سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Fall 2024, 5 (3), 87-100
DOR:

Received: 23 June 2024
Accepted: 3 Aug 2024

مقاله پژوهشی

A Secure and Reliable Architecture for Managing Health Data in the Internet of Things using Blockchain and Deep Learning

Behnam Rezaei Bezanjan[1]. Seyyed Hamid Ghafouri[2*], Reza Gholamrezaei[3]

1. PhD Student, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran.
2. Assistant Professor, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran. .**Corresponding Author*, Sh.Ghafouri@iau.ac.ir
3. Assistant Professor, Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman, Iran.

Abstract

Introduction: The integration of Internet of Things (IoT) devices in the healthcare sector has brought significant advancements in patient care and data management. These technology-driven innovations hold great promise, while simultaneously raising important security concerns, particularly regarding the protection of medical data against potential cyber threats.

Method: In the initial phase, we leverage blockchain-based request and transaction encryption to enhance the security of data transactions, establishing an immutable and transparent framework.

Resultst: is used for attack classification. We compared the performance of the proposed method with three methods: AIBPSF-IoMT, OMLIDS-PBIoT, and AIMMFIDS. We achieved significant improvements in various metrics: accuracy (1%), precision (1%), recalling (1%).

Discussion: This study presents an innovative approach to addressing the critical challenge of medical data security in the Internet of Things landscape. Our method seamlessly integrates blockchain technology and advanced machine learning techniques, providing a robust framework for enhancing the confidentiality and integrity of sensitive healthcare information.

Keywords: Blockchain. Privacy-Preserving, Health Care, Machine Learning, ray Wolf Optimization

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد زنجان

یک معماری امن و قابل‌اعتماد برای مدیریت داده‌های سلامت در اینترنت اشیا با استفاده از بلا ک‌چین و یادگیری عمیق

تاریخ دریافت: ۰۳ /۰٤ /۱٤۰۳
تاریخ پذیرش: ۱۳/ ۰۵/ ۱٤۰۳

دورهٔ پنجم، پاییز ۱٤۰۳
شمارهٔ سوم، صص: ۸۷-۱۰۰

بهنام رضائی بزنجانی[۱] ، ،سیدحمیدرضا غفوری[۲*] ، رضا غلامرضایی[۳]

۱. دانشجوی دکتری، گروه کامپیوتر و فناوری اطلاعات، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران. B.rezai@kmu.ac.ir
۲. استادیار، گروه کامپیوتر و فناوری اطلاعات، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران. (نویسنده مسئول) Sh.Ghafouri@iau.ac.ir
۳. استادیار، گروه کامپیوتر و فناوری اطلاعات، واحد کرمان، دانشگاه آزاد اسلامی، کرمان، ایران.gholamrezaei@iauk.ac.ir

چکیده: ترکیب د ستگاه‌های اینترنت ا شیا (IoT) در بخش بهدا شت و درمان، پی‌شرفت‌های زیادی در مراقبت از بیمار و مدیریت داده ها ایجادکرده‌اســت. این نوآوری های مبتنی بر تکنولوژی وعده های بزرگی دارند، همزمان نگرانی های امنیتی مهمی را نیز به‌ویژه در محافظت از داده‌های پز شکی در برابر تهدیدات سایبری بالقوه ایجادمی‌کنند. با توجه به ماهیت حساس اطلاعات مرتبط با سلامت افراد، نیازمند اقدامات قوی برای تضمین محرمانگی، یکپارچگی و دسترس‌پذیری داده‌ها ی بیمار در محیط‌های پزشکی مبتنی بر اینترنت اشیا است. برای پاسخگویی به نیاز ضروری امنیت بیشتر در سیستم‌های مراقبت بهداشتی مبتنی بر اینترنت ا شیا، ما یک روش جامع شامل ســه مرحله متمایز را پیشــنهادمی‌کنیم. در مرحله اول، از رمزگذاری درخواســت و تراکنش مبتنی بر بلاک‌چین برای تقویت امنیت ترا کنش‌های داده اســتفاده‌می‌کنیم که یک چارچوب تغییرناپذیر و شــفاف را فراهم‌می‌کند. در مرحله دوم، با اس‌تفاده از منابع داده متنوع، بررسی الگوی تشخیص درخواست را برای شناسایی و خنثی کردن تلاش‌های دسترسی غیرمجاز بالقوه معرفی‌می‌کنیم. در نهایت، مرحله سوم شامل انتخاب ویژگی و شبکه GRU برای افزایش دقت و کارایی ت شخیص نفوذ از طریق تکنیک‌های پی شرفته یادگیری ما شین اســت. ما نتایج شــبیه‌ســازی روش پیشــنهادی را با ســه روش مرتبط اخیر به نام‌هایAIBPSF-IoMT ، OMLIDS-PBIoT و AIMMFIDS مقایسه‌کردیم. معیارهای ارزیابی شامل نرخ ت شخیص، نرخ ه شدار کاذب، دقت، بازخوانی و صحت، معیارهای مهم در ارزیابی عملکرد کلی سی ستم‌های ت شخیص نفوذ ه ستند. یافته‌های ما ن شان‌می‌دهد که روش پی شنهادی در مقای سه با تمام معیارهای ارزیابی شده، عملکرد بهتری ن سبت به روش‌های موجود دارد که برتری آن را در بهبود و ضعیت امنیتی سی ستم‌های مراقبت بهدا شتی مبتنی بر اینترنت اشیا تأکیدمی‌کند.

واژه‌های کلیدی: بلا ک‌چین، حریم خصوصی، یادگیری عمیق، داده‌های سلامت، یادگیری ماشین.

۱. مقدمه

در سال‌های اخیر، ادغام دستگاه‌های اینترنت اشیاء (IoT) در بخش بهداشت و درمان، پیشرفت‌های انقلابی زیادی در صنعت مراقبت بهداشتی و مدیریت داده‌های سلامت به همراه آورده‌است که همزمان نگرانی‌های جدی و مهمی در مورد آسیب‌پذیری‌های امنیتی و تهدیدات سایبری بالقوه را ایجادمی‌کنند. ماهیت حساس اطلاعات مرتبط با سلامت نیازمند اقدامات قوی و فوری برای تضمین محرمانگی، یکپارچگی و در دسترس بودن داده‌های بیمار در محیط‌های پزشکی مجهز به IoT است.[1]

۱- گسترش فناوری های اینترنت اشیا (IoT) تحولاتی انقلابی در صنایع مختلف ایجادکرده و اتصال و سهولت بی‌سابقه‌ای را ارائه‌داده‌است . با این حال، گسترش سیستم‌های IoT نگرانی‌های را نیز در مورد آسیب پذیری امنیتی و حملات سایبری بالقوه ایجادکرده‌است. [۱، 2] برای رسیدگی به این چالش ها، محققان به

۲- دنبال راه‌حل‌های جدید در تقاطع فناوری بلاک‌چین (BC)و یادگیری عمیق (DL) بوده‌اند تا امنیت و کارایی اکوسیستم های IoT را افزایش دهند.

