مطالعات علوم کاربردی در مهندسی

Online ISSN: ٢٤٧٦-٤٥٠٧

دوره ۱۱، شماره ۱، بهار ۱۴۰۴

Print ISSN: ٢٥٣٨-٢٠٥٥

صفحات ۱۰۰-۹۱

www.irijournals.com

طراحی و پیاده‌سازی سیستم‌های امنیتی مبتنی بر بلاکچین برای شبکه‌های کامپیوتری

رضا دانش

دانشجوی دکتری رشته مهندسی برق گرایش مخابرات سیستم، دانشکده رایانه، شبکه و ارتباطات، دانشگاه جامع امام حسین (ع)، تهران، ایران

چکیده

با گسترش روزافزون حملات سایبری و نقض امنیت داده‌ها در شبکه‌های کامپیوتری، نیاز به سیستم‌های امنیتی غیرمتمرکز و مقاوم در برابر دستکاری بیش از پیش احساس می‌شود. فناوری بلاکچین با ویژگی‌های منحصربه‌فردی مانند تغییرناپذیری، شفافیت و اجماع غیرمتمرکز، می‌تواند به عنوان یک راهکار مؤثر برای بهبود امنیت شبکه‌ها مورد استفاده قرار گیرد. این مقاله به بررسی طراحی و پیاده‌سازی سیستم‌های امنیتی مبتنی بر بلاکچین برای شبکه‌های کامپیوتری می‌پردازد. در این راستا، مزایا، چالش‌ها و کاربردهای بلاکچین در امنیت شبکه تحلیل شده و نمونه‌هایی از پیاده‌سازی‌های عملی ارائه می‌شود. نتایج نشان می‌دهد که استفاده از بلاکچین می‌تواند امنیت، اعتماد و پاسخگویی را در شبکه‌های کامپیوتری به‌طور قابل‌توجهی افزایش دهد.

واژه‌های کلیدی: بلاکچین، امنیت شبکه، سیستم‌های غیرمتمرکز، تغییرناپذیری، اجماع توزیع‌شده

۱. مقدمه

امنیت شبکه‌های کامپیوتری همواره یکی از چالش‌های اصلی در دنیای فناوری اطلاعات بوده است. با افزایش حملات سایبری مانند حملات DDoS، نفوذ به سیستم‌ها و سرقت داده‌ها، نیاز به راهکارهای امنیتی نوین و مقاوم در برابر تهدیدات بیشتر شده است. سیستم‌های متمرکز سنتی به دلیل وجود نقطه شکست واحد (Single Point of Failure) آسیب‌پذیر هستند و ممکن است توسط مهاجمان مورد سوءاستفاده قرار گیرند. به همین دلیل، متخصصان امنیتی به دنبال راه‌حل‌های غیرمتمرکز و توزیع‌شده هستند که نه‌تنها بتوانند از اطلاعات محافظت کنند، بلکه به افزایش اعتماد در زیرساخت‌های دیجیتال نیز کمک کنند. یکی از این راهکارها، استفاده از فناوری بلاک‌چین است که به دلیل ساختار غیرقابل تغییر و شفاف خود، می‌تواند به عنوان یک سپر مؤثر در برابر تهدیدات سایبری عمل کند. بلاک‌چین به کاربران این امکان را می‌دهد که اطلاعات را بدون نیاز به واسطه‌های مرکزی ذخیره و مدیریت کنند، که خود این ویژگی به کاهش ریسک‌های مرتبط با حملات کمک شایانی می‌کند.[1,2]

علاوه بر این، هوش مصنوعی و یادگیری ماشین نیز به عنوان ابزارهای قدرتمند در شناسایی تهدیدات و الگوهای غیرعادی در ترافیک شبکه به کار گرفته می‌شوند. این فناوری‌ها قادرند تا با تحلیل داده‌های بزرگ و شناسایی رفتارهای مشکوک، به سرعت به حملات پاسخ دهند و سیستم‌ها را در برابر نفوذها ایمن سازند. در نتیجه، سازمان‌ها می‌توانند با بهره‌گیری از این تکنولوژی‌های پیشرفته، پایداری و امنیت شبکه‌های خود را افزایش دهند. اما در کنار این پیشرفت‌ها، باید به نکته‌ای اساسی توجه داشت: آگاهی کاربران. آموزش و توانمندسازی افراد در خصوص تهدیدات سایبری و نحوه مقابله با آن‌ها، به عنوان یک عنصر کلیدی در امنیت شبکه‌ها به شمار می‌آید. سازمان‌ها باید فرهنگ امنیتی را در میان کارکنان خود ترویج دهند و آن‌ها را در جریان آخرین روش‌های محافظت از داده‌ها قرار دهند.[3,4]

