ارایه یک رویکرد جدید برای ارسال و ذخیره کردن اطلاعات در اینترنت اشیا جهت استفاده در خانه های هوشمند

ابراهیم طالبی برام [۱]: دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، مؤسسه آموزش عالی کارون، اهواز، ایران

دکتر محمدرضا محمدرضائی[۲]:استادیار، گروه مهندسی کامپیوتر، مؤسسه آموزش عالی کارون، اهواز، ایران

چکیده

با گسترش اینترنت استفاده از دستگاه هایی که به اینترنت مجهز هستند در خانه ها افزایش پیدا کرد به طوری که این دستگاه ها اطلاعات محیط را با کمک حسگرهای خود دریافت می کردند و بعد از پردازش رویدادی در محیط اجرا می شد و یا تصمیمی اتخاذ می شد که باعث به وجود آمدن خانه های هوشمند شد. اما از آنجا که این حسگرها به داده های شخصی افراد دسترسی داشتند حریم خصوصی کاربران به خطر می افتاد. بنابراین روش های مختلفی برای ایجاد امنیت در این شبکه ها ارائه شده است. خیلی از این روش های ارائه شده بر پای رمزنگاری سنتی هستند اما این روش ها در محیط های توزیع شده ای مثل اینترنت اشیا کارایی ندارند. بنابراین در این پژوهش به ارائه ی راهکاری بر پایه ی هولوچین خواهیم پرداخت تا امنیت داده ها و حریم خصوصی کاربران را در شبکه های اینترنت اشیا حفظ کند.

کلیدواژه‌ها: ارسال، ذخیره کردن ،اطلاعات، اینترنت اشیا، خانه های هوشمند.

[۱] - دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، مؤسسه آموزش عالی کارون، اهواز، ایران

[۲] – دکتر محمدرضا محمدرضائی[۲]:استادیار، گروه مهندسی کامپیوتر، مؤسسه آموزش عالی کارون، اهواز، ایران

۱. مقدمه و بیان مسئله:

اینترنت اشیا که به آن IoT نیز می گویند جز شبکه هایی است که روز به روز افزایش پیدا کرده و دامنه ی کاربرد آن زیاد و زیادتر شده است. این شبکه ها از تعدادی شی یا "چیز" تشکیل شده اند که هر کدام به حسگرهایی مجهز هستند و این حسگرها باید داده های محیط را حس کرده و جمع آوری کنند [۱]، [۲]. این حسگرها داده ها را از محیط جمع آوری می کنند، با توجه به کاربرد شبکه امکان دارد برخی پردازش های محلی انجام دهند و یا داده های خام را به سمت سرور ارسال کنند و در آنجا پردازش ها انجام شود و تصمیمات اتخاذ شود. با افزایش و پیشرفت شبکه هایی که دارای اجزای ناهمگن هستند، کاربردهای اینترنت اشیا نیز افزایش پیدا کرد به عنوان مثال کاربردهای اینترنت اشیا عبارتند از : مراقبت‌های بهداشتی هوشمند، خانه‌های هوشمند، شهرهای هوشمند، کشاورزی، آموزش، صنایع غذایی و بسیاری موارد دیگر. حسگرهای موجود در شبکه های اینترنت اشیا، داده ها را جمع آوری کرده و با توجه به رسانه ی انتقالی که به ان مجهز هستند داده های جمع آوری شده را به ابر ارسال می کنند تا در آنجا پردازش های سنگین تر اجرا شود. رسانه ی ارتباطی برای اتصال همزمان اشیاء ناهمگن به منظور ارائه خدمات دیجیتال خاص استفاده می شود که می توان به عنوان مثال به WiFi [3]، بلوتوث [4]، Zigbee [3,5]، MQTT[6]، ۸۰۲.۱۵.۴IEEE، OPC-UA، NFC، Z-wave، LoRaWAN [7]، SigFox و LTE-Advanced اشاره کرد. یکی از مشکلاتی که در این شبکه ها وجود دارد ارتباط امن و حفظ حریم خصوصی داده های جمع آوری شده است. در زمانی که داده ها جمع آوری می شوند و یا رد و بدل می شوند باید از یک سری قوانین پیروی کنند تا حریم خصوصی داده ها حفظ شود. یکی از راه حل های برقراری امنیت بهبود مدیریت کلید برای رمزنگاری داده ها [9،8] و بهبود عملکرد غیرقابل کلون سازی فیزیکی [10] است. یکی از راه حل های برقراری امنیت در اینترنت اشیا استفاده از بلاکچین است که در این مدل تمام تراکنش های کاربر به شکل یک زنجیره به دنبال هم ذخیره می شوند. اما در بلاکچین هایی که دارای زنجیره های طولانی هستند نیاز به مقدار بیشتری فضا برای ذخیره سازی داریم که این مورد خود چالشی برای شبکه های اینترنت اشیا محسوب می شود. مشکل دیگری که استفاده از بلاکچین با زنجیره های طولانی برای شبکه ایجاد می کند این است که این زنجیره های طولانی پهنای باند بیشتری را نیاز دارند تا داده ها را به اشتراک بگذارند که این مساله خود باعث کاهش امنیت می شود. این چالش با نیاز به انرژی محاسباتی اضافی برای استخراج و الگوریتم‌های اجماع تشدید می‌شود [۱۱]. در زمانی که در بلاکچین عمل اعتبار سنجی یک تراکنش انجام می شود تمام گره های موجود در بلاکچین باید عمل استخراج را انجام دهند و اولین گره ای که در عمل ماینینگ موفق شده باشد می تواند اعتبارسنجی تراکنش را انجام دهد. همین امر باعث افزایش بار محاسباتی می شود که خود یک مساله و چالش برای شبکه های اینترنت اشیا است. از این رو، بلاک چین باعث افزایش هزینه های محاسباتی اضافی برای سیستم های اینترنت اشی با محدودیت منابع می شود. بنابراین، یک راه حل عملی برای سیستم های اینترنت اشیا مورد نیاز است که بتواند بر این چالش غلبه کند. هولوچین یک فناوری نوظهور است که یک زیرساخت شبکه توزیع شده منبع باز را برای برقراری ارتباط ایمن بدون به ارث بردن نیازهای ذخیره سازی عظیم و تبادل داده مانند بلاک چین فراهم می کند [12]. هولوچین این کار را با ترکیب دو تکنیک انجام می دهد: (۱) جدول هش توزیع شده (DHT) و (۲) زنجیره هش. DHT بر مسائل انتشار داده ها متمرکز است و

زنجیره های هش برای حفظ یکپارچگی داده ها ساخته شده اند. DHT را می توان در شبکه های IoT برای ذخیره زنجیره داده های انتقال در هر گره جداگانه پیاده سازی و استفاده کرد تا از ماهیت مستقل یک شبکه مبتنی بر هولوچین اطمینان حاصل شود. برای به اشتراک گذاری داده ها در شبکه و ارائه یک چارچوب توزیع واقعی می توان از DHT استفاده کرد. یکی از مزایای ذخیره سازی داده ها در DHT این است که شبکه مانند شبکه هایی که مبتنی بر بلاک چین هستند شلوغ نمی شود. DHT موجود در هولوچین به شبکه اجازه می دهد تا مقیاس پذیر را در شبکه فراهم کند. بنابراین، تمام این مزیت ها هولوچین را به یک انتخاب مناسب برای سیستم‌های اینترنت اشیا تبدیل می‌کند. در این پژوهش، یک مدل اینترنت اشیاء مبتنی بر هولوچین را پیشنهاد می‌کنیم که چالش‌های امنیتی و حریم خصوصی را کاهش می‌دهد و جایگزینی با پیچیدگی پایین و بسیار امن برای بلاک چین ارائه می‌دهد.

