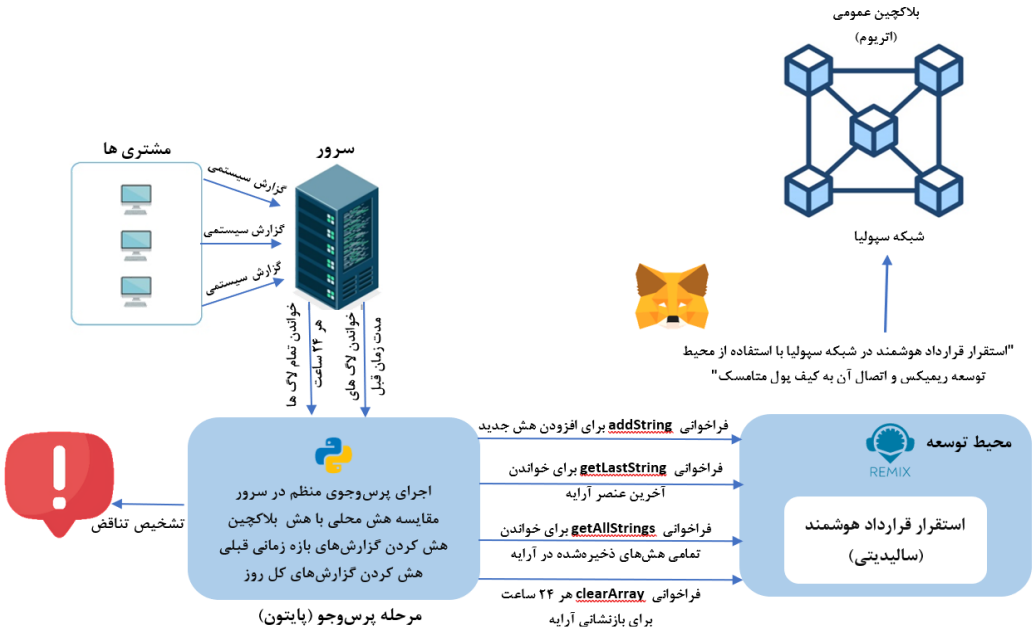
۳-۶-بررسی امنیت قراردادهای هوشمند

در مدل پیشنهادی استفاده از قراردادهای هوشمند نقش کلیدی در تأمین امنیت و صحت داده‌های ثبت رخداد داشت. قرارداد هوشمند به‌عنوان یک سازوکار مطمئن برای ذخیره و مقایسهٔ هش‌های داده‌های ثبت رخداد در بلاک‌چین عمل و تضمین می‌کند که تغییرات غیرمجاز در داده‌ها شناسایی شوند؛ از آنجا که بلاک‌چین تغییرناپذیر است قرارداد هوشمند قادر است هر گونه مغایرت بین هش‌های ذخیره‌شده و هش‌های جدید را خودکار شناسایی کند و به کاربر اطلاع دهد. استفاده از قرارداد هوشمند در این مدل به‌دلیل طراحی دقیق آن امنیت بالایی را فراهم می‌آورد.

نخستین دلیل جلوگیری از Replay attack این است که هر هش به‌طور مستقل و برای هر بازه زمانی مشخص در بلاک‌چین ذخیره می‌شود و هیچ گونه تکرار هش‌های قدیمی وجود ندارد. برای Reentrancy attack، چون هیچ‌گونه فراخوانی به توابع خارجی یا تغییرات پیچیدهٔ وضعیت در قرارداد وجود ندارد، امکان سوءاستفاده از وضعیت قرارداد وجود ندارد؛ درنهایت، Front-running attack به‌دلیل زمان‌بندی خودکار و دقیق عملیات و ذخیرهٔ هش‌ها در بازه‌های زمانی مشخص، درعمل غیرممکن می‌شود؛ به این ترتیب، استفاده از قرارداد هوشمند در مدل باعث می‌شود که این حملات نتوانند به سامانه آسیب برسانند و عملیات به‌طور امن و دقیق انجام شود.

(شکل-۱): مدل پیشنهادی

(Figure-1): Proposed Model



۴-پیاده‌سازی و ارزیابی

در این بخش از مقاله پیاده‌سازی روش پیشنهادی که در بخش سوم شرح داده شد، مورد بررسی قرار می‌گیرد. در اینجا، جزئیات و اجزای مختلف روش مورد نظر به طور کامل بیان می‌شود و نتایج حاصل از اجرای آن ارائه می‌شود. هدف اصلی این روش تضمین صحت داده‌های ثبت رخداد به‌صورت خودکار و حفظ محرمانگی آن‌هاست. برای ارزیابی اثربخشی این روش، پیاده‌سازی آن انجام شده‌است. هدف از این پیاده‌سازی، محاسبهٔ دقیق هزینه‌های مالی و سربار زمانی مرتبط با اجرای این روش است. سربار زمانی به مدت زمانی اطلاق می‌شود که سرور برای هش‌گرفتن از داده‌های ثبت رخداد با حجم‌های مختلف نیاز دارد. این زمان تحت تأثیر مستقیم حجم داده‌ها و زمان پردازش آن‌ها قرار دارد. **هزینهٔ مالی** به هزینه‌هایی اشاره دارد که برای ذخیره‌سازی رشته‌های هش در شبکهٔ بلاک‌چین مورد نظر صرف می‌شود. این هزینه بسته به طول رشتهٔ هش و تعداد تراکنش‌ها متفاوت است.

۴-۱- محیط پیاده‌سازی

پیاده‌سازی‌های مورد نظر در این پژوهش بر روی یک سامانه با مشخصات پردازندهٔ **Intel Core i7** حافظهٔ **شانزده**

[DOI: 10.61882/jsdp.22.2.65]

گیگابایت و سامانه عامل **Windows 11** انجام شده‌است. تابع مورد استفاده برای هش‌گرفتن از داده‌های ثبت رخداد به زبان برنامه‌نویسی پایتون پیاده‌سازی شده‌است و از الگوریتم **SHA-256** برای تولید هش از داده‌های ثبت رخداد با حجم‌های مختلف استفاده شده‌است. داده‌های ثبت رخداد از مجموعه‌دادهٔ [۲۴] استخراج شده‌اند. در این پژوهش، قرارداد هوشمند با استفاده از زبان برنامه‌نویسی **Solidity**، که زبان اصلی پشتیبانی‌شده به‌وسیلهٔ شبکه اتریوم است[۲۵]، طراحی و پیاده‌سازی شده‌است. برای ذخیره‌سازی داده‌ها، از تست‌نت **Sepolia**، جدیدترین شبکهٔ آزمایشی اتریوم استفاده شده‌است که مبتنی بر **Solidity** عمل می‌کند.