در نهایت، امنیت شبکه‌های کامپیوتری نه تنها به فناوری‌های پیشرفته وابسته است، بلکه به یک رویکرد همه‌جانبه و متعادل نیاز دارد. ترکیب تکنولوژی‌های نوین، فرایندهای مدیریتی مؤثر و آموزش مداوم به کاربران می‌تواند به ایجاد یک محیط دیجیتال امن‌تر و پایدارتر کمک کند. در این دنیای پیچیده و در حال تغییر، تنها با همکاری و نوآوری می‌توان بر چالش‌های امنیتی غلبه کرد و آینده‌ای روشن‌تر را برای فناوری اطلاعات رقم زد. فناوری بلاکچین به‌عنوان یک سیستم غیرمتمرکز و توزیع‌شده، می‌تواند بسیاری از مشکلات امنیتی موجود را حل کند. ویژگی‌هایی مانند تغییرناپذیری داده‌ها، استفاده از الگوریتم‌های اجماع ایمن و حذف نیاز به واسطه‌های قابل اعتماد، بلاکچین را به گزینه‌ای ایده‌آل برای طراحی سیستم‌های امنیتی تبدیل کرده است[5,6]. در این مقاله، به بررسی نحوه طراحی و پیاده‌سازی چنین سیستم‌هایی پرداخته می‌شود.

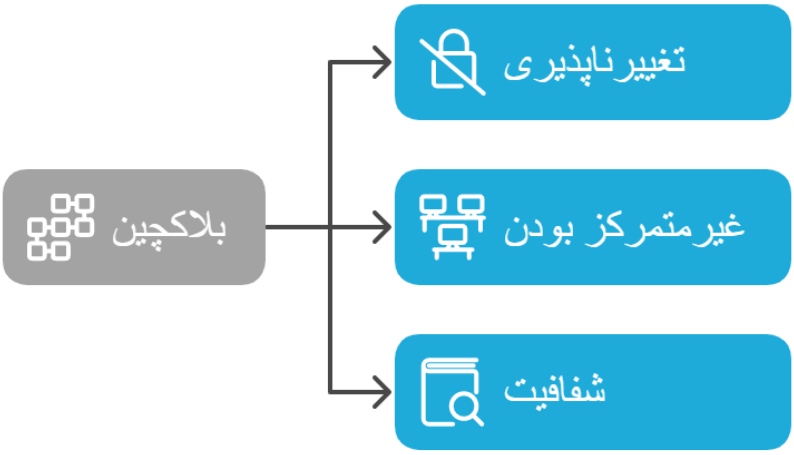
۲. مفاهیم تحقیق

۲.۱. فناوری بلاکچین

بلاکچین یک دفتر کل توزیع‌شده است که در آن تراکنش‌ها به‌صورت بلوک‌های رمزنگاری‌شده ذخیره می‌شوند. این فناوری از سه ویژگی اصلی برخوردار است:

- تغییرناپذیری: داده‌های ثبت‌شده پس از تأیید، غیرقابل تغییر هستند.
- غیرمتمرکز بودن: هیچ نهاد مرکزی کنترل شبکه را در اختیار ندارد.

- شفافیت: تمام تراکنش‌ها برای اعضای شبکه قابل مشاهده است.



شکل ۱: ویژگی‌های اصلی بلاکچین

۲.۲. امنیت شبکه‌های کامپیوتری

امنیت شبکه شامل مجموعه‌ای از سیاست‌ها و فناوری‌ها برای محافظت از زیرساخت‌های شبکه در برابر حملات سایبری است. برخی از چالش‌های امنیتی رایج عبارتند از:

- حملات انکار سرویس (DDoS)

حملات انکار سرویس توزیع‌شده (DDoS) یکی از تهدیدات جدی در دنیای فناوری اطلاعات به شمار می‌روند که به‌طور هدفمند به دنبال مختل کردن دسترسی کاربران به منابع آنلاین هستند. در این نوع حملات، مهاجمان با استفاده از شبکه‌ای از دستگاه‌های آلوده، به‌طور هم‌زمان به یک سرور یا وب‌سایت حمله می‌کنند و با ارسال حجم بالایی از درخواست‌ها، تلاش می‌کنند تا منابع آن را اشباع کنند. این اقدام نه تنها باعث کندی عملکرد سیستم می‌شود، بلکه ممکن است باعث از کار افتادن کامل سرویس نیز گردد. با افزایش وابستگی کسب‌وکارها به فضای مجازی، این نوع حملات به یک چالش بزرگ برای امنیت سایبری تبدیل شده‌اند.[7]