سؤالات پژوهش

- **سوال اول پژوهش)** تا چه اندازه وجود یک محیط توزیع شده می تواند به امنیت داده و تایید صحت داده ها کمک کند؟
- **سوال دوم پژوهش)** چه مقدار استفاده از روش های فشرده سازی و هش می تواند بار محاسباتی را در شبکه های با محدودیت منابع، کاهش دهد؟
- **سوال اول پژوهش)** برتری روش ارائه شده مبتنی بر هولوچین نسبت به روش های انجام شده مبتنی بر بلاکچین چقدر است؟

۲. مبانی نظری

همانطور که در فصل قبل تعریفی از اینترنت اشیا داشتیم، اینترنت اشیا تکنولوژی جدید است که دستگاه های هوشمند که دارای حسگر هستند را قادر می سازد که با استفاده از شبکه های ارتباطی مثل اینترنت و یا اینترانت با هم در ارتباط باشند و داده های حس شده از محیط را برای یکدیگر و یا برای یک سیستم مرکزی ارسال کنند. از این تکنولوژی می توانیم در کاربردهایی مثل نظارت های امنیتی و یا کشاورزی و یا حتی در مراقبت های بهداشتی و درمانی استفاده کنیم.[۶]. همین‌طور واضح است که اینترنت اشیاء شامل تعداد بسیار زیادی از دستگاه‌ها که به اینترنت وصل می‌شوند، خواهد شد. دولت انگلیس در حرکتی فعال برای انطباق تکنولوژی‌های جدید و نوظهور میلیون ۴۰ پوند را در بودجه‌شان در سال ۲۰۱۵ به تحقیق درباره اینترنت اشیاء داده شد. به عقیده جرج آزبرن، رئیس خزانه سابق انگلیس، با توجه به اتصال همه چیز از جمله وسایل حمل و نقل شهری و دستگاه‌های پزشکی و لوازم خانگی به اینترنت، اینترنت اشیاء گام بعدی انقلاب اطلاعات است[۷]. اینترنت اشیاء با قابلیت جاسازی سی‌پی‌یو و حافظه و منابع انرژی قادر به اتصال تقریباً همه چیز به شبکه با استفاده از برنامه‌ها می باشد. این سیستم‌ها موظف به گردآوری اطلاعات، تنظیمات اکوسیستم‌های طبیعی و حتی ساختمان‌ها و کارخانه‌ها هستند. هم چنین کاربردهایی را در زمینه‌های رصد محیط زیست و برنامه‌ریزی شهری می‌توان پیدا کرد [۸]. از طرف دیگر، سیستم‌های اینترنت اشیاء همچنین می‌توانند برای اجرای فعالیت پاسخگو باشند. به عنوان مثال سیستم‌های خرید هوشمند می‌توانند عادات خرید کاربران در یک فروشگاه را توسط تلفن همراه‌شان ردیابی کنند. به این کاربران در مورد کالاهای مورد علاقه‌شان یا حتی مکان اقلام مورد نیازشان، پیشنهادهای ویژه‌ای که توسط یخچالشان به گوشی آن‌ها منتقل شده‌است، می‌توانند ارائه کنند. نمونه‌های اضافی از سنجش و بیماری در برنامه‌هایی که با مدیریت گرما و آب و الکتریسیته و انرژی سر و کار دارند از جمله حالت کروز

در سامانه ترابری هوشمند منعکس می‌شوند. کاربرد دیگر اینترنت اشیاء ایجاد ویژگی‌های امنیتی خانه و اتوماسیون خانگی است به منظور توضیح شبکه سنسورهای بیولوژی، اینترنت اشیاء زنده مطرح شده‌است که قادر است با آنالیز ابری اطلاعات به کاربران اجازه مطالعه دی ان ای و دیگر مولکول‌ها را بدهد [۹].

در صنعت رسانه داده‌های بزرگ به دو طریق بررسی می‌شود:

۱. هدف قرار دادن مصرف‌کنندگان
۲. ضبط داده‌ها

اینترنت اشیا برای گرد آوری و تحلیل آمارهای رفتاری مختلف و روزافزون، فرصت بوجود می آورد. همبستگی این داده‌ها می‌تواند سبب دگرگونی بازاریابی هدفمند محصولات و خدمات شود. به عنوان مثال، همان‌طور که میدوز کلو اشاره کرده، ارقام ردیابی و تحلیل تغییرات با هدف قرار دادن رفتارها، سطح جدیدی از دقت را بوجود آورده است که تبلیغات بر روی دستگاه‌های مردم را امکان پذیر می کند. از نقطه نظر رسانه‌ها، داده کلیدی است که از اتصال دستگاه گرفته می شود، درحالی که اساساً افزایش دقت هدف قرار دادن را ممکن می‌سازد [۱۰] .

یک پروژه تحقیقاتی در سال ۲۰۲۱ نشان داد که خانه های هوشمند معمولی در برابر تعداد زیادی از حملات داده آسیب پذیر هستند.[۲] موارد گزارش‌شده از حملات خانه‌های هوشمند شامل کنترل از راه دور چراغ‌های هوشمند و تلویزیون‌های هوشمند توسط هکرها، باز کردن قفل درهای مجهز به اینترنت اشیا، و روشن کردن و پخش ویدئو از راه دور از دوربین‌های هوشمند توسط هکرها است.[۴] در یک نمونه، خانه ای از میلواکی تنها زمانی متوجه شد که پس از اینکه ترموستات آنها روی دمای بیش از ۳۰ درجه سانتیگراد برنامه ریزی شده بود، از خواب بیدار شدند [۵].