۴-۲- نحوهٔ پیاده‌سازی

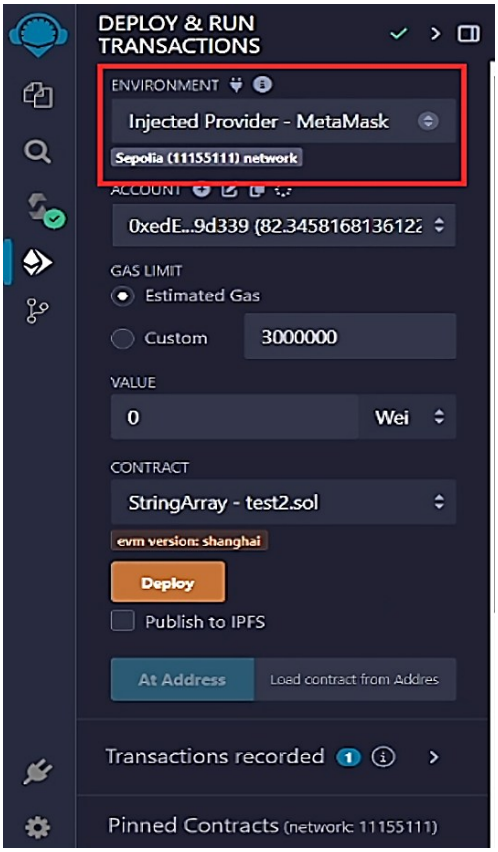
جهت ارتباط با شبکهٔ بلاک‌چین دو ابزار کلیدی مورد استفاده قرار گرفتند: محیط توسعهٔ **Remix IDE** که یک ابزار قدرتمند و کاربرپسند برای توسعهٔ قراردادهای هوشمند است، و کیف پول **MetaMask** که به‌دلیل امنیت و محبوبیت بالا برای مدیریت تراکنش‌ها و ارتباط با شبکه انتخاب شد. این ترکیب از ابزارها فرایند توسعه و آزمایش قرارداد هوشمند را ساده و ایمن کرده‌است.

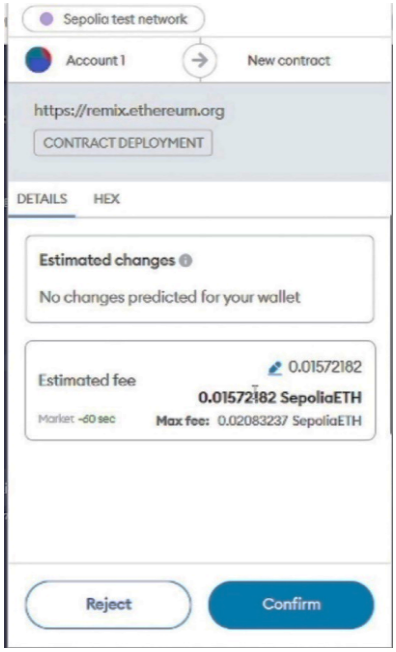
در ابتدا، قرارداد هوشمند مورد نظر در شبکهٔ تست‌نت سپولیا مستقر شد. شبکهٔ سپولیا به‌عنوان یک شبکهٔ آزمایشی بلاک‌چین مبتنی بر اتریوم برای آزمایش و ارزیابی قراردادهای هوشمند مورد استفاده قرار می‌گیرد و این امکان را فراهم می‌آورد که عملکرد قراردادها بدون نیاز به پرداخت هزینه‌های تراکنش در شبکهٔ اصلی بررسی شود. هزینهٔ استقرار این قرارداد هوشمند حدود ۰.۰۱۶ اتر بود که در شکل (۲) نمایش‌داده‌شده‌است. این هزینه شامل هزینه‌های ذخیره‌سازی کد قرارداد و انجام نخستین تراکنش‌های آن در شبکهٔ بلاک‌چین سپولیا می‌شود.

برای ارزیابی عملکرد سامانه زمان لازم برای هش‌گرفتن از داده‌های ثبت رخداد با حجم‌های مختلف محاسبه شد؛ به این منظور، تابع مورد نظر بر روی سرور اجرا شد.

این تابع داده‌های ثبت رخداد را با حجم‌های مختلف از مجموعه‌داده استخراج کرده و از آن‌ها هش تولید کرد. این هش‌ها با استفاده از الگوریتم **SHA-256** محاسبه شدند؛ سپس با فراخوانی توابع قرارداد هوشمند مستقر شده در شبکهٔ سپولیا، هش‌ها در آرایه‌ای ذخیره شدند. استفاده از قرارداد هوشمند در این فرایند به‌طور عمده برای تضمین یک‌پارچگی و صحت ذخیره‌سازی هش‌ها در بلاک‌چین بود. هر هش محاسبه‌شده از داده‌ها به‌طور ایمن در بلاک‌چین ذخیره شد که ویژگی تغییرناپذیری بلاک‌چین صحت داده‌ها را تضمین می‌کند.

این فرایند شامل مراحل مختلفی از جمله اجرای تابع، محاسبهٔ هش‌ها و ذخیره‌سازی آن‌ها در شبکهٔ بلاک‌چین سپولیا بود که به‌طور مؤثری سربار زمانی و هزینه‌های مالی مرتبط با پیاده‌سازی را اندازه‌گیری کرد.





(شکل-۲): اتصال به شبکهٔ سپولیا از طریق کیف پول متامسک
(Figure-2): Connecting to the Sepolia network via Metamask wallet

[DOI: 10.61882/jsdp.22.2.65]