۳- فناوری BC که در ابتدا به عنوان چارچوب زیربنایی برای ارزهای دیجیتال طراحی شده‌بود، به عنوان یک رویکرد قوی و غیرمتمرکز برای ایمن سازی ترا کنش‌های داده ظهورکرد .[3] کاربرد آن در حوزه IoTپارادایم جدیدی را معرفی‌می‌کند که در آن اعتماد، شفافیت و تغییرناپذیری نقش‌های اساسی در محافظت از اطلاعات حساس ایفامی‌کنند. مطالعات اخیر مانند [4] GT x Chain و-AIBPSF [5] IoMTتو سعه معماری‌های امن و هو شمند BC IoT را ن شان می‌دهند که از تکنیک‌های پیشرفته از جمله شبکه‌های عصبی گرافی و هوش مصنوعی برای تقویت یکپارچگی شبکه‌های IoT استفاده‌می‌کنند. از سوی دیگر، DL به دلیل دقت بی‌نظیر خود در تحلیل داده و تشخیص الگو، توجه بسیاری در حوزه های مختلف جلب‌کرده‌است[6,7] با کاربردهایی در حوزه‌های بهداشت، پردازش تصویر پزشکی و امنیت سایبری [8، 9]، الگوریتم‌های DL توانایی خود را در حل چالش های پیچیده نشان‌داده‌اند. ادغام BC و DL در تحقیقات اخیر مورد بررسی قرارگرفته‌است تا از نقاط قوت هر دو فناوری برای افزایش امنیت و قابلیت‌های پیش‌بینی استفاده‌شود [11،10]

این مقاله رویکرد نوآورانه‌ای برای رسیدگی به چالش حیاتی امنیت داده‌های پزشکی در چشم‌انداز اینترنت اشیا معرفی‌می‌کند . روش ما به طور یکپارچه فناوری بلاک‌چین و تکنیک‌های پیشرفته یادگیری ماشین را ادغام می‌کند. به‌طور خاص، **(GRU)** واحد بازگشتی دروازه دار(چارچوبی قوی برای افزایش محرمانگی و یکپارچگی اطلاعات حساس

سهم اصلی این مطالعه به شرح زیر است:

تقویت امنیت داده‌های پز شکی: ما یک روش نوآورانه پی شنهاد میکنیم که فناوری بلاک‌چین را با شبکه GRUسبک شده ادغام مراقبتی فراهم‌می‌کند . یک رویکرد جامع با سه مرحله متمایز برای پاسخگویی به نیاز فوری بهبود امنیت در سیستم‌های مراقبت بهداشتی مبتنی بر اینترنت اشیا پیشنهادگردید. در مرحله اول، ما قابلیت اطمینان دستگاه‌های IoT را از طریق تخمین اعتماد مبتنی بر شهرت و ذخیره-سازی داده خارج از زنجیره ارزیابی کردیم .مرحله دوم از فناوری بلاک-چین برای جلوگیری از حملات و تأیید اعتبار داده‌ها استفاده‌می‌کند. در مرحله سوم، از هوش مصنوعی، به‌ویژه GRU سبک‌شده، برای طبقه-بندی حملات استفاده‌می‌شود. جنبه‌های منحصر به فرد ادغام:

ادغامGRU با بلاک‌چین رویکرد نوآورانه‌ای است که از نقاط قوت هر دو فناوری بهره‌می‌برد. در حالی که بلا ک‌چین امنیت و تغییرناپذیری داده ها را تضمین‌می‌کند، GRUدر مدیریت داده‌های ترتیبی برتری دارد و آن را برای تشخیص الگوها و ناهنجاری‌های در داده‌های بهداشتی بسیار مؤثر می‌سازد.

توانایی GRU سبک‌شده در پردازش داده‌ها دقت و قابلیت اطمینان تشخیص حملات را بهبود می‌بخشد و از روش‌های سنتی یادگیری ماشین که وابستگی‌های زمانی در داده‌ها را در نظر نمی-گیرد، بهتر عمل‌می‌کند.

فناوری بلاک‌چین با غیرمتمرکز کردن ذخیره داده‌ها و ارائه یک دفتر کل شفاف و ضد دستکاری، یک لایه امنیتی اضافه‌می‌کند که به طور قابل‌توجهی یکپارچگی و اعتماد به داده‌ها را افزایش می‌دهد.

با وجود راه‌حل‌های ارائه‌شده توسط محققان، هنوز مشکلاتی وجود دارد که باید بررسی و حل شود. ما این مشکلات را در بخش ۱،۱ بیان‌کرده‌ایم.

لازم به توضیح است این مقاله توسعه‌ای از مقاله [1] که در ژورنال "Supercomputing" در سال ۲۰۲۴ منتشر شده‌است می‌باشد که ما در این تحقیق برخی الگوریتم‌ها و تکنیک‌ها را مورد بررسی و پژوهش قرار داده‌ایم.

2. بیان مسأله

با وجود پیشرفت‌های قابل‌توجه در این زمینه، چندین مسئله بحرانی همچنان حل‌نشده باقی مانده‌است ازجمله ناتوانی در پیش‌بینی حملات جدید: تکنیک‌های یادگیری ماشین سنتی، گرچه دقیق هستند، اما به دلیل انطباق محدود با الگوهای حمله جدید و پیچیده، قادر به شناسایی تهدیدات جدید و پیچیده نیستند.[4-1] فقدان تعمیم پذیری: تحقیقات قبلی معمولاً بر طیف محدودی از انواع حملات متمرکز بوده‌است که تشخیص جامع الگوهای مختلف حمله را مانع شده و شکاف‌های امنیتی قابل‌توجهی را ایجادمی‌کند [22،20،10]

۳. مشارکت اصلی ما

می‌کند تا حریم خصوصی و امنیت داده ها را افزایش‌دهد، که به‌طور خاص برای مقابله با مشکل تشخیص تهدیدات جدید و پیچیده طراحی شده‌است.

جلوگیری از بیش برازش و کاهش زمان آموزش: روش ما از یک رویکرد انتخاب ویژگی استفاده‌می کند که از بیش برازش جلوگیری می‌کند و زمان آموزش و آزمایش شبکه GRU را بدون حفظ دقت بالا کاهش می‌دهد. این به طور مستقیم با چالش تعمیم پذیری محدود با بهبود کارایی و انطباق‌پذیری مدل مقابله می‌کند.

پیش‌بینی انواع مختلف حمله: روش پیشنهادی بر روی دو مجموعه داده مختلف ارزیابی شده‌است و عملکرد برتر در پیش‌بینی بیش از ده نوع حمله مختلف را نشان‌می‌دهد، بنابراین پوشش گسترده‌تر و جامع‌تر تهدیدات بالقوه را تضمین می‌کند. جدول ۱ مقایسه روش‌های قبلی با روش پیشنهادی را نشان‌می‌دهد. برخی اختصارات در متن استفاده‌شده‌است.