- دستگاه های ضعیف اینترنت اشیا

محققان در مجموع ۱۶ دستگاه خانگی هوشمند پرکاربرد را از طیف وسیعی از برندها آزمایش کردند و ۵۴ آسیب پذیری را یافتند که کاربران را در معرض حمله هکرها قرار می داد. پتانسیل این حملات از غیرفعال کردن سیستم‌های امنیتی تا سرقت داده‌های شخصی متغیر است.[۶] تخمین زده می شود که ۸۰ درصد از دستگاه های اینترنت اشیا در برابر طیف وسیعی از حملات آسیب پذیر هستند.[۷]

هولوچین

هولوچین یک فناوری نوظهور است که پتانسیل رفع ایرادات بلاک چین در فعال کردن شبکه های مراقبت بهداشتی IoT ایمن را دارد. هولوچین بر اساس یک زیرساخت شبکه توزیع شده منبع باز است که به طور ایمن بدون به ارث بردن نیازهای ذخیره سازی و تبادل داده عظیم یک بلاک چین ارتباط برقرار می کند. برای کاربردهای مبتنی بر اینترنت اشیا، پیاده‌سازی فناوری مصرف بالای منابع مانند بلاک چین ممکن است راه‌حلی غیرواقعی ایجاد کند. از این رو، این بخش به نشان دادن چگونگی برخورد هولوچین با محیط محدود منابع و ارائه راه حل های بهتر در مقابل بلاک چین برای تحقق سیستم های مراقبت بهداشتی IoT ایمن اختصاص یافته است.

الف. مقیاس پذیری بهتر

بلاک چین یک رویکرد امنیتی توزیع شده مبتنی بر داده است که در آن هدف اصلی ایجاد یک بلوک مشترک از داده ها در بین تمام کاربران مجاز در شبکه است. بنابراین اندازه داده ها با تعداد موجودیت های شبکه درگیر در هر تراکنش افزایش می یابد و مقیاس پذیر نیست [۲۹]. در مقابل، هر برنامه هولوچین (hApp) توسط یک عامل نگهداری می‌شود

که می‌تواند به طور مستقل در رمزگذاری داده‌ها شرکت کند، تراکنش را در یک زنجیره منبع منحصر به فرد شبکه هولوچین ذخیره کند و داده‌های مورد نیاز را با یک عامل همتا به اشتراک بگذارد. این رویکرد هولوچین عامل محور بسیار مقیاس پذیر است.

ب. کاهش ترافیک شبکه

از آنجایی که هولوچین ترکیبی از امضای دیجیتال و DHT است، می‌تواند جایگزین مؤثری برای بلاک چین برای بهبود عملکرد بازیابی اطلاعات از شبکه توزیع‌شده همتا به همتا (P۲P) باشد. هر عامل در یک شبکه هولوچین داده های فردی خود را به صورت محلی ذخیره می کند. در شبکه های اینترنت اشیا، بسیاری از دستگاه ها به دلیل محدودیت حافظه و قدرت محاسباتی، از مفاهیم بارگذاری، گره های مه یا ابرها برای ذخیره پایگاه داده خود استفاده می کنند. با این حال، هر عامل قادر است مقدار هش خود را محاسبه کند و بخش قابل توجهی را با سایر همتایان با استفاده از DHT به اشتراک بگذارد. در مقابل، همه همتایان یک شبکه بلاک چین یک کپی غیرقابل تشخیص از انتقال را ذخیره می کنند که به تبادل ارتباطی قابل توجهی بین گره ها نیاز دارد. علاوه بر این، پهنای باند اضافی برای هر موجودیت مورد نیاز است که به طور قابل توجهی مصرف پهنای باند شبکه را افزایش می‌دهد و بر مقیاس‌پذیری تأثیر می‌گذارد. با این حال، در holochain، عامل ها نیازی به اشتراک گذاری اطلاعات تراکنش فردی خود با سایر همتایان شبکه ندارند، به جز برخی گره ها که هر زمان که مالک به حالت آفلاین می رود، یک نسخه پشتیبان تهیه می کنند. بنابراین، holochain می تواند به میزان قابل توجهی میزان پهنای باند مورد نیاز و ترافیک را در شبکه کاهش دهد [۳۰].

ج. اعتبار معامله با پیچیدگی کم

در بلاک چین، ماینرها مسئول اعتبارسنجی تراکنش های جدید با حل یک مسئله ریاضی هستند. هر گره شبکه می تواند به عنوان ماینر عمل کند و در هر زمان ماینینگ را آغاز کند. به عنوان مثال، اگر ۲۰ گره شبکه وجود داشته باشد و ۱۰ تای آنها شروع به استخراج برای اعتبارسنجی یک تراکنش کنند. گره‌ای که زودتر راه‌حل چالش ریاضی را پیدا کند، تراکنش را تأیید می‌کند. یک ماینر می تواند با گره های دیگر همکاری کند و همزمان استخراج کند. مشارکت ۹ گره دیگر در فرآیند استخراج، اتلاف کامل زمان و منابع است. اگر یک تقسیم شبکه در میان فرآیند استخراج اتفاق بیفتد، تشخیص اینکه کدام بخش از شبکه هنوز فعال است دشوار می شود و در نتیجه مسائل امنیتی جدیدی برای آن تراکنش ایجاد می شود. این ممکن است در برخی موقعیت‌ها، مانند تراکنش‌های مربوط به پرداخت، حیاتی باشد. به عنوان مثال، اگر یک تراکنش دارای اطلاعات ارزهای دیجیتال باشد، رویدادهای تقسیم ممکن است باعث اختلاف نظر و عدم اطمینان بین کاربران شود [۳۱].

در مقابل، هولوچین به گره‌های جداگانه اجازه می‌دهد تا تراکنش خود را تأیید کنند و گره‌های همسایه با فاصله از پیش تعریف‌شده اجازه دارند اعتبار ثانویه آن تراکنش را هنگامی که اطلاعات تراکنش همراه با برخی اطلاعات از پیش تسویه‌شده برای آنها ارسال می‌شود، انجام دهند. از آنجایی که تنها تعداد کمی از گره‌ها کپی تراکنش را به جای تمام گره‌های شبکه نگه می‌دارند، فضای حافظه و میزان تبادل اطلاعات به طور قابل‌توجهی کمتر از بلاک چین است.

د. مکانیسم اجماع کارآمد

برخلاف بلاک چین، هولوچین نیازی به سازوکار اجماع جهانی ندارد. هولوچین به گونه ای طراحی شده است که برای هر کاربر یا گروهی از کاربرانی که می توانند تراکنش را بدون هیچ اجماع جهانی اعتبارسنجی کنند، استقلال ایجاد می

کند. بدیهی است که هولوچین کارآمدتر از بلاک چین است. برای تأیید یک تراکنش، بلاک چین تراکنش جاری را برای ذخیره اطلاعات کامل گره به همه گره ها ارسال می کند در حالی که هولوچین تنها به چند میزبان هولو نیاز دارد که در اجرای همان برنامه درگیر هستند تا تراکنش فعلی را بدون نیاز به اجماع جهانی تأیید کنند. علاوه بر این، فرآیند اعتبار سنجی، حقوق مالکیت داده و حاکمیت شبکه تنها توسط عوامل و سازندگان مدیریت می شود. در برخی موارد، ممکن است اتفاق بیفتد که داده‌ای که برای اعتبارسنجی گره‌ها یا تراکنش‌ها ارسال می‌شود، خود مجاز یا معتبر نباشد. برای رفع این مشکل، از اثر انگشت هش شده برای کمک به تشخیص احراز هویت یک تراکنش استفاده می شود.