مقابله با حملات DDoS نیازمند استراتژی‌های پیچیده و چندلایه است که شامل نظارت مستمر بر ترافیک شبکه، استفاده از فایروال‌های پیشرفته و به‌کارگیری خدمات ابری برای توزیع بار ترافیکی می‌باشد. شرکت‌ها باید درک عمیقی از نقاط ضعف خود داشته باشند و با اتخاذ تدابیر مناسب، از خود در برابر این تهدیدات محافظت کنند. در دنیای دیجیتال امروزی که هر روزه بر تعداد و پیچیدگی این حملات افزوده می‌شود، آگاهی و آمادگی در برابر چنین خطراتی برای هر سازمانی امری ضروری است.[8]

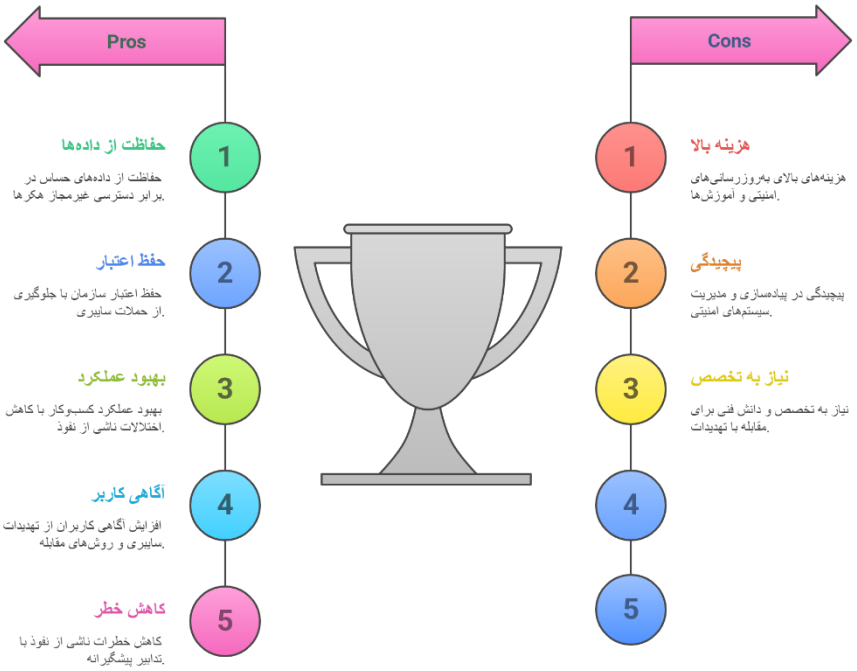
- جعل هویت (Spoofing)

جعل هویت، پدیده‌ای پیچیده و نگران‌کننده است که در دنیای دیجیتال امروز به طور فزاینده‌ای شایع شده است. این عمل به فرد یا گروهی اجازه می‌دهد تا خود را به جای فرد دیگری معرفی کند و از این طریق به اطلاعات حساس یا منابع مالی دسترسی پیدا کند. جعل هویت می‌تواند به اشکال مختلفی بروز کند، از جمله ایمیل‌های فیشینگ، تماس‌های تلفنی تقلبی و حتی ایجاد حساب‌های کاربری جعلی در شبکه‌های اجتماعی. این نوع سوءاستفاده نه تنها موجب از بین رفتن اعتماد عمومی می‌شود، بلکه خطرات جدی برای امنیت سایبری و حریم خصوصی افراد نیز به همراه دارد.[9]

در واکنش به این تهدیدات، بسیاری از سازمان‌ها و نهادها تدابیر امنیتی متعددی را به منظور شناسایی و مقابله با جعل هویت به کار گرفته‌اند. فناوری‌های پیشرفته‌ای چون احراز هویت چندعاملی و نرم‌افزارهای تشخیص تقلب به کمک کاربران می‌آیند تا از وقوع چنین جرائمی جلوگیری کنند. با این حال، آگاهی عمومی نیز نقش مهمی در کاهش این نوع تهدیدات دارد. آموزش کاربران در مورد نشانه‌های جعل هویت و ترفندهای رایج می‌تواند به آن‌ها کمک کند تا در برابر این خطرات هوشیارتر باشند و از خود و اطلاعاتشان بهتر محافظت کنند.[10]