۴-۳- ارزیابی

برای ارزیابی روش پیشنهادی ابتدا لازم است، معیارهای مطرح‌شده در مدل تعیین شوند. در این پژوهش، از الگوریتم **SHA-256** برای هش‌گرفتن از داده‌های ثبت رخداد استفاده شده‌است. خروجی این الگوریتم رشته‌های ۳۲ بایتی است. طول این رشته‌ها تأثیر مستقیم بر هزینهٔ ذخیره‌سازی آن‌ها در شبکهٔ سپولیا دارد؛ هر چه طول رشته‌های خروجی بیشتر باشد، هزینهٔ ذخیره‌سازی آن‌ها در شبکهٔ بلاک‌چین افزایش می‌یابد؛ همچنین بازه زمانی نخست برابر با پانزده دقیقه در نظر گرفته شده‌است که انتخاب این زمان بستگی کامل به کمترین زمان مورد نیاز برای حملات سایبری دارد؛ یعنی اگر این زمان برابر حداقل زمان لازم برای حملات سایبری در نظر گرفته شود این مدل به صورت صددرصد می‌تواند صحت داده‌ها را تضمین بدهد، اما با پژوهش‌های انجام‌شده و فاکتورهای پیچیده‌ای که در شبکه‌های مختلف متفاوت است نمی‌توان کمترین زمانی را برای حملات سایبری مختلف در نظر گرفت؛ از طرفی این بازه زمانی تأثیر مستقیمی بر هزینهٔ ذخیره‌سازی رشته‌ها در شبکهٔ سپولیا دارد؛ به‌طوری که هرچه بازه زمانی کوتاه‌تر باشد، هزینهٔ ذخیره‌سازی بیشتر خواهد بود؛ در حالی که دقت مدل بالاتر می‌رود؛ بنابراین میزان زمان پانزده دقیقه برای بازه زمانی نخست در این مدل می‌تواند با توجه به اهمیت بین میزان دقت مدل و میزان هزینهٔ مورد انتظار متفاوت باشد. باید توجه داشت که مدل پیشنهادی برای تضمین صحت داده‌های ثبت رخداد، زمانی که حملات در بازه زمانی کوتاه‌تر از پانزده دقیقه رخ دهند، نمی‌تواند به‌طور کامل پاسخ‌گو باشد؛ زیرا این زمان برابر کمینه زمان مورد نیاز برای حملات مختلف سایبری نیست و اگر نفوذگری به‌طور دقیق در این بازه زمانی وارد سامانه شده و عملیات مخرب انجام دهد و درنهایت داده‌های ثبت رخداد حاصل از کار خود را حذف کرده و از سامانه خارج شود هشی که روی شبکه ذخیره می‌شود یک مقدار تغییر یافته است که صحت آن معنایی ندارد. قرارداد هوشمند مورد استفاده در این پژوهش به زبان سالیدیتی نوشته شده و در محیط **Remix**کامپایل شده‌است؛ سپس با استفاده از کیف پول **MetaMask** قرارداد در شبکهٔ تست‌نت سپولیا مستقر شده‌است؛ همچنین، برای ارزیابی دقیق‌تر، بازه زمانی دوم برابر با یک روز در نظر گرفته شده‌است. داده‌های ثبت رخداد با حجم‌های مختلف از ۲۸۰ کیلوبایت تا یک گیگابایت به تابع هش داده شده‌اند تا مدت زمان لازم برای هش‌گرفتن از این داده‌ها ثبت و تحلیل شود.

۴-۳-۱- ارزیابی سربار زمانی

شکل (۳) زمان مورد نیاز برای تولید هش از داده‌های ثبت رخداد با حجم‌هایی بین ۲۸۰ کیلوبایت تا یک گیگابایت را نمایش می‌دهد؛ همان‌طورکه در شکل مشاهده می‌شود، در پیاده‌سازی انجام‌شدهٔ فایل‌های ثبت رخداد با اندازه‌های مختلف به تابع مربوطه به‌عنوان ورودی داده شد و درنتیجه ۳.۱۸ ثانیه زمان برد تا هش یک فایل با حجم یک گیگابایت محاسبه شود. این زمان قابل‌توجهی محسوب نمی‌شود؛ زیرا این تابع بر روی یک سامانه معمولی اجرا شده‌است؛ علاوه‌بر این حجم داده‌های ثبت رخداد تولیدشده با سامانه‌های معمولی در شبکه به‌طور متوسط بسیار کمتر از یک گیگابایت است؛ همچنین درصورت استفاده از سرورهایی با سخت‌افزار قدرتمندتر این زمان به مراتب کاهش خواهد یافت. با استناد به پژوهش انجام‌شده توسط بارتولتی [۲۵] حجم داده‌های تولیدشده در یک سرور معمولی شبکهٔ متوسط طی یک ربع، بسیار کمتر از یک گیگابایت است. با درنظرگرفتن اینکه این سرورها به‌طور معمول از سخت‌افزار بسیار قوی‌تری نسبت به سامانه مورد استفاده در این آزمایش بهره می‌برند، می‌توان انتظار داشت که زمان لازم برای هش‌گیری کاهش چشم‌گیری یابد.