ذ. کارایی منابع ارتباطی

در یک شبکه P۲P، بلاک چین بر ارتباط مداوم بین کاربران توزیع شده متکی است. علاوه بر این، شامل مجموعه‌ای از ماینرها می‌شود تا یک تراکنش را پردازش و تأیید کنند و آن را در همه کاربران ذخیره کنند. مکانیسم اجماع که است بخش قابل توجهی از زنجیره بلوکی نیز نیازمند تعداد زیادی کانال ارتباطی است که توان عملیاتی تراکنش شبکه را محدود می کند [۳۷]. برعکس، مکانیسم اجماع هولوچین عامل محور است و نیازی به ارتباط مکرر با گره های دیگر ندارد که تعداد کانال های ارتباطی اشغال شده را تا حد زیادی کاهش می دهد.

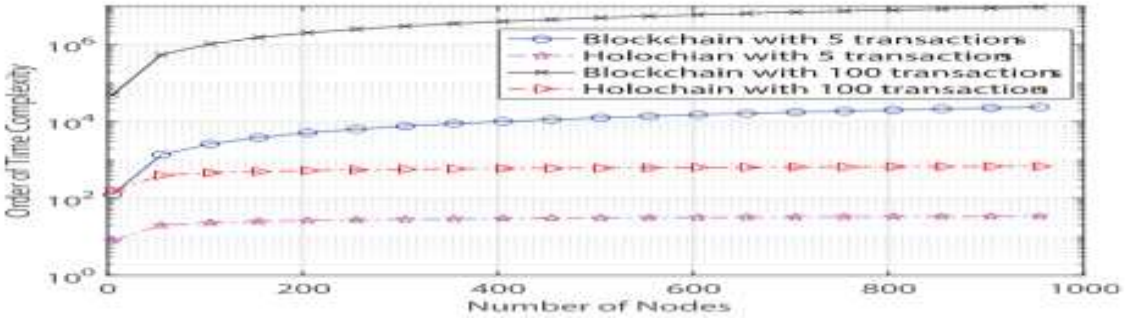
ر. زمان عملیات و کارایی حافظه

یک ویژگی ذاتی بلاک چین این است که اطلاعات تراکنش یکسانی در همه گره ها برای ارائه یکپارچگی داده در سراسر درخت هش داشته باشد. در بسیاری از کاربردهای عملی، داده‌های یک کاربر خاص ممکن است برای دیگران جالب نباشد، اما یک شبکه بلاک چین همه کاربران را مجبور می‌کند تا تمام اطلاعات را ذخیره کنند و در نتیجه زمان پردازش داده‌ها و فضای حافظه بزرگ‌تر افزایش می‌یابد. با توجه به اینکه بسیاری از دستگاه های مراقبت بهداشتی اینترنت اشیا سبک وزن هستند، این برای هدف طراحی آنها مضر است. در نتیجه، کل سیستم در مقایسه با همتای مبتنی بر هولوچین کندتر می شود [۳۰]. به عنوان مثال، در یک سیستم مدیریت مراقبت بهداشتی هوشمند، دکتر X و بسیاری دیگر، اگر نه همه، نیازی به دانستن سطح گلوکز بیمار Y ندارند. در بلاک چین، دکتر X و سایر گره‌ها نیز برای ذخیره تراکنش در مورد سطح گلوکز اعمال می‌شوند. اطلاعات بیمار Y. با این حال، در holochain، فقط برخی از عوامل انتخاب شده آن را ذخیره می کنند تا از یکپارچگی داده ها اطمینان حاصل کنند و تراکنش را به صورت محلی ذخیره کنند که باعث صرفه جویی در حافظه و همچنین زمان پردازش می شود. علاوه بر این، عوامل hApp داده های تراکنش را با استفاده از DHT به اشتراک می گذارند که به فضای کمتری نیاز دارد و شبکه را سریعتر می کند.

ز. کارایی در شبکه های بزرگ

از آنجایی که فناوری بلاک چین تمام تراکنش ها را در هر گره متصل به شبکه نظارت و ذخیره می کند، بار شبکه به سرعت با افزایش تعداد کاربران افزایش می یابد که منجر به ناکارآمدی بالا در شبکه های مقیاس بزرگ می شود. به عنوان مثال، اگر یک شبکه از ۱۰۰ گره تشکیل شده باشد، به دلیل افزایش افزونگی داده ها و همچنین پیچیدگی زمانی برای هر تراکنش، بازده شبکه ۱۰۰ برابر کاهش می یابد. در مقابل، برای holochain، وظایف پردازش تنها به صورت خطی افزایش می‌یابد و بارهای پردازشی را بین سایر گره‌های شبکه توزیع می‌کند. با در نظر گرفتن مثال بالا، اگر یک شبکه هولوچین شامل ۱۰۰ عامل باشد، کل بار شبکه بین ۱۰۰ گره توزیع می شود و هر گره تنها بخش کوچکی از کل تراکنش ها را پردازش می کند. بنابراین، اکثر گره ها ظرفیت پردازش قابل توجهی را ذخیره می کنند. با بهره‌برداری از

تعاریف پیچیدگی زمانی بالا، شکل ۲-۱ تحلیل مقایسه‌ای از ترتیب پیچیدگی زمانی را برای شبکه‌های بلاک چین و هولوچین در برابر تعداد گره‌ها ارائه می‌کند. می توان مشاهده کرد که ترتیب پیچیدگی زمانی برای یک شبکه بلاک چین به طور تصاعدی با تعداد گره ها افزایش می یابد در حالی که میانگین ترتیب پیچیدگی زمانی در یک شبکه هولوچین تا حد زیادی برای تعداد بیشتری از گره های متصل ثابت باقی می ماند.



شکل ۲-۱ ترتیب پیچیدگی زمانی شبکه های بلاک چین و هولوچین

ح. حفاظت بهتر در برابر حملات مبتنی بر اجماع

از آنجایی که بلاک چین یک تکنیک اجماع محور است، ممکن است تعدادی از حملات را هدف قرار دهند تا عملیات اجماع را مختل کنند. تعداد زیادی از گره ها برای شناسایی و جلوگیری از حملاتی که نیاز به ظرفیت محاسباتی بالایی دارند، نیاز دارند. برعکس، نمایندگان در هولوچین بیشتر در قبال سابقه تراکنش های خود پاسخگو هستند و به طور مداوم ارز هولو دیگران را بررسی می کنند تا وضعیت هزینه های اعتباری را تأیید کنند. بنابراین، عامل ها فقط باید به کد خود اعتماد کنند و بنابراین کمتر مستعد حملات مبتنی بر اجماع مانند حملات اکثریت، حملات sybil، حملات PoW، حملات انتخابی دراپ و غیره هستند.