جدول ۱: مقایسه روش‌های قبلی و روش جدید

نرخ خطا	نرخ تشخیص	دقت	F1امتیاز	فراخوانی	صحت	متد
×	✓	✓	×	×	✓	[11]
×	✓	✓	×	×	✓	[33]
✓	×	✓	×	✓	×	[35]
✓	✓	✓	✓	✓	✓	**روش پیشنهادی**

جدول ۲: توضیح اختصارات

شرح	نماد	شرح	نماد
شبکه های عصبی بازگشتی	RNN	اینترنت اشیا	IoT
مثبت واقعی	TP	واحد بازگشتی دروازه دار	GRU
مثبت کاذب	TN	اینترنت اشیا وسیله نقلیه	IoV
منفی واقعی	FP	ذخیره‌سازی بهینه داده‌های پویا	ODDS
منفی کاذب	FN	الگو ریتم بهینه‌سازی گرگ خاکستری	GWO
یادگیری عمیق	DL	یادگیری ماشین	ML
اینترنت اشیا داده‌های پزشکی	IoMT	بلا کچین	BC

۴. کارهای مرتبط

با گسترش فناوری‌های مانند داده‌های بزرگ، رایانش ابری و اینترنت ا شیا، اطلاعات شخ صی و داده‌های حساس بیشتری در شبکه ذخیره می‌شوند. این نه‌تنها خطر دسترسی غیرقانونی و سرقت داده ها را افزایش می‌دهد، بلکه خسارات بالقوه حملات سایبری را نیز جدی تر می‌کند. چگونگی بهبود دقت و توانایی پاسخ دهی بلادرنگ ادراک امنیت سایبر ی (CSP) در محیط‌های شبکه پیچیده، به موضوعی ترند در تحقیقات فعلی تبدیل شده‌است. تحقیقات موجود نشان می‌دهد که فناوری یادگیری عمیق دارای طیف گسترده ای از چشم اندازهای کاربردی در حوزه امنیت سایبر ی است، که در آن شبکه های عصبی کانولوشنال (CNN) و شبکه های عصبی بازگشتی (RNN) به دلیل مزایای آن‌ها در استخراج ویژگی و تحلیل سری‌های زمانی، محبوب ترین‌ها در حوزه CSP شده‌اند. با این حال، با وجود عملکرد عالی CNNها در پردازش داده‌های تصویر و دنباله، یک مدل واحد CNN هنوز در مواجهه با تهدیدات چندبعدی در محیط‌های شبکه پیچیده، محدودیت‌هایی دارد . [37]در سال های اخیر چندین روش با استفاده از BC و DL برای حفظ امنیت و حریم خصوصی داده ها پیشنهاد شده‌است. در این بخش، کارهای مرتبط را بررسی و مقایسه می کنیم. یک رویکرد پیشرفته برای تشخیص حملات با ت نت در سیستم های IoT صنعتی در [15] پیشنهاد شده‌است. روش آن ها از DL چندلایه استفاده می‌کند و یک استراتژی پیشگیرانه برای کاهش تهدیدات امنیتی در ارتباطات بی سیم و محیط‌های محاسبات موبایل را نشان می‌دهد. این مطالعه بر تقویت پایداری سیستم‌های IoT صنعتی در برابر تهدیدات سایبری در حال تحول، به‌ویژه تهدیدات مرتبط با حملات بات نت، تمرکز دارد. در [16]، نویسندگان روش جدیدی به نام BlockMedCare، یک سیستم مراقبت بهداشتی جدید که IoT، BC و سیستم فایل بین‌سیاره‌ای (IPFS) را ادغام می‌کند، معرفی‌کردند. کار آن‌ها به مسائل امنیتی مدیریت داده در مراقبت‌های

بهداشتی با استفاده از فناوری BC می پردازد. این سیستم هدف دارد یکپارچگی و محرمانگی داده‌های بهداشتی را تضمین کند و به بحث گسترده تر در مورد افزایش امنیت در انفورماتیک سلامت کمک می‌کند. یک روش رمز گذاری و احراز هویت سبک توزیع‌شده با مصرف انرژی کم در [17] ارائه شده‌است که برای افزایش امنیت در ارتباطات IoT طراحی شده‌است. در تحقیق دیگری [25]، نویسندگان مدل‌های پرتگاه مبتنی بر محلی سازی ترکیبی را برای ایمن سازی مهاجرت داده در مراکز ابری پیشنهاد کرده‌اند. این کار بر افزایش امنیت فرآیندهای انتقال داده در محیط‌های ابری تمرکز دارد. با استفاده از یک رویکرد محلی سازی ترکیبی، این مطالعه به پرتگاه‌ها می‌پردازد و به امنیت کلی مهاجرت داده در مراکز ابری کمک می‌کند. در [26]، با استفاده از یک رویکرد مبتنی بر بلاک‌چین توزیع شده، یک چارچوب محافظتی برای سیستم‌های قدرت مدرن در برابر حملات سایبری معرفی شده‌است. این کار حول محور تقویت امنیت سایبری سیستم‌های قدرت مدرن با استفاده از فناوری BC می‌چرخد. این چارچوب با استفاده از اقدامات حفاظت از داده توزیع‌شده و امن، از سیستم‌های قدرت در برابر تهدیدات سایبری محافظت می‌کند. نویسندگان یک معماری ناقل داده انعطاف‌پذیر و مقرون به صرفه برای قراردادهای هوشمند در بلاک‌چین ارائه می‌دهند [27]. با تمرکز بر کاربردهای قرارداد هوشمند، این مطالعه به مسائل مقیاس‌پذیری و هزینه در سیستم‌های مبتنی بر بلاک‌چین می‌پردازد. معماری پیشنهادی کارایی و مقرون به صرفه بودن ناقل‌های داده در اجرای قراردادهای هوشمند را افزایش می‌دهد. در [28]، یک چارچوب تشخیص حمله توزیع شده مبتنی بر یادگیری نیمه نظارتی برای اینترنت اشیا پیشنهاد شده‌است. این چارچوب با استفاده از تکنیک های یادگیری نیمه‌نظارتی به بهبود تشخیص حمله در محیط‌های IoT کمک می‌کند. این رویکرد با استفاده از داده‌های برچسب دار و بدون برچسب، پایداری تشخیص حمله در سناریوهای IoT توزیع شده را افزایش می‌دهد. یک سیستم تشخیص نفوذ مبتنی بر DL در [29] معرفی شده‌است. با تمرکز بر امنیت شبکه، از تکنیک‌های DL برای تقویت تشخیص نفوذ استفاده می‌کند. این مطالعه با پرداختن به چالش های ایجاد شده تو سط مخالفان و افزایش قابلیت های DL در کاربرد های امنیتی، به حوزه تشخیص نفوذ کمک‌می‌کند.

۵.روش پیشنهادی

ظهور تکنولوژِی‌های جدید در جهت بازسازی روش‌های نو برای مقاصد پزشکی و سلامت به‌شدت در حال تکامل است با این حال، با گسترش دستگاه‌های متصل و تبادل یکپارچه داده‌های پزشکی، نگرانی اصلی تضمین امنیت و حریم خصوصی اطلاعات حساس می‌شود. این مقاله به بررسی یک رویکرد جامع برای حفظ امنیت داده های پزشکی در چارچوب IoT می‌پردازد. با بررسی هم‌افزایی فناوری BC، روش گرگ خاکستری بهینه شده برای انتخاب ویژگی و شبکه GRU،سبک شده که با هم تلفیق‌شده و در آن قصد داریم یک استراتژی یکپارچه را تشریح‌کنیم که نه‌تنها محرمانگی و یکپارچگی داده‌های پزشکی را تقویت می‌کند، بلکه تاب‌آوری کل اکوسیستم مراقبت بهداشتی را در برابر تهدیدات سایبری که در حال تحول است را تضمین می‌کند. در این کار یک سیستم تشخیص نفوذ ترکیبی ارائه شده‌است که بر اساس تکنیک-های یادگیری ماشین/یادگیری عمیق می باشند.

رویکرد پیشنهادی بر پایه استفاده از شبکه عصبی بازگشتی دروازه دار (GRU) در ترکیب با الگوریتم گرگ خاکستری (GWO) (GRU-GWO)استوار است. از یک تکنیک فراابتکاری (GWO) برای کاهش بعد و پیچیدگی ویژگی‌ها با استخراج زیرمجموعه‌ای از ویژگی‌ها با عملکرد برتر از مجموعه داده‌های NSL-KDD و UNSW-NB15برای تحلیل شبکه ترافیک استفاده‌می‌کند. برای هر مجموعه داده، زیرمجموعه‌ای از ویژگی‌ها از کل مجموعه انتخاب‌شد.