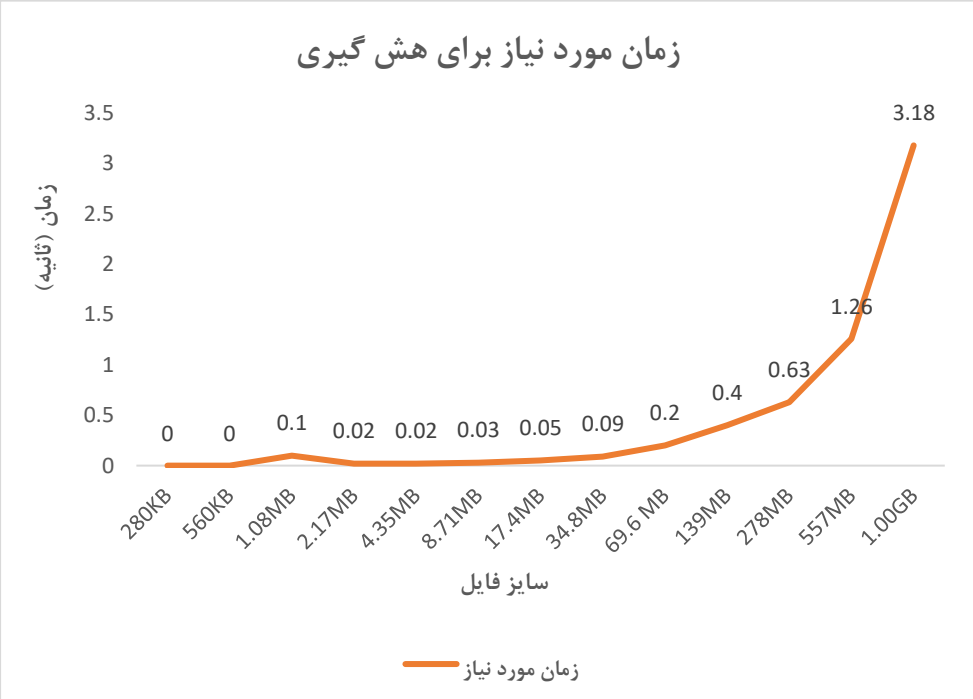
۴-۳-۲- ارزیابی هزینهٔ مالی

هزینهٔ مالی شامل ذخیرهٔ رشته‌های هش ۳۲ بایتی هر پانزده دقیقه بر روی شبکهٔ سپولیا و همچنین هزینهٔ بازنشانی آرایهٔ حاوی هش‌ها در انتهای هر روز است. گفتنی است که خواندن داده‌ها از بلاک‌چین هزینه‌ای ندارد. شکل (۴) هزینهٔ لازم برای ذخیرهٔ رشته‌های ۳۲ بایتی بر روی یک آرایه با طول‌های مختلف در شبکهٔ سپولیا را نشان می‌دهد؛ این رشته‌ها همان داده‌هایی است که هر پانزده دقیقه بر روی شبکهٔ بلاک‌چین ذخیره می‌شود و حاصل هش‌گیری داده‌های ثبت رخداد در همان بازه است. رفتار سینوسی نمودار به‌طور عمده به‌دلیل شرایط متغیر شبکه در زمان‌های مختلف است، نه به‌دلیل طول آرایه‌ای که هش‌ها در آن ذخیره می‌شوند. این هزینه بین ۰.۰۰۱ تا ۰.۰۰۳ اتر متغیر است، اما به‌طور متوسط حدود ۰.۰۰۲ اتر است. شکل (۵) هزینهٔ ریست‌کردن آرایه با طول‌های مختلف را نشان می‌دهد که در انتهای بازه زمانی دوم انجام می‌شود و هرچه تعداد رشته هایی که در طول این بازه زمانی روی آرایه ذخیره شده‌اند، بیشتر باشد هزینهٔ ریست‌کردن آن هم بیشتر می‌شود.

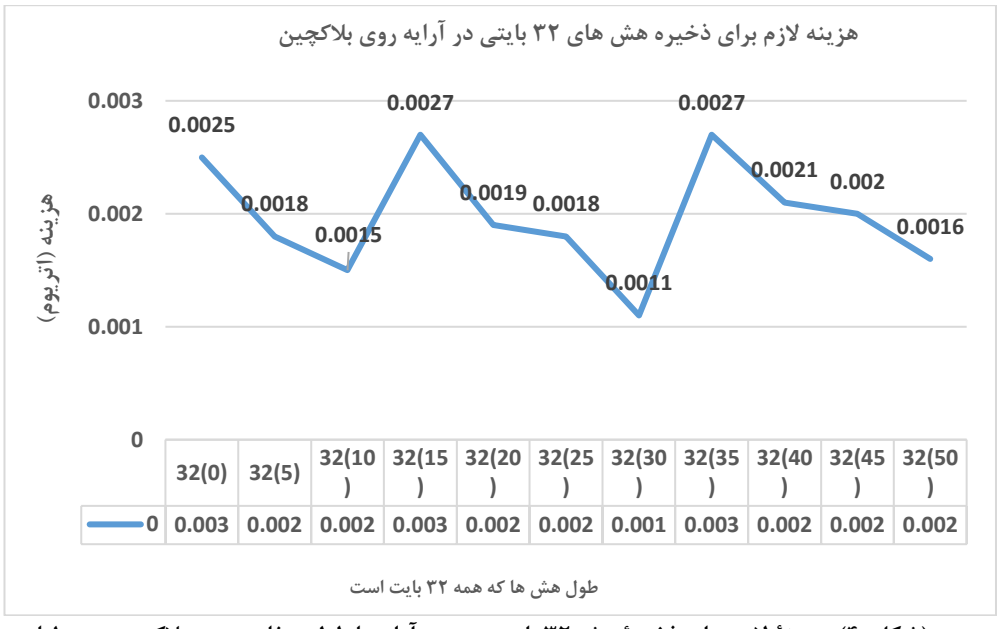
طبق روش پیشنهادی، برای به‌کمترین‌حدرساندن احتمال خطا، صحت داده‌ها باید طی دو مرحله تضمین شود:
مرحلهٔ نخست: در انتهای بازه زمانی نخست انجام می‌شود، و در آن، تنها هش مربوط به بازه زمانی پیشین صحت‌سنجی می‌شود.
مرحلهٔ دوم: در انتهای بازه زمانی دوم که بازهٔ طولانی‌تر است، صحت هش داده‌های چندین بازه زمانی ذخیره‌شده در آرایه

[DOI: 10.61882/jsdp.22.2.65]

بررسی می‌شود. طول آرایه از تقسیم بازه زمانی دوم بر بازه زمانی نخست به‌دست می‌آید. در مرحلهٔ دوم، داده‌ها از آرایهٔ ذخیره‌شده روی بلاک‌چین خوانده می‌شوند و پس از صحت‌سنجی آرایه ریست می‌شود. دقت شود که خواندن از آرایه هزینه‌ای به دنبال ندارد، اما نوشتن در آن هزینه‌بر است. همان‌طورکه در شکل (۵) مشاهده می‌شود، هرچه طول آرایه بزرگ‌تر باشد، هزینهٔ بازنویسی آن نیز بیشتر خواهد بود. باید توجه داشت که در زمانی که طول آرایه برابر با هشتاد بود، هزینهٔ بازنشانی در بالاترین مقدار خود قرار داشت که این امر به‌دلیل شرایط خاص شبکه در آن لحظه است. در حالت کلی، این نمودار صعودی است، بدین معنا که با افزایش طول آرایه، هزینهٔ بازنشانی آن نیز بیشتر می‌شود.

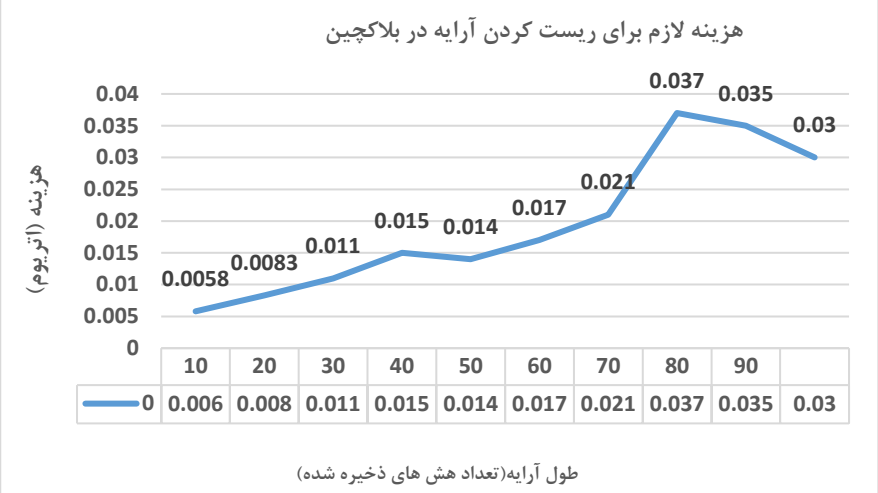


(شکل-۳): هزینهٔ زمانی مورد نیاز برای هش‌گرفتن از داده‌های ثبت رخداد توسط کوئری با حجم‌های متفاوت
(Figure-3): The time cost required for hashing event log data using queries with varying sizes