۳پیشینه تحقیق

یزدانی نژاد و همکاران در سال ۲۰۱۹ پژوهشی با عنوان احراز هویت کنترلر های SDN مبتنی بر بلاکچین برای شبکه های IoT با مصرف انرژی بهینه ارائه کردند [13]. در این مقاله ، محققان به پتانسیل ادغام شبکه های blockchain و نرم افزار تعریف شده (SDN) در کاهش برخی از چالش ها پرداخته اند. به طور خاص ، یک معماری ایمن و با کارآیی blockchainبا استفاده از کنترل کننده های SDN برای شبکه های IoT با استفاده از یک ساختار خوشه ای با یک پروتکل مسیریابی جدید پیشنهاد شده است. این معماری از blockchain های عمومی و خصوصی برای ارتباط Peer to Peer (P2P)بین دستگاه های IoT و کنترلرهای SDN استفاده می کند ، که Proof-of-Work (POW) را از بین می برد . نتایج تجربی نشان می دهد که پروتکل مسیریابی مبتنی بر ساختار خوشه دارای توان بالاتر ، تأخیر کمتر و مصرف انرژی کمتری نسبت به پروتکل های مسیریابی EESCFD ، SMSN، AODV، AOMDVو DSDV است.

کار آل و همکاران [14] نشان می‌دهد که تخصیص کانال غنی‌شده ی ایمن، به عنوان مثال، کانال مشترک، با استفاده از جابجایی RSA(CRSA) انجام می شود. در طرح CRSA لازم است دو عدد اول با استفاده از پارامترهای رمزنگاری و رمزگشایی اعداد تصادفی برای تمامی خودروهای موجود در شبکه اینترنت اشیا ارسال شود و لازم است کلید هر خودرو مبادله شود. داده ها پس از رمزگذاری در چندین وسیله نقلیه توسط کلید آنها به وسیله نقلیه مقصد ارسال می شود و وسیله نقلیه مقصد با استفاده از کلیدهای هر وسیله نقلیه، داده ها را رمزگشایی می کند.

مشرام و همکاران [15] یک پروتکل ارتباطی امن شهر هوشمند با استفاده از کارت هوشمند، رمز عبور و نقشه‌های آشفته گسترده پیشنهاد کرد. این پروتکل از اعداد تصادفی با توابع هش (۳۱ بار) استفاده کرد تا آن را سبک کند. این روش شامل فرآیندهایی برای تغییر رمز عبور و ابطال کارت هوشمند است. اگر کارت هوشمند دزدیده شود و مهاجم بتواند رمز عبور آنلاین را از طریق حمله کانال جانبی حدس بزند، شهر هوشمند ممکن است به خطر بیفتد.

سرینیواس و همکاران در [۱۶] یک مکانیسم احراز هویت با استفاده از ECC برای شبکه وسایل نقلیه را نشان داد. این روش باید بهینه شود زیرا به دلیل محاسبات پیچیده به هزینه محاسباتی و سربار ارتباطی بالایی نیاز دارد.

ولیانگیری و همکاران [۱۷] یک روش احراز هویت مبتنی بر ECC را برای Industry ۴.۰ پیشنهاد کرد. این روش دارای چهار مرحله است که عبارتند از مرحله اولیه سازی، ثبت گواهی، مرحله انتشار گواهی و مرحله رمزگذاری داده ها. این مقاله استفاده مناسب از هر پارامتر مورد استفاده در مرحله اولیه را ارائه نکرده است و مقاله نیاز به نشان دادن فرآیندهای دقیق دارد. علاوه بر این، هزینه محاسباتی حدود ۸ ثانیه است که باید بهینه شود.

خو و همکاران یک مدل تراکنش کارآمد با استفاده از زنجیره بلوکی در [۱۸] پیشنهاد کرد. این کار عمدتاً بر تراکنش‌های کمتر برای کاهش ترافیک شبکه متمرکز بود. از رمزگذاری نامتقارن برای تلفیق امنیت استفاده کرد. به جای ارسال داده های مستقیم، توابع را با استفاده از یک الگوریتم پیش بینی خطی تطبیقی که در آن مقدار معینی از داده های واقعی آموزش داده می شود، ارسال می کند. اگر داده جدید در مقدار از پیش تعیین شده نباشد، تابع را ارسال می کند. با سنجش مصرف انرژی/سیستم سکه پاداش، سیستم متوجه می شود که آیا دستگاه ها در معرض خطر هستند یا خیر. دقت داده ها به مقدار داده بستگی دارد. اگر حجم داده زیاد باشد، میزان خطا کمتر خواهد بود.

یک چارچوب احراز هویت مبتنی بر بلاک چین و ECC برای شهر هوشمند توسط Vivekanandan و همکاران پیشنهاد شد. در [۱۹]. احراز هویت متقابل بین دو دستگاه با اشتراک گذاری کلید مخفی ذخیره شده در دستگاه ها اتفاق می افتد. این روش استفاده از گره های دروازه را برای کاهش هزینه محاسباتی حذف می کند و همچنین از بلاک چین خصوصی برای اهداف ثبت استفاده می کند که فقط توسط پرسنل مجاز قابل دسترسی است. از مکان به عنوان یک ویژگی برای اهداف احراز هویت استفاده کرد. این روش در حین احراز هویت به جز زمان ثبت نام از مرجع مرکزی استفاده نکرده است، اما این روش به هیچ اطلاعاتی از مرجع مرکزی نیاز ندارد. بنابراین، اطلاعات ثبت نام مرجع مرکزی بی ربط است. علاوه بر این، می گوید که ID یک راز دائمی است، اما از شناسه دستگاه های دیگر در هنگام احراز هویت استفاده می کند. یک مهاجم می تواند جریان پیام را استراق سمع کند و می تواند اسرار را برای جعل هویت در آینده به دست آورد. علاوه بر این، نویسندگان چارچوب احراز هویتی را که برای مشاهده کامل خوانندگان لازم است، توصیف نکردند.

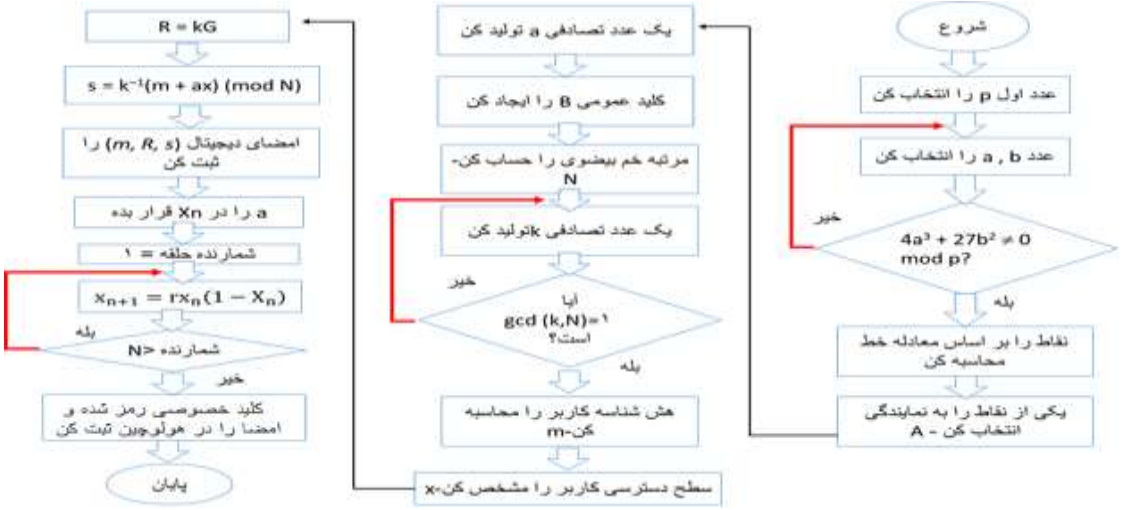
سون و همکاران [۲۰] چارچوب احراز هویت مبتنی بر بلاک چین را با در نظر گرفتن تحویل برای ارتباطات I2V پیشنهاد کرد. در این روش از ECC برای انجام احراز هویت اولیه استفاده می شود. برای جلوگیری از محاسبات پیچیده در زمان تحویل، این روش فقط از عملیات هش و XOR استفاده می‌کرد. RSU مسئول احراز هویت است و از امضا برای تأیید تراکنش استفاده می کند. در مورد چند پارامتر به وضوح نیاز است زیرا آنها به عنوان ذخیره یا محاسبه شده نشان داده نمی شوند. علاوه بر این، اگر بتوان از تأیید در وسیله نقلیه برای شروع احراز هویت اجتناب کرد، روش می‌تواند تحت تأثیر ضبط تماس هوشمند و حمله فرهنگ لغت قرار گیرد.