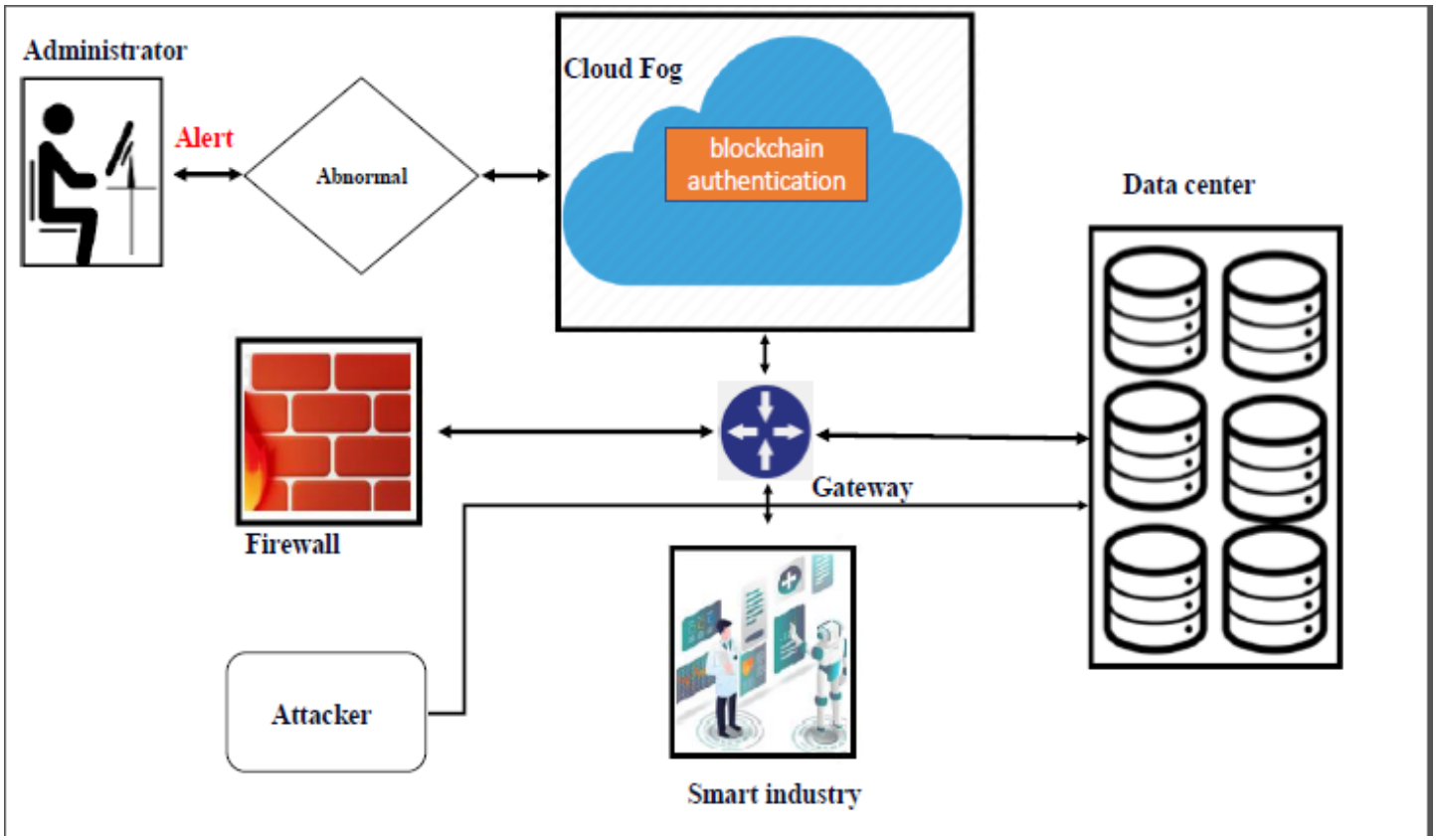

Figure 1: Framework of the proposed method

چارچوب روش پیشنهادی (شکل 1) شامل دو جزء است. قابلیت همکاری عامل امنیتی هوش مصنوعی فعال شده توسط بلاک‌چین در یک فرآیند سه مرحله‌ای نشان داده شده است :فاز ۱: رمزگذاری درخواست و تراکنش فعال شده توسط بلا ک‌چین: این فاز تضمین می کند که همه درخواست‌ها و تراکنش‌ها با استفاده از سکو بلاک‌چین امضا و تأیید می‌شوند. این یک چارچوب تغییر ناپذیر و شفاف برای تراکنش‌های داده ایمن فراهم می‌کند. فاز:۲ الگوریتم ویژگی ها قبل از آموزش مدل با استفاده از GWO اصلاح شده انتخاب می شوند. این مرحله برای افزایش دقت و کارایی سیستم تشخیص نفوذ بسیار مهم است. ویژگی‌های انتخاب شده سپس توسط شبکه GRU شده پردازش می‌شوند که در مورد مشروعیت درخواست ها تصمیم‌گیری می کند. در ادامه اجرای الگوریتم فرابتکاری و آموزش مدل دروازه بازگشتی را شرح‌می‌دهیم.

۵،۱. اجرای الگوریتم GWO

۱. **ابتداسازی جمعیت گرگ‌ها :**یک جمعیت اولیه از گرگ‌ها در فضای جستجو ایجاد می شود، هر گرگ یک مجموعه از پارامترهای مدل را نشان می‌دهد.

۲. **به‌روزرسانی موقعیت گرگ‌ها:** با استفاده از قوانین به‌روزرسانیGWO ، موقعیت گرگ‌ها را در هر تکرار به روز رسانی می‌شود.

۳. **گرگ‌ها:** عملکرد هر گرگ را با ارزیابی آن بر روی داده‌های آموزشی ارزیابی می‌شود.

۴. **توقف:** به این فرآیند ادامه‌می‌دهیم تا یک شرط توقف مانند رسیدن به تعداد مشخصی تکرار یا کاهش خطا به زیر یک آستانه مشخص برآورده می‌شود.

۵،۲.آموزش مدل GRU

- **آموزش مدل GRU با پارامترهای بهینه :** مدل GRU را با ا ستفاده از پارامترهای بهینه یافت شده توسط GWO آموزش‌می‌دهیم.
- **ابتدا سازی GRU:** وزن‌های GRU به صورت تصادفی مقدار دهی اولیه می‌شود.
- **آموزش GRU:** GRU با استفاده از BPTT روی داده‌های آموزشی آموزش داده می‌شود.
- **بهینه سازی پارامترهای با GWO:** GWO برای بهینه سازی پارامترهای GRU استفاده می‌شود. هر گرگ یک مجموعه از پارامترهای GRU را نشان می‌دهد و GWO به تدریج به سمت بهترین مجموعه پارامترهای همگرا می‌شود.
- **آموزش مجدد GRU:** GRU با پارامترهای بهینه شده مجددا آموزش داده می‌شود
- .**تکرار مراحل ۳ و ۴:** مراحل ۳ و ۴ تا رسیدن به هم گرایی یا دستیابی به عملکرد رضایت‌بخش تکرار می‌شوند.