- نفوذ به سیستم‌ها (Intrusion)

نفوذ به سیستم‌ها یکی از چالش‌های پیچیده در دنیای فناوری اطلاعات به شمار می‌آید. هکرها و مجرمان سایبری با استفاده از تکنیک‌های متنوع و نوآورانه به دنبال دسترسی غیرمجاز به اطلاعات حساس و منابع دیجیتال هستند. آنها ممکن است از روش‌هایی چون فیشینگ، بدافزار یا بهره‌برداری از آسیب‌پذیری‌های نرم‌افزاری استفاده کنند تا بتوانند به شبکه‌های سازمان‌ها نفوذ کنند. این اقدام نه تنها تهدیدی جدی برای امنیت داده‌ها محسوب می‌شود، بلکه می‌تواند به اعتبار و عملکرد کسب‌وکارها آسیب بزند.[11]



شکل ۲: امنیت سایبری

به همین دلیل، سازمان‌ها باید به طور مداوم به روزرسانی‌های امنیتی و آموزش‌های لازم را برای کارکنان خود فراهم کنند. اتخاذ تدابیر پیشگیرانه همچون سیستم‌های تشخیص نفوذ و مدیریت آسیب‌پذیری می‌تواند به کاهش خطرات کمک کند. در عین حال، فرهنگ‌سازی در زمینه امنیت سایبری و آگاهی از تهدیدات ممکن، به کاربران این امکان را می‌دهد که در برابر حملات احتمالی هوشیار باشند. در دنیای دیجیتال امروز، نیاز به یک رویکرد جامع و استراتژیک برای مقابله با نفوذ به سیستم‌ها نه تنها حیاتی است، بلکه به عنوان یک ضرورت انکارناپذیر به شمار می‌آید.[12]

۲.۳. کاربرد بلاکچین در امنیت شبکه

- مدیریت هویت غیرمتمرکز: استفاده از بلاکچین برای احراز هویت کاربران بدون نیاز به مرجع مرکزی.

مدیریت هویت غیرمتمرکز به عنوان یک راهکار نوین در دنیای دیجیتال، امکان احراز هویت کاربران را بدون نیاز به مرجع مرکزی فراهم می‌کند. در این سیستم، بلاکچین به عنوان بستری امن و غیرقابل تغییر عمل می‌کند که اطلاعات هویتی را به صورت رمزنگاری شده ذخیره می‌سازد. این رویکرد به کاربران این امکان را می‌دهد که کنترل کاملی بر داده‌های خود داشته باشند و بدون وابستگی به نهادهای ثالث، هویت خود را مدیریت کنند. به این ترتیب، خطرات ناشی از نقض داده‌ها و سوءاستفاده‌های احتمالی به شدت کاهش می‌یابد و اعتماد بیشتری میان کاربران و سرویس‌دهندگان ایجاد می‌شود.[13]

علاوه بر این، هویت‌های غیرمتمرکز به کاربران اجازه می‌دهند تا با استفاده از کلیدهای خصوصی، به طور ایمن و مستقیم به خدمات مختلف دسترسی پیدا کنند. این فرآیند نه تنها سرعت احراز هویت را افزایش می‌دهد، بلکه هزینه‌های مرتبط با مدیریت هویت را نیز به حداقل می‌رساند. به عنوان مثال، کاربران می‌توانند با استفاده از هویت دیجیتال خود، به راحتی در پلتفرم‌های مختلف ثبت‌نام کرده و از خدمات گوناگون بهره‌مند شوند، بدون اینکه نیازی به ایجاد حساب‌های متعدد و ارائه اطلاعات شخصی مکرر داشته باشند. این نوآوری، افق‌های جدیدی را برای تعاملات دیجیتال باز می‌کند و به سمت آینده‌ای امن‌تر و شفاف‌تر هدایت می‌کند.[14]

- ثبت امن رویدادهای شبکه: ذخیره‌سازی لاگ‌های امنیتی در بلاکچین برای جلوگیری از دستکاری.