۳. روش‌شناسی پژوهش

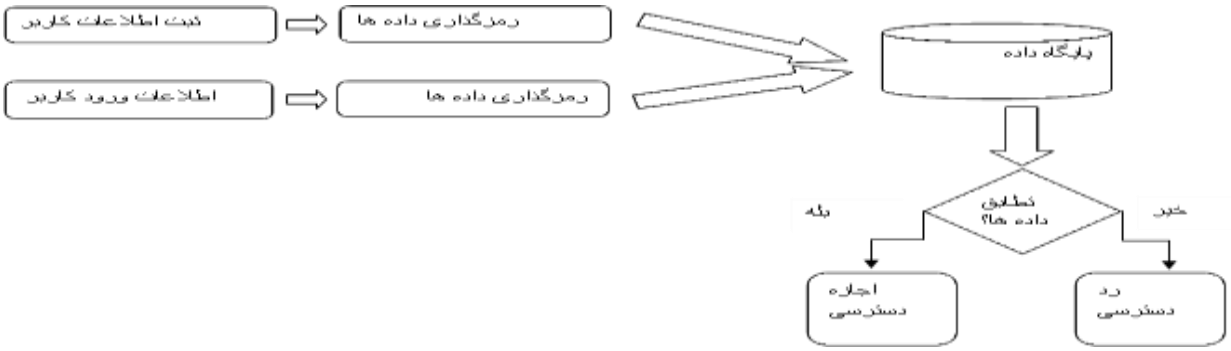
در این فصل روش پیشنهادی در این پژوهش توضیح داده خواهد شد. هدف از ارائه ی این روش و راهکار به شرح زیر است:

کاهش پیچیدگی محاسباتی مدل نسبت به مدل مبتنی بر بلاکچین : روش بلاکچین از روش هش SHA-1 استفاده می کند که این روش هش سرعتی معادل 909 MiBps دارد که برای سریع تر کردن روش پیشنهادی برای فاز هشینگ از روش black2b استفاده می شود.

ایجاد بستری امن برای ارتباطات گره ها در اینترنت اشیا : در روش هایی که مبتنی بر بلاکچین هستند از یک دفتر عمومی برای ثبت تمام داده های مورد نیاز برای احراز هویت استفاده می شود که این امر باعث می شود روند کلی الگوریتم و امنیت شبکه به همان دفتر عمومی وابسته باشد که این مساله در هولوچین به دلیل استفاده از یک روش توزیع شده به جای نگهداری متمرکز داده در دفتر عمومی برطرف می شود. در شکل زیر فلوچارت روش پیشنهادی نمایش داده شده است:



فلوچارت ۱ : نحوه تولید امضا و اجرای خم بیضوی



فلوچارت ۲: نحوه ثبت و احراز هویت

روش پیشنهادی

هولوچین ترکیبی از چندین فناوری رمزنگاری است – زنجیره هش، امضای رمزنگاری و یک DHT. هر گره بخش های داده مربوطه خود را با هش های رمزنگاری امضا شده با امضای دیجیتال خود در شبکه ذخیره و ایمن می کند. سپس

گره ها داده های امضا شده را با DHT به اشتراک می گذارند، که دارای مجموعه ای از قوانین اعتبارسنجی برای تعیین پذیرش یا رد داده های ورودی است.

- زنجیره‌های درهم‌سازی به کاربرد متوالی یک تابع هش رمزنگاری در یک مجموعه داده معین اشاره دارد. آنها ذخیره‌سازی غیرقابل تغییر داده و محافظت در برابر مهاجمانی که سعی در ربودن داده‌ها دارند، فراهم می‌کنند.

BLAKE2b یک تابع هش رمزنگاری همه منظوره است. این بدان معنی است که برای هش کردن رمزهای عبور و استخراج کلیدهای رمزنگاری از رمزهای عبور مناسب نیست. در حالی که کلیدهای رمزنگاری معمولاً صدها بیت آنتروپی دارند، رمزهای عبور اغلب بسیار پیچیده تر هستند. هنگام ذخیره رمزهای عبور به صورت هش یا هنگام استخراج کلیدها از آنها، معمولاً هدف جلوگیری از تکرار سریع همه رمزهای عبور ممکن توسط مهاجمان است. از آنجایی که گذرواژه‌ها ساده هستند، بسیار مهم است که با استفاده از الگوریتم‌های هش محاسباتی، سرعت مهاجمان را به‌طور مصنوعی کاهش دهیم. بنابراین Monocypher crypto_argon2 را برای هش کردن رمز عبور و استخراج کلیدها از پسوردها فراهم می کند. حلقه هسته به طور پیش فرض باز می شود .این امر سرعت BLAKE2b را در پردازنده های مدرن حدود ۲۰ درصد افزایش می دهد .از سوی دیگر، این اندازه باینری را چندین کیلوبایت افزایش می دهد و در برخی از پلتفرم های تعبیه شده کندتر است.