(شکل-۴): هزینهٔ لازم برای ذخیرهٔ هش ۳۲ بایتی بر روی آرایه با طول متفاوت روی بلاک‌چین سپولیا
(Figure-4): The cost required to store a 32-byte hash on an array with varying lengths on the Sepolia blockchain

[DOI: 10.61882/jsdp.22.2.65]



(شکل-۵): هزینهٔ لازم برای ریست‌کردن آرایه با طول‌های مختلف در شبکهٔ سپولیا
(Figure-5): The cost required to reset an array with varying lengths on the Sepolia network

با توجه به معیارهای مشخص‌شده در این پیاده‌سازی، برای محاسبهٔ هزینهٔ کل مالی که این مدل در طول یک ماه ممکن است داشته باشد، فرضیات زیر در نظر گرفته می‌شود:

فرض نخست: الگوریتم مورد استفاده SHA-256 است که طول رشتهٔ خروجی آن ۳۲ بایت است.

فرض دوم: در انتهای هر روز، آرایهٔ حاوی هش‌ها بازنشانی می‌شود.

فرمول محاسبهٔ هزینهٔ کل در یک ماه به شرح زیر است:

$$T=A+30\times(Z+24\times(X\times Y)) \quad (۱)$$

که در آن:

T=هزینهٔ کل در یک ماه

A=هزینهٔ استقرار اولیهٔ قرارداد هوشمند

X=هزینهٔ مورد نیاز برای ذخیرهٔ هش ۳۲ بایتی در شبکهٔ بلاک‌چین

Y=تعداد دفعات هش‌گیری در ساعت

Z=هزینهٔ بازنشانی‌کردن آرایه با طول مشخص

گفتنی است که برای ماه‌های بعدی، هزینهٔ استقرار اولیهٔ قرارداد هوشمند تکرار نخواهد شد و این هزینه تنها یک‌بار در محاسبات اعمال می‌شود. بر اساس فرمول به‌دست‌آمده، هرچه تعداد دفعات هش‌گیری در طول روز کمتر باشد، هم هزینهٔ ذخیرهٔ داده‌ها روی بلاک‌چین کاهش می‌یابد و هم هزینهٔ بازنشانی آرایه. این موضوع با توجه به فرمول و شکل‌های (۴) و (۵) مشخص است. شکل (۴) بیان‌کنندهٔ این نکته است که در هر بار ذخیره‌سازی یک هش ۳۲ بایتی در هر یک از خانه‌های مختلف آرایه هزینهٔ ثابتی وجود ندارد و به شرایط شبکه وابسته است. در این شکل برای مثال خانه‌هایی با اندیس مضرب پنج آرایه در نظر گرفته شده‌اند؛ بااین‌حال، باید در نظر داشت که هش‌گیری از داده‌ها در بازه‌های زمانی کوتاه‌تر منجر به تضمین صحت مؤثرتر داده‌ها می‌شود؛ بنابراین، با توجه به بیشینهٔ هزینه‌ای که در نظر گرفته می‌شود، می‌توان مدت زمان مشخصی را برای هش‌گیری تعیین کرد.

با تمامی پارامترهای تعیین‌شده، این طرح قادر است صحت داده‌های ثبت رخداد را به صورت خودکار تضمین کند؛ همچنین با توجه به پیاده‌سازی انجام‌شده، هزینه‌های پیاده‌سازی این طرح، شامل هزینهٔ مالی و سربار زمانی، محاسبه شده‌است؛ بااین‌حال، همان‌طورکه در تمامی تمهیدات امنیتی پیش‌بینی شده‌است، هیچ تمهید امنیتی قادر به تضمین صددرصدی نسبت به هدف خود نیست. به‌طور خاص، طبق طرح پیشنهادی اگر حمله‌ای صورت گیرد که مدت زمان آن کمتر از مدت زمان هش‌گیری باشد و به‌طور دقیق در این بازه زمانی اتفاق بیفتد و نفوذگر اقدام به حذف داده‌های ثبت رخداد کند، طرح پیشنهادی قادر به تضمین صددرصدی صحت این نوع داده‌ها نخواهد بود.

۴-۳-۳- ارزیابی پیچیدگی زمانی مدل

با توجه به جدول (۲)، برای بررسی پیچیدگی زمانی روش‌های مختلف ذخیره‌سازی داده‌های ثبت رخداد در بلاک‌چین، نحوهٔ پردازش، هش‌گذاری و ذخیره‌سازی اطلاعات در هر پژوهش مورد بررسی قرار گرفت. در روش پیشنهادی، تنها هش داده‌ها در بلاک‌چین ذخیره شده و داده‌های خام خارج از زنجیره باقی می‌مانند. این فرایند موجب کاهش چشم‌گیر هزینه و زمان پردازش می‌شود. از آنجا که طول هش همواره ثابت است، زمان لازم برای ذخیره‌سازی مستقل از حجم داده‌ها بوده و درنتیجه، پیچیدگی زمانی این روش $O(1)$ است. این ویژگی باعث می‌شود که روش پیشنهادی، یک راه‌کار بهینه و کم‌هزینه برای تضمین صحت داده‌ها باشد. در پژوهش [۱۶] نیز رویکردی مشابه اتخاذ شده و تنها هش داده‌ها در بلاک‌چین اتریوم ذخیره می‌شود؛ بنابراین، این روش نیز

[DOI: 10.61882/jsdp.22.2.65]

دارای پیچیدگی زمانی O(1) است؛ بااین‌حال، امکان وجود تأخیر جزئی در تأیید هش‌ها از طریق قراردادهای هوشمند وجود دارد که در برخی موارد، زمان پردازش را تحت تأثیر قرار می‌دهد.