۵،۳.مراحل الگوریتم پیشنهادی

الگوریتم پیشنهادی یک رویکرد جامع برای ایجاد یک سیستم امنیتی پیش‌بینی کننده مبتنی بر هوش مصنوعی و بلاک‌چین است که به‌طور خاص برای داده‌های پزشکی IoT طراحی شده‌است. در ادامه، هر مرحله از این الگوریتم مفصل توضیح داده‌می‌شود

مرحله ۱: راه‌اندازی بلاک‌چین ایجاد شبکه بلاک‌چین: در این مرحله، یک شبکه بلاک‌چین جدید ایجادمی شود. بلاک‌چین به عنوان یک دفتر کل توزیع شده عمل‌می‌کند و تمام تراکنش‌ها و داده‌ها را به صورت امن و شفاف ثبت‌می‌کند.

تعریف قراردادهای هوشمند: قراردادهای هوشمند برنامه های کامپیوتری هستند که مستقیماً در بلاک‌چین اجرا می‌شوند. در این مرحله، قراردادهای هوشمندی تعریف می‌شوند که قوانین و مقررات مربوط به یکپارچگی و امنیت داده‌ها را اجرا می‌کنند. این قراردادهای تضمین می‌کند که داده‌ها به صورت ایمن ذخیره و پردازش شوند

مرحله ۲: جمع‌آوری داده جمع‌آوری داده از دستگاه‌های IoT پز شکی: داده‌ها از طیف و سیعی از د ستگاه های IoT پز شکی مانند حس گرها، دستگاه‌های پوشیدنی و سایر دستگاه‌های متصل جمع‌آوری می‌شود.

پیش‌پردازش داده‌ها: داده‌های جمع‌آوری شده ممکن است حاوی نویز، مقادیر گم‌شده یا ناسازگاری باشند. بنابراین، قبل از استفاده از داده‌ها، باید آن‌ها را تمیز و نرمال‌سازی کرده و مقادیر گم شده را پر کرد.

مرحله ۳: استخراج ویژگی‌های مرتبط: از داده‌های پیش پردازش شده، ویژگی‌های مهمی که برای تشخیص ناهنجاری یا مدل‌سازی پیش‌بینی‌کننده مفید هستند، استخراج می‌شوند. این ویژگی‌ها می‌توانند آماری، زمانی یا مبتنی بر فرکانس باشند.

انتخاب ویژگی و کاهش ابعاد: پس از ا ستخراج ویژگی‌ها، ویژگی‌های مهم‌تر انتخاب‌می‌شوند و ابعاد فضای ویژگی کاهش می‌یابد تا کارایی مدل یادگیری ماشین بهبودیابد.

مرحله ۴: آموزش مدل یادگیری ماشین تقسیم داده ها به مجموعه آموزش و آزمون: داده های آ ماده‌شده به دو مجموعه تقسیم‌می‌شوند: مجموعه آموزش برای آموزش مدل و مجموعه آزمون برای ارزیابی عملکرد مدل.

آموزش مدل بر روی داده های آموز شی: مدل یادگیری ماشین با استفاده از داده‌های آموزشی آموزش داده می‌شود. در این مرحله، پارامترهای مدل به گونه‌ای تنظیم می‌شود که خطای بین خروجی پیش‌بینی شده و خروجی واقعی به حداقل برسد.

اعتبار سنجی مدل با ا ستفاده از روش‌های اعتبار سنجی متقابل: عملکرد مدل آموزش دیده با استفاده از تکنیک‌های اعتبارسنجی متقابل مانند اعتبارسنجی متقاطع k برابر ارزیابی می‌شود. این کار برای جلوگیری از بیش‌برازش مدل و ارزیابی توانایی تعمیم مدل به داده های جدید انجام می‌شود.

مرحله ۵: استقرار مدل آموزش‌دیده بر روی دستگاه‌های لبه: مدل آموزش‌دیده بر روی دستگاه‌های لبه مانند دروازه‌های IoT یا دستگاه‌های موبایل مستقر می‌شود. این کار به پردازش داده‌ها در زمان واقعی و کاهش تأخیر کمک‌می‌کند.

پیاده‌سازی استنباط محلی برای تشخیص ناهنجاری: مدل مستقر شده برای تشخیص ناهنجاری‌های داده‌های ورودی در زمان واقعی

اســـتفاده می‌شـــود. هرگونه انحراف از الگوهای نرمال به عنوان یک ناهنجاری علامت‌گذاری می‌شود

مرحله ۶: یکپارچه‌سازی بلاک‌چین ثبت ناهنجاری‌های تشخیص داده شده و داده های د ستگاه بر روی بلاک‌چین: هنگامی که یک ناهنجاری تشخیص داده می‌شود، اطلاعات مربوط به آن (مانند شناسه دســتگاه، زمان و نوع ناهنجاری) بر روی بلاک‌چین ثبت می‌شـــود. این کار تضمین می کند که داده ها غیرقابل تغییر و شفاف باشند.

استفاده از قراردادهای هوشمند برای ایجاد هشدار و پاسخ های خودکار: قراردادهای هوشمند می‌تواند بر اساس ناهنجاری‌های ثبت‌شده فعال شوند و هشدارها را برای کاربر ارسال‌کنند یا پاسخ‌های خودکار را اجراکنند. این پاسخ‌ها ممکن شامل فعال‌کردن پروتکل های امنیتی، اطلاع دادن به پرسنل پزشکی یا انجام اقدامات اصلاحی دیگر باشد. این الگوریتم یک رویکرد جامع برای ایجاد یک سیستم امنیتی پیش‌بینی کننده برای داده‌های پزشکی IoT ارائه‌می‌دهد. با ترکیب قدرت هوش مصنوعی و بلاک‌چین، این سیستم قادر است ناهنجاری‌ها را دقیق تشخیص‌دهد، یکپارچگی داده ها را حفظکند و پاسخ‌های خودکار را برای اطمینان از امنیت داده های پزشکی فعال کند.

۶..ارزیابی و نتایج

نتایج شـــبیه‌ســـازی روش پیشـــنهادی بر روی دو مجموعه داده مجزا، NSL-KDD [30]، UNSW-NB15 [۳۳] و ارزیابی شده‌ا ست. در ادامه، نتایج با یافته‌های کارهای قبلی که به عنوان [۱۱، 33] و [۳۵] ذکر شده مقایسه می‌شود. این تحلیل مقایسه‌ای با هدف سنجش اثربخ شی و عملکرد روش پی شنهادی در مقای سه با رویکردهای موجود بر روی مجموعه داده‌های UWSN، WUSTLEHMS-2020 و NSL-KDD انجام‌می‌شود.

۶,۱ تنظیمات آزمایشی

آزمایش‌ها بر روی سیستمی با پردازنده Intel Core i7-10700K با ۸ هســته و ۱۶ رشــته با فرکانس پایه ۳,۸۰ گیگاهرتز انجام‌شـد. این ســیســتم به ۳۲ گیگابایت رم DDR4 و یک SSD NV Me 1 ترابایتی برای ذخیره‌ســـازی مجهز بود. در مرحله انتخاب ویژگی، از الگوریتم بهینه‌سازی گرگ خاکستری (GWO) با اندازه جمعیت 25 و حداکثر 50 تکرار استفاده‌شد.