در دنیای دیجیتال امروز، ثبت امن رویدادهای شبکه به یکی از نیازهای اساسی سازمان‌ها تبدیل شده است. استفاده از بلاکچین برای ذخیره‌سازی لاگ‌های امنیتی، روشی نوآورانه برای جلوگیری از دستکاری و تغییر اطلاعات است. با بهره‌گیری از این فناوری، هر رویداد به صورت غیرقابل تغییر در زنجیره‌ای از بلوک‌ها ثبت می‌شود. این امر موجب می‌گردد که هرگونه تلاش برای تغییر یا حذف داده‌ها به راحتی قابل شناسایی باشد و در نهایت، سطح امنیت اطلاعات به طرز چشمگیری افزایش یابد.[15]

علاوه بر این، ذخیره‌سازی لاگ‌ها در بلاکچین به سازمان‌ها این امکان را می‌دهد که به طور همزمان به شفافیت و قابلیت ردیابی دست یابند. با هر بار ورود یک رویداد جدید، اطلاعات به صورت خودکار در شبکه توزیع شده قرار می‌گیرد و کاربران مجاز می‌توانند به سادگی به تاریخچه فعالیت‌ها دسترسی پیدا کنند. این روش نه تنها به کاهش خطرات ناشی از دستکاری داده‌ها کمک می‌کند، بلکه می‌تواند به عنوان ابزاری قدرتمند در تحلیل و مدیریت امنیت سایبری به کار گرفته شود. بدین ترتیب، سازمان‌ها می‌توانند با اعتماد به نفس بیشتر به فعالیت‌های خود ادامه دهند و تهدیدات آینده را بهتر مدیریت کنند.[16]

- حفاظت از داده‌های حساس: استفاده از قراردادهای هوشمند برای کنترل دسترسی به داده‌ها.

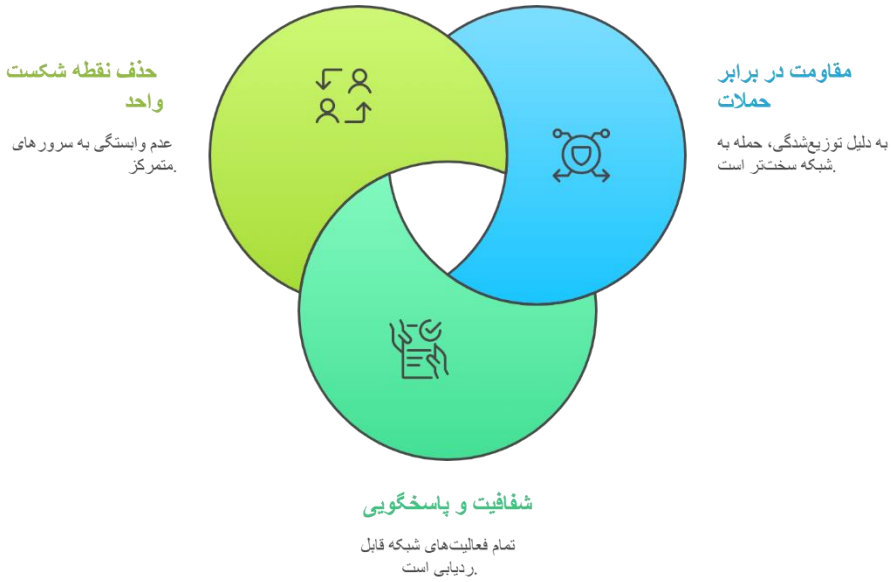
در دنیای دیجیتال امروز، حفاظت از داده‌های حساس به یکی از اولویت‌های اساسی سازمان‌ها تبدیل شده است. قراردادهای هوشمند، که بر بستر فناوری بلاک‌چین عمل می‌کنند، راهکاری نوآورانه برای کنترل و مدیریت دسترسی به اطلاعات حساس ارائه می‌دهند. این قراردادها با کدگذاری شرایط و قوانین دسترسی به داده‌ها، اطمینان حاصل می‌کنند که تنها افراد مجاز قادر به مشاهده یا تغییر اطلاعات هستند. به این ترتیب، شفافیت و قابلیت اعتماد در فرآیندهای مدیریت داده افزایش می‌یابد و خطرات ناشی از دسترسی غیرمجاز به حداقل می‌رسد.[17]