برخی پژوهش‌ها مانند [۱۷] و [۲۲] برای کاهش هزینه‌های ذخیره‌سازی از فناوری IPFS استفاده کرده‌اند. در این روش‌ها، داده‌های اصلی در IPFS ذخیره شده و تنها هش آن‌ها در بلاک‌چین ثبت می‌شود. این روش باعث کاهش هزینه‌های ذخیره‌سازی در بلاک‌چین می‌شود، اما به‌دلیل ماهیت توزیع‌شدهٔ IPFS، بازیابی داده‌ها مستلزم جست‌وجو در یک ساختار درختی (Merkle DAG) است که پیچیدگی زمانی آن O(log N) خواهد بود. این موضوع می‌تواند منجر به افزایش زمان تأیید داده‌ها شود. در مقابل، روش‌هایی مانند [۲۰] و [۷] داده‌های ثبت رخداد را به‌طور کامل در بلاک‌چین ذخیره می‌کنند. در این روش‌ها، هرچه حجم داده‌های ثبت رخداد افزایش یابد، زمان پردازش و هزینهٔ ذخیره‌سازی نیز افزایش می‌یابد؛ ازاین‌رو، پیچیدگی زمانی این روش‌ها O(N) است؛ این بدان معناست که زمان ذخیره‌سازی به‌صورت خطی با افزایش حجم داده‌ها رشد می‌کند که موجب هزینهٔ بالاتر و تأخیر بیشتر در پردازش داده‌ها می‌شود؛ درنهایت، روش‌هایی مانند [۲۱] که از بلاک‌چین‌های خصوصی مانند Multichain استفاده می‌کنند، تنها هش داده‌ها را ذخیره کرده و نیازی به پردازش اضافی ندارند. این باعث می‌شود که پیچیدگی زمانی این روش نیز O(1) باشد؛ بااین‌حال، وابستگی به بلاک‌چین خصوصی موجب کاهش شفافیت و محدودشدن دسترسی عمومی به داده‌ها می‌شود.

در کل مقایسهٔ روش‌های موجود نشان می‌دهد که روش پیشنهادی با پیچیدگی زمانی O(1) ضمن کاهش هزینهٔ ذخیره‌سازی از نظر زمان پردازش نیز بهینه‌ترین گزینه است؛ در مقابل، روش‌هایی که از IPFS استفاده می‌کنند، هزینهٔ ذخیره‌سازی را کاهش می‌دهند، اما باعث افزایش زمان بازیابی داده‌ها می‌شوند O(log N)؛ درنهایت روش‌هایی که داده‌های ثبت رخداد را مستقیم در بلاک‌چین ذخیره می‌کنند؛ اگرچه امنیت بالایی دارند، اما هزینه و زمان پردازش بالاتری را به همراه دارند (O(N))؛ بر این اساس، روش پیشنهادی تعادلی بین امنیت، هزینه و سرعت پردازش ایجاد کرده و می‌تواند یک گزینهٔ کاربردی و مقرون‌به‌صرفه برای تضمین صحت و محرمانگی داده‌های ثبت رخداد باشد.

(جدول-۲): مقایسهٔ عملکرد با پژوهش‌های دیگر
(Table-2): Performance comparison with other studies

پژوهش	پلتفرم	محرمانگی	پیچیدگی زمانی	کارایی هزینه	کارایی زمان	معایب
Proposed Method	اتریوم (سپولیا)	بله	O (۱)	بهینه (ارزیابی‌شده برای کاهش هزینهٔ ذخیره‌سازی)	بهینه (ارزیابی‌شده برای سربار محاسبات)	در برابر حملات بسیار سریع محدودیت دارد
Javed et al. [16]	اتریوم	بله	O (۱)	بالا (به‌دلیل ذخیره‌سازی مستقیم بلاک‌چین)	متوسط	تأخیر جزئی در اجرای قرارداد هوشمند
Khor et al. [17]	Hyperledger Fabric	بله	O (logN)	متوسط (IPFS هزینه را کاهش می‌دهد)	سریع (بلاک‌چین خصوصی زمان پردازش را کاهش می‌دهد)	کندی در بازیابی داده‌ها
Ali et al.[20]	EXONUM	بله	O (N)	بالا (بلاک‌چین‌های مجاز هزینه‌های راه‌اندازی بالایی دارند)	متوسط	هزینه و زمان ذخیره‌سازی بالا
Li et al. [21]	Multichain	بله	O (۱)	متوسط (چند زنجیره‌ای کارایی را بهبود می‌بخشد)	سریع	نیاز به بلاک‌چین خصوصی
Jain et al. [7]	اتریوم	بله	O (N)	بالا (ذخیره‌سازی مستقیم در اتریوم)	متوسط	هزینه بالا، زمان ذخیرهٔ طولانی
Jiang et al. [26]	اتریوم	خیر	O (logN)	کم (IPFS هزینه را به میزان قابل توجهی کاهش می‌دهد)	آهسته (بازیابی IPFS تأخیر را اضافه می‌کند)	کندی در بازیابی داده‌ها

۵- نتیجه‌گیری و کارهای آینده

در این پژوهش، روشی نوین برای تأیید خودکار صحت داده‌های ثبت رخداد ارائه شده‌است. این روش با بهره‌گیری از فناوری بلاک‌چین و قراردادهای هوشمند، علاوه‌بر تضمین صحت داده‌ها، محرمانگی اطلاعات را نیز حفظ می‌کند. یکی از ویژگی‌های برجستهٔ این کار، محاسبهٔ دقیق هزینه‌های عملیاتی اجرای این روش است؛ در این راستا، با پیاده‌سازی عملی این روش بر روی شبکهٔ سپولیا (یک شبکهٔ آزمایشی اتریوم)، هزینه‌های ذخیره‌سازی داده‌ها و پردازش محاسباتی دقیق محاسبه شد؛ بااین‌حال، این روش در برابر حملات بسیار کوتاه‌مدت (حملاتی که مدت زمان آن‌ها کمتر از بازه زمانی نخست است) قادر به ارائهٔ تضمین صددرصدی نیست؛ لذا همواره نیاز است که بین هزینهٔ مالی (زمان فراخوانی توابع رابطهٔ مستقیم با هزینه دارد) و میزان ضمانت مورد انتظار موازنه‌ای تعیین شود.