۶,۲ معیارهای عملکرد

۶,۲,۱ دقت :(precision) این معیار سنجش نشان‌می‌دهد که یک مدل چقدر می‌تواند موارد مثبت را در ست شنا سایی کند، بدون اینکه موارد منفی کاذب (false positive) را در نظر بگیرد .به عبارت دیگر، دقت بیانگر آن است که چه درصدی از پیش‌بینی‌های مثبت مدل، واقعاً درست هستند.

$$Prec. = \frac{TP}{FP + TP} \qquad (1)$$

۶,۲,۴ بازخوانی :(Recall) این معیار سنجش نشان می‌دهد که یک مدل چقدر می‌تواند تمام موارد مثبت واقعی را به‌درســتی شــناســایی کند . به عبارت دیگر، بازخوانی بیانگر آن است که چه درصدی از موارد مثبت واقعی توسط مدل به عنوان مثبت پیش‌بینی شده‌اند.

$$Rec. = \frac{TP}{FP + FN} \qquad (4)$$

$$Accuracy = \frac{TP + TN}{Total\ Instances} \qquad (3)$$

۶,۲,۶ F1-Score: این معیار ســنجش میانگین وزنی بین دقت و بازخوانی اســت F1-Score .به شـما کمک می‌کند تا تعادلی بین این دو معیار مهم ایجادکنید.

$$F1 - Score = \frac{2 \times Prec. \times Rec.}{Prec. + Rec.} \qquad (2)$$

۶,۲,۳ دقت: (Accuracy)معیاری اســـت که میزان درســـتی کلی پیش‌بینی‌ها را اندازه‌گیری می‌کند .

۶,۲,۵ نرخ تشخیص (Detection Rate) : معیاری است که به طور گسترده در زمینه‌های مختلف مانند پزشکی، مهندسی، علوم کامپیوتر و ...برای سنجش عملکرد سیستم‌ها یا مدل‌ها در شناسایی موارد مثبت واقعی استفاده می‌شود .این معیار به عنوان **نرخ مثبت واقعی (True Positive Rate)**و **حساسیت (Sensitivity)**نیز شناخته می‌شود.

$$DR = \frac{TP}{TP+FN} \quad (5)$$

۶،۲،۶. نرخ هشدار اشتباه : (False Alarm Rate)معیاری است که نشـان می‌دهد یک سـیسـتم یا مدل چقدر در تشـخیص موارد مثبت کاذب (False Positives) تمایل دارد .این معیار با فرمول (۱۸) که در متن اصلی ذکرشده، محاسبه می‌شود.

$$FAR = \frac{FP}{FP+TN} \quad (6)$$

۷. تجزیه و تحلیل نتایج

روش پیشـــنهادی، همراه با ســـایر روش‌های ارزیابی‌شـــده، متریک‌های عملکرد بالاتری را در مجموعه داده NSL-KDD نســـبت به مجموعه داده UNSW-NB15 نشان‌می‌دهد.

نمرات دقت، فراخوانی درجدول ۳ و ۴ آمده‌است، روش پیشنهادی و سایر روش‌ها در مجموعه داده NSL-KDD نسبت به مجموعه داده UNSW-NB15 عملکرد بهتری داشـته‌اند. دلیل این امر تعداد بالای حملات در مجموعه داده UNSW-NB15 اســـت که پیچیده‌تر از داده‌های NSL-KDD اســـت. تکنیک انتخاب ویژگی که در این مقاله اســـتفاده کردیم، به GRUســـبک شـــده قدرت تعمیم خوبی بخشـــید.

جدول ۵ و ۶ روش‌های مختلف را از نظر دقت، فراخوانی، در مجموعه داده UNSW-NB15 مقایسه‌می‌کنند.

دقت: توانایی شبکه دروازه بازگشتی در پردازش و درک از وابستگی‌های زمانی را افزایش می‌دهد و منجر به بهبود عملکرد پیش‌بینی می‌شـــود. در نتیجه، مدل پیشـــنهادی مداوم دقت بالاتری نســـبت به ســـایر رویکردهای به دست می‌آورد.

جدول 3: نمرات دقت روش‌های مختلف اعمال‌شده بر روی مجموعه داده NSL-KDD

نوع حمله	روش پیشنهادی	AIBPSF-IoMT	OMLIDS-PBIoT	AIMMFIDS
DoS	**94.2**	93.2	91.4	88.7
R2L	**95.6**	95.4	93.3	90.9
Probe	**96.8**	94.1	91.7	89.8
U2R	**94.9**	91.8	89.7	88.2
Normal	**95.1**	95.9	93.8	91.8
Average	**95.3**	94.4	92.2	90.3

جدول 4:نمرات فراخوانی روش های مختلف اعمال شده بر روی مجموعه داده.NSL-KDD

نوع حمله	روش پیشنهادی	AIBPSF-IoMT	OMLIDS-PBIoT	AIMMFIDS
DoS	**94.1**	93.2	91.4	88.7
R2L	**95.2**	95.4	93.3	90.9
Probe	**94.2**	94.1	91.7	89.8
U2R	**92.1**	91.8	89.7	88.2
Normal	**96.1**	95.9	93.8	91.8

Average	**94.3**	94.4	92.2	90.3

جدول 5: نمرات دقت روش های مختلف اعمال شده بر روی مجموعه داده.UNSW-NB15

نوع حمله	روش پیشنهادی	AIBPSF-IoMT	OMLIDS-PBIoT	AIMMFIDS
Backdoor	**93.1**	94.2	92.3	90.2
Worms	**95.7**	96.4	94.1	92.1
Shellcode	**95.2**	94.7	92.9	93.0
Exploits	**92.3**	93.5	91.7	89.3
Fuzzers	**96.9**	95.9	94.6	91.3
DoS	**94.9**	94.8	92.8	91.2
Reconnaissance	**94.2**	94.2	92.5	90.3
Analysis	**97.1**	95.8	94.3	92.1
Generic	**95.0**	94.7	93.4	91.2
Normal	**95.2**	94.8	92.8	91.3
Average	**94.9**	94.7	93.1	91.1

جدول 6: نمرات فراخوانی روش های مختلف اعمال شده بر روی مجموعه داده.UNSW-NB15

نوع حمله	روش پیشنهادی	AIBPSF-IoMT	OMLIDS-PBIoT	AIMMFIDS
Backdoor	**93.9**	92.3	90.2	88.4
Worms	**95.4**	94.5	92.1	90.2
Shellcode	**95.2**	93.4	91.3	88.9
Exploits	**94.3**	91.3	89.6	87.5
Fuzzers	**96.1**	95.1	92.6	90.8
DoS	**95.3**	92.9	91.4	89.1
Reconnaissance	**94.3**	92.1	90.2	88.7
Analysis	**95.1**	94.2	92.3	90.3
Generic	**91.3**	92.9	91.2	88.8
Normal	**94.9**	92.7	90.6	88.7
Average	**94.5**	93.1	91.2	89.1

نتایج آزمایش‌های نرخ تشـخیص و نرخ هشـدار کاذب در درصـدهای مختلف حمله در جدول ۷ و ۸ نشـان داده شـده‌اسـت. در تمام مقادیر AP، روش پیشـنهادی عملکردی بهتر از سـایر روش‌ها دارد. به عنوان مثال، در AP=30، نرخ تشخیص تنظیم شده 97.6٪ است که بالاتر از (95.8%)AIBPSF-IoMT، OMLIDS-PBIoT (۹۶،۲%) و AIMMFIDS (۹۳،۷٪) اسـت. ، در مجموعه داده UNSW-NB15، روش پیشـنهادی عملکرد برتر را در تمـام مقـادیر AP نشان‌می‌دهد. به عنوان مثال، در AP=30، نرخ تشخیص تن‌ظیم شده 94.3٪ اسـت که از (94.8%) AIBPSF-IoMT، OMLIDS-PBIoT (۹٤،٦%) و AIMMFIDS (۹۲،۸%) کاهش داشت.