استفاده از قراردادهای هوشمند همچنین امکان پیگیری و ثبت دقیق تمامی فعالیت‌ها و تغییرات در داده‌ها را فراهم می‌کند. با این ویژگی، هرگونه تلاش برای نفوذ یا تغییر غیرمجاز به سرعت شناسایی و گزارش می‌شود. این سیستم نه تنها امنیت داده‌ها را تقویت می‌کند، بلکه به سازمان‌ها این امکان را می‌دهد که با رعایت قوانین و مقررات مربوط به حفاظت از اطلاعات، اعتبار و اعتماد بیشتری در میان مشتریان و ذینفعان خود به دست آورند. در نتیجه، قراردادهای هوشمند به عنوان ابزاری کارآمد در راستای حفاظت از داده‌های حساس و افزایش امنیت سایبری، نقش بسزایی ایفا می‌کنند.[18,19]

۳. بحث و بررسی

۳.۱. مزایای استفاده از بلاکچین در امنیت شبکه

- مقاومت در برابر حملات: به دلیل توزیع‌شدگی، حمله به شبکه سخت‌تر است.
- شفافیت و پاسخگویی: تمام فعالیت‌های شبکه قابل ردیابی است.
- حذف نقطه شکست واحد: عدم وابستگی به سرورهای متمرکز.



شکل ۳: مزایای بلاکچین در امنیت شبکه

مقاومت در برابر حملات یکی از ویژگی‌های اساسی شبکه‌های توزیع‌شده است. به دلیل ساختار غیرمتمرکز این شبکه‌ها، حمله به یک نقطه خاص به سادگی امکان‌پذیر نیست. هر گره در این سیستم می‌تواند به عنوان یک دفاع عمل کند و به همین دلیل، نفوذ به کل شبکه دشوار می‌شود. این ویژگی به کاربران اطمینان می‌دهد که حتی در صورت بروز حمله، عملکرد کلی شبکه تحت تأثیر قرار نخواهد گرفت و سیستم به فعالیت خود ادامه خواهد داد.

شفافیت و پاسخگویی از دیگر مزایای کلیدی شبکه‌های توزیع‌شده به شمار می‌رود. تمامی فعالیت‌ها و تراکنش‌ها در این سیستم‌ها به‌طور کامل قابل ردیابی هستند، که این امر به کاربران اجازه می‌دهد تا هرگونه تغییر را به‌راحتی پیگیری کنند. همچنین، حذف نقاط شکست واحد به امنیت و پایداری شبکه کمک می‌کند. این عدم وابستگی به سرورهای متمرکز، خطراتی مانند از دست رفتن اطلاعات یا خرابکاری را به حداقل می‌رساند و به کاربران این امکان را می‌دهد که با اطمینان بیشتری از خدمات شبکه استفاده کنند.

۳.۲. چالش‌های پیاده‌سازی

- مقیاس‌پذیری: برخی بلاکچین‌ها در پردازش تراکنش‌های انبوه کند عمل می‌کنند.
- مصرف انرژی: الگوریتم‌های اجماع مانند اثبات کار (PoW) انرژی زیادی مصرف می‌کنند.
- پیچیدگی فنی: نیاز به تخصص بالا برای طراحی و استقرار سیستم‌های بلاکچینی.

مقیاس‌پذیری یکی از چالش‌های اساسی در دنیای بلاکچین است. برخی از بلاکچین‌ها، به دلیل محدودیت‌های فنی و ساختاری، در پردازش تراکنش‌های انبوه با کندی مواجه می‌شوند. این کندی می‌تواند به علت طراحی‌های ناکارآمد یا ظرفیت پایین شبکه باشد، که به نوبه خود مانع از پذیرش گسترده تکنولوژی‌های بلاکچینی در کاربردهای تجاری و مالی می‌شود. در دنیای رو به رشد فناوری، نیاز به راه‌حل‌هایی که بتوانند تراکنش‌های بیشتری را در زمان کمتر پردازش کنند، بیش از پیش احساس می‌شود.

از سوی دیگر، مصرف انرژی یکی دیگر از معضلات مهم بلاکچین‌هاست. الگوریتم‌های اجماع مانند اثبات کار (PoW) به شدت انرژی‌بر هستند و این مسئله نگرانی‌های زیست‌محیطی را به همراه دارد. با توجه به افزایش تعداد ماینرها و رقابت برای استخراج بلاک‌ها، مصرف انرژی به طور قابل توجهی افزایش می‌یابد. علاوه بر این، پیاده‌سازی و طراحی سیستم‌های بلاکچینی نیازمند تخصص و دانش فنی بالاست که بسیاری از کسب‌وکارها به راحتی نمی‌توانند به آن دسترسی پیدا کنند. این پیچیدگی فنی ممکن است مانع از نوآوری و توسعه در این حوزه شود.