در این پژوهش تنها هش داده‌ها در بلاک‌چین ذخیره شده‌است، نه خود داده‌های ثبت رخداد. این رویکرد برای حفظ

[DOI: 10.61882/jsdp.22.2.65]

محرمانگی داده‌ها بسیار مهم است؛ زیرا ذخیره‌سازی داده‌های خام بر روی بلاک‌چین به‌دلیل ماهیت عمومی آن امنیت را تهدید می‌کند؛ بنابراین، تنها هش‌های تولیدشده از داده‌های ثبت رخداد در بلاک‌چین ذخیره شدند. این هش‌ها به‌عنوان اثر انگشتی منحصربه‌فرد از داده‌ها عمل می‌کنند که امکان تأیید صحت داده‌ها را فراهم می‌آورد، بدون آنکه خود داده‌ها مستقیم در بلاک‌چین ثبت شوند. در کارهای آینده، به‌منظور کاهش بار مالی اجرای طرح، هدف ما بهره‌برداری از الگوریتم‌های یادگیری ماشین است. استفاده از این الگوریتم‌ها به ما این امکان را می‌دهد که داده‌های با اهمیت و اولویت‌دار را از مجموعه‌داده‌های ثبت رخداد شناسایی کنیم. در حال حاضر، تمام داده‌های ثبت رخداد مستقیم در بلاک‌چین ذخیره نمی‌شوند؛ بلکه هش‌های آن‌ها در بلاک‌چین ثبت می‌شود. با استفاده از الگوریتم‌های یادگیری ماشین می‌توان داده‌هایی را که از نظر امنیتی یا عملیاتی اهمیت بیشتری دارند، شناسایی و اولویت‌بندی کرد؛ سپس تنها این داده‌های اولویت‌دار از طریق هش در بلاک‌چین ذخیره خواهند شد. این رویکرد، به‌ویژه در مقیاس‌های بزرگ، منجر به کاهش چشم‌گیر هزینه‌های ذخیره‌سازی خواهد شد؛ چرا که به‌جای ذخیره‌سازی مستقیم تمام داده‌ها، تنها هش داده‌هایی که در فرایند تحلیل و تضمین صحت اهمیت دارند، در بلاک‌چین ذخیره خواهد شد؛ به این ترتیب، حجم داده‌های ذخیره‌شده در بلاک‌چین کاهش قابل ملاحظه‌ای می‌یابد و درنتیجه، هزینه‌های مربوط به ذخیره‌سازی داده‌ها نیز کاهش خواهد یافت.

علاوه‌براین، با استفاده از الگوریتم‌های یادگیری ماشین امکان سفارشی‌سازی مدل برای انواع مختلف داده‌ها به وجود می‌آید. این امکان به مدل اجازه می‌دهد تا نحوهٔ ذخیره‌سازی و تحلیل داده‌ها را هوشمند بهینه‌سازی کند. این بهبود در کارایی و دقت سامانه، به کاهش زمان پردازش و افزایش کارایی کلی سامانه خواهد انجامید.

6-References ۶-مراجع

[1] پارسائیان، محمودرضا و صمیمی، حسین، «رویکردی نوین برای جلوگیری از آسیب‌پذیری در قراردادهای هوشمند و مقابله با حملات Reentrancy بر بستر بلاک‌چین»، *یازدهمین کنگره ملی سراسری فناوریهای نوین در حوزهٔ توسعهٔ پایدار، ایران*، تهران، ۱۴۰۰.
https://civilica.com/doc/1469930

[1] M. R. Parsaeian and H. Samimi, "A Novel Approach to Prevent Vulnerabilities in Smart Contracts and Counter Reentrancy Attacks on Blockchain Platform," in Proc. 11th National Congress of New Technologies in Sustainable Development, Tehran, Iran, 2021. Avialable: https://civilica.com/doc/1469930

[2] تیموری، احمد، دی پیر، محمود، «سامانه دو سطحی تشخیص نفوذ برای شبکه اینترنت اشیا مبتنی بر یادگیری عمیق»، *پردازش علائم و داده‌ها*، دورهٔ ۲۱، شمارهٔ ۳، ص ۳-۲۲، ۱۴۰۳.

[2] A. Teymouri and M. Deypir, "Two-level intrusion detection system for Internet of Things network based on deep learning", *Signal and Data Processing,* vol. 21, no. 3, pp. 3-22, 2024.

[3] س. کدخدا ده خانی، ح. زنگی آبادی زاده، م. قاسمی، م. رحمانی ,و ف. وظیفه دوست، «فناوری بلاکچین: مروری بر مفاهیم، چالش‌های بلاکچین در خدمات عمومی و طبقه‌بندی توکن‌های بلاکچین»، دو فصلنامهٔ محاسبات و سامانه‌های توزیع شده، شمارهٔ ۶، ۱۱۸-۱۳۶، ۱۴۰۲.

[3] S.kadkhodadehkhani, H.Zangiabadi Zadeh, M.Ghasemi, F.Vazifehdoost, M.Rahmani. Blockchain Technology: A Review of Concepts, Blockchain Challenges in Public Services, and Blockchain Token Classification, *Journal of Distributed Computing and Systems (JDCS)*, Vol 6, Issue 1, Page 118-136, 2023.

[4] ب. پورولیخان نوخندان، «یک طرح ذخیره‌سازی توزیع‌شده بر اساس بلاکچین و IPFS برای داده‌های IoT آتش‌نشانی»، *ششمین همایش و نمایشگاه بین‌المللی آتش‌نشانی و ایمنی شهری*، ۱۴۰۳.
https://civilica.com/doc/2059774

[4] B. Pourvelikhan Noukhendan, "A Distributed Storage Scheme Based on Blockchain and IPFS for Fire Department IoT Data," in Proc. *6th International Conference and Exhibition on Fire Fighting and Urban Safety*, Iran, 2024. [in Persian] Available: https://civilica.com/doc/2059774

[5] پورعسکری، حسن، خطیبی بردسیری، عمید، محمدی قنات قستانی، مختار «حفظ حریم خصوصی در اینترنت اشیا برای انتقال داده‌ها در حوزه سلامت با استفاده از زنجیره بلوکی»، *پردازش علائم و داده‌ها*، دورهٔ ۲۱، شمارهٔ ۳، ص ۱۴۹-۱۷۸، ۱۴۰۳.

[5] A. Hassan Pour Askari, A. Khatibi Bardsiri, and M. Mohammadi Ghanat Ghestani, "IoT privacy for the transmission of data in the field of health using blockchain," (in eng), *Signal and Data Processing,* Research vol. 21, no. 3, pp. 149-178, 2024.
doi: 10.61186/jsdp.21.3.149.

[6] M. H. Rakib, S. Hossain, M. Jahan, and U. Kabir, "A blockchain-enabled scalable network log management system," *Journal of Computer Science,* vol. 18, no. 6, p. 496.508, 2022.

[7] P. Jain, "Decentralize log file storage and integrity preservation using blockchain," *International Journal of Computer Science and Information Technologies,* vol. 11, no. 2, pp. 21-30, 2020.

[8] N. Salunke, S. Sonawane, and D. Motwani, "Decentralized evidence storage system using blockchain and IPFS," in *International Conference on Information, Communication and Computing Technology*, 2023: Springer, pp. 259-280.

[9] M. Kumar, A. K. Singh, and T. S. Kumar, "Secure log storage using blockchain and cloud infrastructure," in *2018 9th International Conference on Computing, Communication and Networking Technolo gies (ICCCNT)*, 2018: IEEE, pp. 1-4.