جدول 7: نرخ تشخیص روش های مختلف اعمال شده بر روی مجموعه داده.NSL-KDD

نوع حمله	AP=30	AP=40	AP=50	AP=60	AP=70	AP=80
روش پیشنهادی	**97. 6**	**97.0**	**95.3**	**90.1**	**88.2**	**84.3**
AIBPSF-IoMT	95.8	94.1	91.9	89.7	84.7	82.2
OMLIDS-PBIoT	96.2	92.7	89.7	86.3	82.5	80.8
AIMMFIDS	93.7	92.65	88.5	85.3	81.8	79.2

جدول 8 :نرخ تشخیص روش های مختلف اعمال شده بر روی مجموعه داده UNSW-NB15

نوع حمله	AP=30	AP=40	AP=50	AP=60	AP=70	AP=80
روش پیشنهادی	**94.3**	**95.2**	**92.8**	**91.3**	**87.7**	**84.6**
AIBPSF-IoMT	94.8	92.7	90.3	88.2	84.3	81.2
OMLIDS-PBIoT	94.6	91.6	88.5	84.7	83.0	80.8
AIMMFIDS	92.8	92.6	87.9	85.3	79.8	77.5

جدول9 تحلیل مقایسه‌ای بین روش پیشنهادی و سه روش موجود: AIBPSF-IoMT، OMLIDS-PBIoT وAIMMFIDSارائه می‌دهد. معیارهای ارزیابی شامل دقت، فراخوانی، صحت، F1-score، نرخ تشخیص و نرخ هشدار کاذب هستند. این جدول به وضوح عملکرد برتر روش پیشنهادی را در همه معیارها، به‌ویژه در دستیابی به نرخ تشخیص بالا و نرخ هشدار کاذب پایین نشان می‌دهد، که برای تشخیص موثر نفوذ در محیط‌های IoT بسیار مهم هستند. این ارزیابی بر روی مجموعه داده WUSTL-EHMS-2020 که برای کار پزشکی ارائه شده‌است، انجام‌شد.

جدول 9. تحلیل مقایسه‌ای روش پیشنهادی و روش های موجود در مجموعه داده.WUSTL-EHMS-2020

متد	دقت(%)	صحت(%)	فراخوانی(%)	F1-امتیاز(%)	نرخ تشخیص (%)	نرخ هشدار کاذب (%)
متد پیشنهادی	**98.3**	**97.8**	**98.5**	**98.1**	**97.6**	**1.2**
AIBPSF-IoMT	95.5	94.2	95.8	95.0	94.7	2.5
OMLIDS-PBIoT	96.1	95.0	96.3	95.6	95.2	2.0
AIMMFIDS	94.8	93.5	95.0	94.2	93.8	3.0

۸.بحث

نتایج کارایی یادگیری عمیق ترکیبی پیشنهادی را نشان‌می‌دهد که شامل انتخاب ویژگی همراه با شبکه GRU برای ارائه تشخیص نفوذ بهبودیافته و دقیق با استفاده از روش‌های یادگیری ماشین است. برای آزمایش این روش، آن را با سه روش جدید دیگر در این زمینه مقایسه کردیم:

AIBPSF-IoMT، OMLIDS-PBIoT و AIMMFIDS.

نتایج نشان‌می‌دهد که ما همواره در دقت، صحت، فراخوانی و امتیاز F1، به طور قابل‌توجهی بهتر از دیگران عمل‌می‌کنیم.

Matlob و همکاران [۳۸] مطالعه‌ای را پیشنهادکردند که بر اهمیت در نظر گرفتن توالی تراکنش‌ها برای درک دقیق‌تر فعالیت‌های کلاهبرداری تأکیدمی‌کند. استفاده از مفاهیم استخراج توالی به این روش اجازه‌داد تا توالی‌های مشترک با الگوهای مختلف ایجاد کند. این انعطاف‌پذیری باعث افزایش انطباق‌پذیری مدل با سناریوهای متنوع و پیچیده مراقبت‌های بهداشتی شد. تنظیم دقیق موتور قوانین برای دقیقاً ضبط و نمایش توالی‌های قانونی و همزمان شناسایی ناهنجاری‌ها یک چالش بود. یافتن تعادل منا سب بین تولید و نگهداری قوانین برای اثربخشی این روش بسیار مهم بود.

Delal و همکاران [۳۹] رویکردی مبتنی بر الگوریتم XGBoost را به کارگرفتند و اهمیت تنظیم ابر پارامترها را برای بهبود عملکرد پیش‌بینی نشان‌دادند. این مطالعه در بهینه‌سازی XGBoost برای پیش‌بینی کلاهبرداری در خدمات پرداخت مالی کمک‌کرد. این رویکرد اثربخشی خود را در تشخیص فعالیت‌های کلاهبرداری در تراکنش‌های مالی دنیای واقعی نشان داد و پتانسیل راه‌حل‌های هوشمند را برای کمک قابل‌توجه به تشخیص کلاهبرداری در دامنه‌های مختلف برجسته‌کرد. علاوه بر این، اطمینان از مقیاس‌پذیری و قابلیت کاربردی بلادرنگ تکنیک ترکیبی پیشنهادی برای مدیریت حجم عظیمی از تراکنش‌های آنلاین و فعالیت‌های مالی یک مانع بالقوه بود که نیاز به توجه دقیق برای پیاده‌سازی عملی داشت.

۹.نتیجه گیری

این مقاله رویکردی نوآورانه برای رسیدگی به چالش حیاتی امنیت داده های پزشکی در چشم‌انداز اینترنت اشیا ارائه می‌دهد. روش ما فناوری بلاک چینو تکنیک‌های پیشرفته یادگیری ماشین را یکپارچه ترکیب می‌کند و چارچوبی قوی برای افزایش محرمانگی و یکپارچگی اطلاعات حساس مراقبتی فراهم‌می‌کند. ما رویکرد جامعی با سه مرحله مجزا برای پاسخگویی به نیاز فوری بهبود امنیت در سیستم‌های مراقبت بهداشتی مبتنی بر اینترنت اشیا پیشنهادکردیم. در مرحله اول، ما قابلیت اطمینان دستگاه‌های اینترنت اشیا را از طریق ذخیره‌سازی داده خارج از زنجیره ارزیابی‌کردیم. مرحله دوم از فناوری بلاک‌چین برای جلوگیری از حملات و تأیید اعتبار داده‌ها استفاده می‌کند. در مرحله سوم، از هوش مصنوعی برای طبقه‌بندی حملات استفاده می شود. ما Amponsah و همکاران [۴۰] رویکرد پیشگامانه‌ای را برای تشخیص کلاهبرداری در سیستم‌های مراقبت بهداشتی معرفی‌کردند که هدف آن کاهش کلاهبرداری به روشی ایمن و شفاف است. این

سیستم اثربخشی خود را در تشخیص دقیق فعالیت‌های کلاهبرداری در پردازش ادعاهای مراقبت‌های بهداشتی بادقت طبقه‌بندی بالا نشان داد. مقیاس‌پذیری سیستم پیشنهادی ممکن است به دلیل پردازش حجم زیادی از داده‌ها در سیستم‌های مراقبت بهداشتی به یک چالش تبدیل شود. اطمینان از عملکرد و پاسخگویی بهینه، به‌ویژه در سناریوهای بزرگ‌مقیاس، به‌عنوان یک جنبه چالش‌برانگیز در نظر گرفته‌شد.