هش کردن یک پیام به یکباره:

```
uint8_t hash   [64]; /* Output hash (64 bytes)         */
uint8_t message[12] = "Lorem ipsum"; /* Message to hash */
crypto_blake2b(hash, sizeof(hash), message, sizeof(message));
```

محاسبه یک کد احراز هویت پیام به طور همزمان:

```
uint8_t hash   [16];
uint8_t key    [32];
uint8_t message[11] = "Lorem ipsu"; /* Message to authenticate */
arc4random_buf(key, sizeof(key));
crypto_blake2b_keyed(hash   , sizeof(hash),
                     key    , sizeof(key),
                     message, sizeof(message));
/* Wipe secrets if they are no longer needed */
crypto_wipe(message, sizeof(message));
crypto_wipe(key,     sizeof(key));
```

هش کردن پیام به صورت تدریجی:

```
uint8_t hash   [ 64]; /* Output hash (64 bytes) */
uint8_t message[500] = {1}; /* Message to hash  */
crypto_blake2b_ctx ctx;
crypto_blake2b_init(&ctx, sizeof(hash));
for (size_t i = 0; i < 500; i += 100) {
   crypto_blake2b_update(&ctx, message + i, 100);
crypto_blake2b_final(&ctx, hash);
```

محاسبه کد احراز هویت به صورت تدریجی:

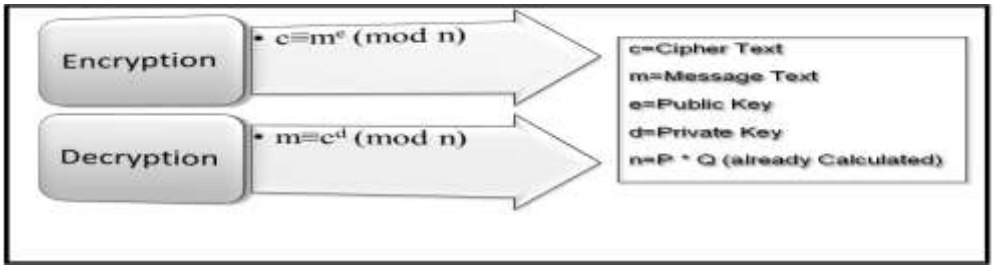
```
uint8_t hash   [ 16];
uint8_t key    [ 32];
uint8_t message[500] = {1}; /* Message to authenticate */
arc4random_buf(key, sizeof(key));
crypto_blake2b_ctx ctx;
crypto_blake2b_keyed_init(&ctx, sizeof(hash), key,
                          sizeof(key));
```

```
/* Wipe the key */
crypto_wipe(key, sizeof(key));
for (size_t i = 0; i < 500; i += 100) {
   crypto_blake2b_update(&ctx, message + i, 100);
   /* Wipe secrets if they are no longer needed */
   crypto_wipe(message + i, 100);
crypto_blake2b_final(&ctx, hash);
```

امضای رمزنگاری به استفاده از الگوریتم های کلید عمومی برای ارائه یکپارچگی داده ها اشاره دارد. فرض کنید یک ماشین خاص پیام ها را با امضای دیجیتال خود امضا می کند. سپس دیگران می توانند امضا را تأیید کنند و ثابت کنند که داده ها تغییر نکرده و از ماشین خاصی منشاء گرفته اند.

برای این بخش از روش رمزنگاری RSA استفاده می شود. در سال ۱۹۷۸ سه نفر به نامهای ری‌وست ،شامیر و اَدلمن الگوریتمی را برای پیاده سازی رمزنگاری کلید عمومی با یک جفت کلید معرفی کردند که به RSA شهرت یافت و در طول سه دهه اخیر بطور گسترده ای مورد استفاده قرار گرفته و در گذر زمان، سخت افزار و نرم افزارهای بهینه آن به بازار عرضه شد. اگر چه بعدها الگوریتم قوی‌تری بنام El Gamal ابداع شد اما هنوز هم روش RSA در صدر فهرست الگوریتمهای کلید عمومی قرار دارد.

فرض کنید فرستنده پیام جفت عدد صحیح و بزرگ (e,n) را بعنوان کلید عمومی برای رمزنگاری اطلاعات خود در اختیار دارد. در طرف مقابل ،گیرنده نیز جفت عدد (d,n) را برای رمزگشایی پیام بکار می برد.بدیهی است که دو جفت عدد (e,n)و (d,n) با یکدیگر ارتباط زیرکانه ای دارند ولی بگونه ای نیست که بتوان با در اختیار داشتن e و n براحتی d را استنتاج کرد.



شکل۳ - ۱ مراحل الگوریتم رمزنگاری

با فرض وجود چنین کلید هایی ،الگوریتم RSA در نهایت سادگی به صورت زیر است:

الف)پیامی که باید رمز شود به بلوکهای K کاراکتری (k بایتی) تقسیم بندی می شود.

ب)هر بلوک طبق قاعده ای کاملا دلخواه به یک عدد صحیح به نام P_i تبدیل می گردد.

ج)با جفت عدد (e,n) به ازای یکایک بلوکهای P_i اعداد جدیدی طبق رابطه زیر بدست می آیند:

$C_i = (P_i)e \bmod n$

Pi	0803	0418	1405	1200	1702	0723
$C_i=(P_i)^e \bmod n$	0779	1983	2641	1444	0052	0802

د) کدهای C_i بجای کدهای اصلی P_i ارسال می شوند.

روش رمزگشایی داده ها دقیقا مثل روش رمزنگاری است یعنی با داشتن جفت عدد (d,n) بلوکهای رمز شده بصورت زیر از رمز خارج می شوند:

$$P_i = (C_i)d \bmod n$$

کل الگوریتم در همینجا خاتمه می یابد.

در RSA ،به جفت عدد (e,n) که متن به کمک آن رمز می شود، اصطلاحا کلید عمومی (public key) و به جفت عدد (d,n) که متن بوسیله آن از رمز در می آید، کلید خصوصی (private key) گفته می شود. نکته اساسی در RSA آن است که جهت تضمین وارون پذیری روش رمز، اعداد و بایستی در رابطه

$$(x)^{e.d} \bmod n = x$$

صدق کنند لذا باید در انتخاب اعداد دقت کرد.

اصل اساسی دیگری که باید در رمزنگاری RSA حتما رعایت شود آن است که کدهای P_i که به هر بلوک نسبت می دهیم باید در شرط $0 \leq P_i < n$ صدق کند .بنابراین اگر بلوکها بصورت رشته های k بیتی مدل شوند، باید شرط $K < n^{۲}$ برقرار باشد. دلیل این امر آن است که براحتی بتوان گزاره $P_i \bmod n = P_i$ را نوشت و الا در حالت کلی این گزاره درست نمی باشد و در این صورت رمزگشایی صحیح داده ها تضمین نخواهد شد.

روش انتخاب e و dکه توسط ابداع کنندگان RSA پیشنهاد شده ،عبارت است از:

الف)دو عدد دلخواه (اما بزرگ) p و qرا انتخاب می شود.

ب)اعداد n و z را طبق دو رابطه زیر محاسبه می گردد:

$$n = p * q$$
$$z = (p-۱) * (q-۱)$$

ج) عدد d طوری انتخاب می شود که نسبت به z اول باشد یعنی هیچ عامل مشترکی که هر دو بر آن بخشپذیر باشند یافت نشود.