[10] W. Pourmajidi and A. Miranskyy, "Logc hain: Blockchain-assisted log storage," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018: IEEE, pp. 978-982.

[11] Y. Taguchi, A. Kanai, and S. Tanimo, "A distributed log management method using a blockchain Scheme," in *2020 IEEE International Conference on Consumer Electronics (ICCE)*, 2020: IEEE, pp. 1-3.

[DOI: 10.61882/jsdp.22.2.65]

[12]K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, "BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem," *Future Generation Computer Systems,* vol. 122, pp. 1-13, 2021.
[13] H. Tian, J. Wang, C.-C. Chang, and H. Quan, "Public auditing of log integrity for shared cloud storage systems via blockchain," *Mobile Networks and Applications,* pp. 1-13, 2023.
[14] M. Altulyan, L. Yao, S. Kanhere, and C. Huang, "A blockchain framework data integrity enhanced recommender system," *Computational Intelligence,* vol. 39, no. 1, pp. 104-120, 2023.
[15]L. Li, D. Jin, T. Zhang, and N. Li, "A secure, reliable and low-cost distributed storage scheme based on blockchain and IPFS for firefighting IoT data," *IEEE Access,* vol. 11, pp. 97318-97330, 2023.
[16]H. Javed *et al.*, "Blockchain-based logging to defeat malicious insiders: The case of remote health monitoring systems," *IEEE Access,* vol. 12, pp. 12062-12079, 2023.
[17]J. H. Khor, M. Sidorov, M. T. Ong, and S. Y. Chua, "Public blockchain-based data integrity verification for low-power IoT devices," *IEEE Internet of Things Journal,* vol. 10, no. 14, pp. 13056-13064, 2023.
[18]B. Putz, F. Menges, and G. Pernul, "A secure and auditable logging infrastructure based on a permissioned blockchain," *Computers & Security,* vol. 87, p. 101602, 2019.
[19]Z. Liu, L. Ren, Y. Feng, S. Wang, and J. Wei, "Data integrity audit scheme based on quad merkle tree and blockchain," *IEEE Access,* vol. 11, pp. 59263-59273, 2023.
[20]A. Ali, A. Khan, M. Ahmed, and G. Jeon, "BCALS: Blockchain-based secure log management system for cloud computing," *Transactions on Emerging Telecommunications Technologies,* vol. 33, no. 4, p. e4272, 2022.
[21]W. Li, Y. Feng, N. Liu, Y. Li, X. Fu, and Y. Yu, "A secure and efficient log storage and query framework based on blockchain," *Computer Networks,* vol. 252, p. 110683, 2024.
[22]P. Jiang, B. Qiu, and L. Zhu, "Toward reliable and confidential release for smart contract via ID-based TRE," *IEEE Internet of Things Journal,* vol. 9, no. 13, pp. 11422-11433, 2021.
[23] او شیلدز، رجی، ناصر، مهدی، صادقی، حسین. «قراردادهای هوشمند: توافقات حقوقی در پرتو بلاکچین»، *پژوهش‌های حقوقی*، مجلهٔ ۱۸، شمارهٔ ۳۷، صص ۲۶۱-۲۸۸، ۱۳۹۸.
10.48300/jlr.2019.91607
[23] O. Shields, R. Naser, and H. Sadeghi, "Smart Contracts: Legal Agreements for the Blockchain", *Journal of Legal Research*, vol. 18, no. 37, pp. 261-288, 2019. [in Persian]10.48300/jlr.2019.91607
[24] J. Zhu, S. He, P. He, J. Liu, and M. R. Lyu, "Loghub: A large collection of system log datasets for ai-driven log analytics," in *2023 IEEE 34th International Symposium on Software Reliability Engineering (ISSRE)*, 2023: IEEE, pp. 355-366.
[25] M. Bartoletti, F. Fioravanti, G. Matricardi, R. Pettinau, and F. Sainas, "Towards benchmarking of Solidity verification tools," *arXiv preprint arXiv:2402.10750,* 2024.
[26] J. Jiang, X. Zhang, and Z. Yuan, "Feature selection for classification with Spearman's rank correlation coefficient-based self-information in divergence-based fuzzy rough sets," *Expert Systems with Applications,* vol. 249, p. 123633, 2024.

فاطمه آملی دانش‌آموختهٔ کارشناسی‌ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری از دانشگاه مازندران است. وی مدرک کارشناسی خود را در رشتهٔ مهندسی کامپیوتر گرایش سخت‌افزار از دانشگاه صنعتی نوشیروانی بابل دریافت کرده‌است. برخی زمینه‌های پژوهشی مورد علاقهٔ ایشان شبکه و امنیت شبکه‌های کامپیوتری است.
نشانی رایانامهٔ ایشان عبارت است از:
amoli.fatemeh.1996@gmail.com

مصطفی بستام استادیار دانشکدهٔ مهندسی کامپیوتر دانشگاه مازندران است. او دکترای خود را در رشتهٔ شبکه‌های کامپیوتری از دانشگاه صنعتی امیرکبیر (پلی‌تکنیک تهران) در سال ۱۳۹۶ دریافت کرد. مدرک کارشناسی خود را در رشتهٔ مهندسی کامپیوتر از دانشگاه شهید باهنر کرمان در سال ۱۳۸۵ و مدرک کارشناسی‌ارشد را در رشتهٔ شبکه‌های کامپیوتری از دانشگاه صنعتی امیرکبیر در سال ۱۳۸۸ دریافت کرد. زمینه‌های پژوهشی مورد علاقهٔ ایشان عبارت‌اند از: رایانش ابری و مه، شبکه‌های نرم‌افزار محور، اینترنت اشیا، یادگیری ماشین و بلاک‌چین.
نشانی رایانامهٔ ایشان عبارت است از:
bastam@umz.ac.ir

احسان عطائی تحصیلات خود را در مقاطع کارشناسی، کارشناسی‌ارشد و دکترای رشتهٔ مهندسی کامپیوتر به‌ترتیب در سال‌های ۱۳۸۱، ۱۳۸۳ و ۱۳۹۶ از دانشگاه صنعتی شریف تهران دریافت کرد و هم‌اکنون دانشیار گروه مهندسی کامپیوتر دانشکدهٔ مهندسی و فناوری دانشگاه مازندران است. زمینه‌های پژوهشی مورد علاقهٔ ایشان عبارت‌اند از: رایانش ابری، سامانه‌های توزیع‌شده و مدل‌سازی کارایی و اتکاپذیری.
نشانی رایانامهٔ ایشان عبارت است از:
ataie@umz.ac.ir

[DOI: 10.61882/jsdp.22.2.65]