۳.۳. نمونه‌های عملی

- GuardTime:یک سیستم امنیتی مبتنی بر بلاکچین برای محافظت از داده‌های دولتی.
- IBM Blockchain:استفاده از بلاکچین برای بهبود امنیت شبکه‌های سازمانی.

GuardTimeیک سیستم نوآورانه امنیتی است که با بهره‌گیری از فناوری بلاکچین، به محافظت از داده‌های دولتی می‌پردازد. این پلتفرم با استفاده از الگوریتم‌های رمزنگاری پیشرفته، امکان ردیابی و تأیید صحت اطلاعات را فراهم می‌آورد. GuardTimeبا ایجاد یک لایه امنیتی غیرمتمرکز، از هرگونه دستکاری و نفوذ غیرمجاز به داده‌ها جلوگیری می‌کند و بدین ترتیب، اعتماد عمومی به اطلاعات دولتی را افزایش می‌دهد. این سیستم به سازمان‌ها کمک می‌کند تا با اطمینان بیشتری در دنیای دیجیتال عمل کنند و امنیت ملی را در برابر تهدیدات سایبری تقویت نمایند.

از سوی دیگر، IBM Blockchainبه عنوان یک راهکار پیشرفته، به بهبود امنیت شبکه‌های سازمانی پرداخته و با استفاده از تکنولوژی بلاکچین، شفافیت و قابلیت اعتماد را در تراکنش‌ها افزایش می‌دهد. این سیستم به کسب‌وکارها امکان می‌دهد تا به آسانی اطلاعات را با یکدیگر به اشتراک بگذارند، در حالی که هرگونه تغییر در داده‌ها به سادگی قابل ردیابی است. با این رویکرد، IBM Blockchainنه تنها به کارایی فرآیندها کمک می‌کند بلکه به کاهش ریسک‌های امنیتی و افزایش تعاملات تجاری میان سازمان‌ها نیز می‌انجامد.

۴. پیشنهادات

- استفاده از الگوریتم‌های اجماع کارآمد: مانند اثبات سهام (PoS) برای کاهش مصرف انرژی.
- ترکیب بلاکچین با یادگیری ماشین: برای تشخیص خودکار حملات سایبری.
- بهبود مقیاس‌پذیری: با استفاده از راهکارهایی مانند شاردینگ(Sharding) .

۵. نتیجه‌گیری

سیستم‌های امنیتی مبتنی بر بلاکچین می‌توانند تحول عظیمی در امنیت شبکه‌های کامپیوتری ایجاد کنند. با وجود چالش‌هایی مانند مقیاس‌پذیری و مصرف انرژی، مزایای این فناوری از جمله غیرمتمرکز بودن، تغییرناپذیری و شفافیت، آن را به یک راهکار امیدوارکننده تبدیل کرده است. با توسعه فناوری‌های مکمل و تحقیقات بیشتر، می‌توان سیستم‌های امنیتی کارآمدتری مبتنی بر بلاکچین طراحی و پیاده‌سازی کرد. از جمله ویژگی‌های بارز سیستم‌های امنیتی بر پایه بلاکچین، قابلیت ایجاد زنجیره‌ای از داده‌های غیرقابل تغییر است که به کاربران امکان می‌دهد به راحتی و با اطمینان به تاریخچه فعالیت‌ها و تراکنش‌ها دسترسی پیدا کنند. این ویژگی، انقلابی در مدیریت هویت دیجیتال فراهم می‌آورد و به سازمان‌ها کمک می‌کند تا هویت کاربران را به صورت ایمن و بدون واسطه تأیید کنند.