عملکرد روش پیشنهادی را با سه روش AIBPSF-IoMT، OMLIDS-PBIoTو AIMMFIDSمقایسه کردیم. برای تأیید اثربخشی آن، چارچوب با مدل‌های امنیتی پیشرفته مقایسه شد. نتایج بهبود قابل توجهی را در چندین معیار نشان داد: افزایش 1٪ در دقت، صحت و فراخوان شد.در مطالعات آینده، تلاش‌های تحقیقاتی ما بر تقویت سیستم در برابر تهدیدهای نوظهور، به‌ویژه حملات خصمانه، تمرکز خواهدکرد. برای دستیابی به این هدف، قصد داریم از تکنیک‌های موازی سازی GPU برای افزایش سرعت محاسبات و اطمینان از درک عمیق‌تر از فرآیندهای تصمیم‌گیری سیستم و افزایش مقاومت آن در برابر سوءاستفاده‌های بالقوه استفاده‌کنیم.

Refrences:

1. Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2024). Fusion of machine learning and blockchain-based privacy-preserving approach for healthcare data in the Internet of Things. *The Journal of Supercomputing*, 1-29.
2. Saheed, Y. K., & Misra, S. (2024). A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the Internet of Things. *International Journal of Information Security*, 1-25.
3. Saheed, K.Y., Usman, A.A., Sukat, F.D., & Abdulrahman, M. (2023). A novel hybrid autoencoder and modified particle swarm optimization feature selection for intrusion detection in the internet of things network. *Frontiers of Computer Science*.
4. Khubrani, M. M. (2023). Artificial Rabbits Optimizer with Deep Learning Model for Blockchain-Assisted Secure Smart Healthcare System. *International Journal of Advanced Computer Science and Applications*, *14*(9).
5. Cai, J., Liang, W., Li, X., Li, K., Gui, Z., & Khan, M. K. (2023). GTxChain: a secure IoT smart blockchain architecture based on graph neural network. *IEEE Internet of Things Journal*.
6. Kumar, P., Kumar, R., Srivastava, G., Gupta, G. P., Tripathi, R., Gadekallu, T. R., & Xiong, N. N. (2021). PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. *IEEE*

Transactions on Network Science and Engineering, *8*(3), 2326-2341.
7. Shrestha, A., & Mahmood, A. (2019). Review of deep learning algorithms and architectures. *IEEE access*, *7*, 53040-53065.
8. Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., ... & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *Journal of big Data*, *8*, 1-74.
9. Ayyoubzadeh, S. M., Ayyoubzadeh, S. M., Zahedi, H., Ahmadi, M., & Kalhori, S. R. N. (2020). Predicting COVID-19 incidence through analysis of google trends data in Iran: data mining and deep learning pilot study. *JMIR public health and surveillance*, *6*(2), e18828.
10. Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. *International journal of medical informatics*, *148*, 104399.
11. Alshammari, B. M. (2023). AIBPSF-IoMT: Artificial Intelligence and Blockchain-Based Predictive Security Framework for IoMT Technologies. *Electronics*, *12*(23), 4806.
12. Afaq, Y., & Manocha, A. (2023). Blockchain and Deep Learning Integration for Various Application: A Review. *Journal of Computer Information Systems*, 1-14.
13. Shafay, M., Ahmad, R. W., Salah, K., Yaqoob, I., Jayaraman, R., & Omar, M. (2023). Blockchain for deep learning: review and open challenges. *Cluster Computing*, *26*(1), 197-221.
14. Mudassir, M., Unal, D., Hammoudeh, M., & Azzedin, F. (2022). Detection of botnet attacks against industrial IoT systems by multilayer deep learning approaches. *Wireless Communications and Mobile Computing*, *2022*.
15. Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal*, *23*(2), 329-343.
16. Sudhakaran, P. (2022). Energy efficient distributed lightweight authentication and encryption technique for IoT security. *International Journal of Communication Systems*, *35*(2), e4198.
17. Yin, C., Zhang, S., Wang, J., & Xiong, N. N. (2020). Anomaly detection based on convolutional recurrent autoencoder for IoT time series. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(1), 112-122.
18. Xu, Z., Liang, W., Li, K. C., Xu, J., & Jin, H. (2021). A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles. *Journal of Parallel and Distributed Computing*, *149*, 29-39.
19. Liang, W., Ning, Z., Xie, S., Hu, Y., Lu, S., & Zhang, D. (2021). Secure fusion approach for the internet of things in smart autonomous multi-robot systems. *Information Sciences*, *579*, 468-482.
20. Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*, 2858-2873.
21. Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics*, *10*(12), 1437.
22. Zhang, J. (2021). Distributed network security framework of energy internet based on internet of things. *Sustainable Energy Technologies and Assessments*, *44*, 101051.
23. Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475-491.
24. Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, *35*(1), 234-241.
25. Philip, A. O., & Saravanaguru, R. K. (2020). Secure incident & evidence management framework (SIEMF) for internet of vehicles using deep learning and blockchain. *Open Computer Science*, *10*(1), 408-421.
26. AlKadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2019). Mixture localization-based outliers models for securing data migration in cloud centers. *IEEE Access*, *7*, 114607-114618.
27. Liang, G., Weller, S. R., Luo, F., Zhao, J., & Dong, Z. Y. (2018). Distributed blockchain-based data protection framework for modern power systems against cyber attacks. *IEEE Transactions on Smart Grid*, *10*(3), 3162-3173.
28. Liu, X., Muhammad, K., Lloret, J., Chen, Y. W., & Yuan, S. M. (2019). Elastic and cost-effective data carrier architecture for smart contract in blockchain. *Future Generation Computer Systems*, *100*, 590-599.
29. Rathore, S., & Park, J. H. (2018). Semi-supervised learning based distributed attack detection framework for IoT. *Applied Soft Computing*, *72*, 79-89.
30. Wang, Z. (2018). Deep learning-based intrusion detection with adversaries. *IEEE Access*, *6*, 38367-38384.
31. Mirjalili, S., & Lewis, A. (2016). The whale optimization algorithm. *Advances in engineering software*, *95*, 51-67.

32. Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009, July). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE symposium on computational intelligence for security and defense applications* (pp. 1-6). Ieee.
33. Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 military communications and information systems conference (MilCIS)* (pp. 1-6). IEEE.
34. Al-Qarafi, A., Alrowais, F., S. Alotaibi, S., Nemri, N., Al-Wesabi, F. N., Al Duhayyim, M., ... & Al-Shabi, M. (2022). Optimal machine learning based privacy preserving blockchain assisted internet of things with smart cities environment. *Applied Sciences*, *12*(12), 5893.
35. Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, *16*(5), 1045-1057.
36. Hady, A. A., Ghubaish, A., Salman, T., Unal, D., & Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, 106576-106584.
37. Huang, Y., Zhao, Z., & Shi, C. (2024). Network Security Perception System Integrating Improved CNN Algorithm and Improved GRU Algorithm. IEEE Access.
38. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak and A. Munir, "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems", IEEE Access, vol. 10, pp. 48447- 48463, 2022.##
39. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak and A. Munir, "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems", IEEE Access, vol. 10, pp. 48447- 48463, 2022.S. Dalal, B. Seth, M. Radulescu, C. Secara and C. Tolea, "Predicting fraud in financial payment services through optimized hyperparameter-tuned XGBoost model", Mathematics, vol. 10, no. 24, 4679, 2021. .
40. I. Matloob, S. A. Khan, R. Rukaiya, M. A. K. Khattak and A. Munir, "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems", IEEE Access, vol. 10