علاوه بر این، پروتکل‌های رمزنگاری پیشرفته که در این فناوری به کار می‌روند، سطح بالایی از امنیت را فراهم می‌کنند. با استفاده از الگوریتم‌های پیچیده، هرگونه دستکاری در داده‌ها به سادگی شناسایی می‌شود و این امر موجب افزایش اعتماد در بین کاربران و سازمان‌ها می‌گردد. به عنوان مثال، در صنایع مالی، این تکنولوژی می‌تواند به کاهش تقلب و سوءاستفاده‌های مالی کمک شایانی کند. در کنار این مزایا، قابلیت هم‌افزایی با فناوری‌های نوظهور نیز یکی از نقاط قوت بلاکچین محسوب می‌شود. با ادغام سیستم‌های مبتنی بر هوش مصنوعی و اینترنت اشیا با بلاکچین، می‌توان به راهکارهای نوآورانه‌ای دست یافت که به بهینه‌سازی فرآیندها و افزایش امنیت در شبکه‌های مختلف کمک می‌کند. به عنوان نمونه، در صنعت حمل و نقل، ردیابی دقیق محموله‌ها و اطمینان از صحت اطلاعات به اشتراک‌گذاری شده می‌تواند از طریق این فناوری تسهیل شود. با این حال، برای رسیدن به پتانسیل کامل این سیستم‌ها، نیاز به همکاری بین‌المللی و ایجاد استانداردهای جهانی وجود دارد. تحقیقات مستمر در زمینه کاهش مصرف انرژی و افزایش مقیاس‌پذیری می‌تواند به پذیرش گسترده‌تر این فناوری منجر شود. در نهایت، با توجه به تحولات سریع در دنیای دیجیتال، استفاده از سیستم‌های امنیتی مبتنی بر بلاکچین می‌تواند یکی از ارکان اصلی ایجاد زیرساخت‌های امن و پایدار در آینده باشد.

منابع:

1. Swapnil, B.; Erlend, A.; Hans-Henrik, H. Tools and practices for tactical delivery date setting in engineer-to-order environments: A systematic literature review. Int. J. Prod. Res. 2022, 1–33.
2. McKendry, D.A.; Whitfield, R.I.; Duffy, A.H. Product Lifecycle Management implementation for high value Engineering to Order programmes: An informational perspective. J. Ind. Inf. Integr. 2022, 26, 100264.
3. Cocca, P.; Schiuma, G.; Viscardi, M.; Floreani, F. Knowledge management system requirements to support Engineering-To-Order manufacturing of SMEs. Knowl. Manag. Res. Pract. 2021, 1–14.
4. Thajudeen, S.; Elgh, F.; Lennartsson, M. Supporting the Reuse of Design Assets in ETO-Based Components—A Case Study from an Industrialised Post and Beam Building System. Buildings 2022, 12, 70.
5. Shahbazi, Z.; Byun, Y.C. Smart manufacturing real-time analysis based on blockchain and machine learning approaches. Appl. Sci. 2021, 11, 3535.
6. Lim, M.K.; Li, Y.; Wang, C.; Mltd, E. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. Comput. Ind. Eng. 2021, 154, 107133.
7. Zhai, P.; He, J.; Zhu, N. Blockchain-Based Internet of Things Access Control Technology in Intelligent Manufacturing. Appl. Sci. 2022, 12, 3692.
8. Manogaran, G.; Alazab, M.; Shakeel, P.M.; Hsu, C.H. Blockchain assisted secure data sharing model for Internet of Things based smart industries. IEEE Trans. Reliab. 2021, 71, 348–358.
9. Mohamed, N.; Al-Jaroodi, J. Applying blockchain in industry 4.0 applications. In Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 7–9 January 2019; pp. 852–858.
10. Cao, Y.; Jia, F.; Manogaran, G. Efficient Traceability Systems of Steel Products Using Blockchain-Based Industrial Internet of Things. IEEE Trans. Ind. Inform. 2020, 16, 6004–6012.
11. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 839–858.
12. Leng, J.; Zhou, M.; Zhao, J.L.; Huang, Y.; Bian, Y. Blockchain security: A survey of techniques and research directions. IEEE Trans. Serv. Comput. 2020, 15, 2490–2510.
13. Bhushan, B.; Sinha, P.; Sagayam, K.M.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. Comput. Electr. Eng. 2021, 90, 106897.
14. Huang, H.; Kong, W.; Zhou, S.; Zheng, Z.; Guo, S. A Survey of State-of-the-Art on Blockchains: Theories, Modelings, and Tools. ACM Comput. Surv. 2022, 54, 44.1–44.42.
15. Das, S.; Mohanta, B.K.; Jena, D. A state-of-the-art security and attacks analysis in blockchain applications network. Int. J. Commun. Netw. Distrib. Syst. 2022, 28, 199–218.

16. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Trans. Syst. Man Cybern. Syst. 2019, 49, 2266–2277.
17. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.D.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
18. Yu, B.; Wright, J.; Nepal, S.; Zhu, L.; Liu, J.; Rajiv, R. IoTChain: Establishing trust in the Internet of Things ecosystem using blockchain. IEEE Cloud Comput. 2018, 5, 12–20.
19. Wan, J.; Li, J.; Imran, M.; Li, D.; E-Amin, F. A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans. Ind. Inform. 2019, 15, 3652–3660.