د)بر اساس d ،عدد e طوری انتخاب می شود که رابطه زیر برقرار باشد: (بعبارتی معکوس ضربی d در پیمانه z محاسبه شده و e نامیده می شود)

$$(e * d) \bmod z = ۱$$

آنچه که مشخص است در کاربردهای عملی، اعدادp وq حداقل صد رقمی (صد رقم در مبنای ده) انتخاب می شوند یعنی این دو عدد حداقل از مرتبه ۱۰۱۰۰ هستند .در این حالت عدد صحیح متناظر با بلوکهای P_i که طبق شرط فوق باید کمتر از n باشند، نبایستی از ۸۳ کاراکتر بیشتر باشند،زیرا:

$$p , q \approx ۱۰۱۰۰ \rightarrow n = p * q \approx ۱۰۲۰۰ \rightarrow (Pi < (۲۶۶۴ \approx ۱۰۲۰۰)) \rightarrow P_i < ۲۶۶۴$$

پس هر بلوک متن بایستی حداکثر۶۶۴ بیت یا ۸۳ کاراکتر هشت بیتی باشد.

در اینجا توجه به این نکته ظریف لازم است که برای محاسبه $A^e \bmod n$ لازم نیست که A به تعداد e بار در خودش ضرب و سپس باقیمانده اش بر n پیدا شود زیرا با استفاده از برخی خواص ریاضی نتیجه محاسبات هیچگاه از n فراتر نمی رود.

حال فرض کنید یک نفذگر بخواهد با در اختیار داشتن کلید عمومی (e,n) ، را بدست آورد.در اینصورت باید در وهله اول n را به دو عامل اول آن یعنی p و q تجزیه کند تا بتواند z را محاسبه کرده و سپس d را بدست آورد. برای تجزیه اعداد به عوامل اول آن هیچ راهی بجز جستجو و آزمون وجود ندارد و با توجه به این که n حداقل دویست رقمی است،تجزیه چنین اعدادی حتی به کمک کامپیوتر هزاران سال طول خواهد کشید.

برای مثال، طبق گزارشی از سایت RSA، تخمین زده می شود که یک کلید ۲۱۵ بیتی می تواند با هزینه ای کمتر از ۱ میلیون دلار و یک تلاش ۸ ماهه شکسته شود. RSA توصیه میکند که کلیدهای ۲۱۵ بیتی در حال حاضر امنیت کافی ایجاد نمی کنند و باید بنفع کلیدهای ۸۶۷ بیتی برای استفاده های شخصی کنار بروند! به همین ترتیب برای استفاده شرکتها کلیدهای ۱۰۲۴ بیتی و از ۲۰۴۸ بیت برای کلیدهای فوق العاده ارزشمند استفاده شود. البته پیش بینی شده است که این مقادیر تا حداقل سال ۲۰۰۴ معتبر خواهد بود. با پیشرفتهای موجود احتمالا در این زمان نیاز به افزودن بر طول کلید ها خواهد بود.

جدول زیر نشاندهنده افراد یا گروههایی است که توانایی شکستن کلیدها با طولهای متفاوت را دارند.

طول کلید	نفوذگران بالقوه
۲۵۶ بیتی	افراد عادی
۳۸۴ بیتی	گروههای تحقیق دانشگاهی و شرکتها
۵۱۲ بیتی	گروههای دولتی با تمام امکانات
۷۶۸ بیتی	امن برای کوتاه مدت
۱۰۲۴ بیتی	امن تا آینده نزدیک
۲۰۴۸	امن احتمالا تا چند ده سال!

الگوریتم RSA

الگوریتم رمزنگاری RSA به صورت زیر تعریف شده است:

```
function cipherrsa=rsa(p,q,str)
e=p;
Pk=q;
M=str;
x=length(M);
c=0;
for j= 1:x
   for i=0:122
      if strcmp(M(j),char(i))
         c(j)=i;
      end
   end
end
for j= 1:x
  cipher(j)= crypt(str(j),Pk,e);
end
cipherrsa=cipher;
end
```

۳-۴ کاربردهای برخی الگوریتمهای کلید عمومی

الگوریتم	رمزگذاری/ رمز گشایی	امضاء رقمی	توزیع کلید
RSA	√	√	√
Diffie Hellman	×	×	√
DSS	×	√	×

- فناوری جدول هش توزیع شده به عنوان یک سرویس جستجوی داده استفاده می شود. جداول هش را که شاخص‌هایی از کلیدها (شناسه‌های منحصربه‌فرد) هستند که به مقادیر (هر داده دلخواه) اشاره می‌کنند، در ماشین‌های مختلف برای اهداف غیرمتمرکز پخش می‌کند. اگر یکی از ماشین ها ناپدید شود، فقط داده های آن ماشین خاص از بین می رود. اما با پیاده سازی این روش رمزنگاری به این نتیجه می رسیم که این روش نسبت به حمله ی دیفن هلمن مقاوم نمی باشد. در نتیجه از روش رمزنگاری خم بیضوی استفاده می شود. در خم بیضوی p یک عدد اول است . ما یک مجموعه به نام z_p تشکیل می دهیم که عناصر این مجموعه بین ۱ تا p-1 است. که این گروه تحت عمل mod p شکل می گیرد. مرتبه[1] یک گروه از اجزای g که زیر مجموعه ای از گروه G می باشند حداقل عدد صحیح مثبت N است، هنگامی که میدان متناهی را به شکل F_p تعریف می کنیم p باید برابر q^m باشد که q یک عدد اول است و m یک توان مثبت صحیح می باشد. خم بیضوی E تحت F_p به صورت فرمول۱ تعریف می شود[14]:

فرمول۱

$$E = \{(x.y) \in k^2 | y^2 = X^3 + ax + b\} \cup \{\emptyset\}$$

در این خم بیضوی معادله خط به صورت فرمول۲ تعریف می شود[14] :

فرمول2

$$Y^2 = x^3 + ax + b$$

که در این فرمول مقادیر a , b باید به گونه ای انتخاب شوند که شرط موجود در فرمول۳ را برقرار کند[14]:

فرمول3

$$4a^3 + 27b^2 \neq 0 \bmod p$$

که a , b عضو F_p هستند و $4a^3 + 27b^2 \neq 0 \bmod p$

$E(F_p)$ شامل تمام نقاط (x,y) که x,y عضو F_p هستند که توسط معادله بالا بدست می آیند. سپس یک نقطه اولیه[2] A از مجموعه نقاط موجود انتخاب می شود. یک عدد تصادفی a بین [1 , n-1] پیدا می شود. آنگاه B=aA محاسبه می شود که B کلید عمومی و a کلید خصوصی است. البته کلید عمومی به صورت مجموعه (E, F_p, N, A, B) درنظرگرفته می شود. این مقادیر در فرمول۴ نمایش داده شده اند[14]:

فرمول۴

$$a \in [1 , n-1]$$
$$(E, F_p, N, A, B) \quad و \quad B=aA$$

در این فرمولA یک نقطه است و هنگامی که یک نقطه به مختصات (x,y) در عددی ضرب می شود به این معنی است که آن نقطه به تعداد عدد ضرب شده باید با خودش جمع شود. درواقع در فرمول بالا نقطه ی A به تعداد a بار با خودش جمع شده است. قواعد جمع نقاط دریک خم بیضوی به صورت زیر می باشد اگر PوQ باهم مساوی نباشند از روابط ۵ تا ۷ استفاده می شود[14]:

فرمول ۵

[1] order
[2] Generic

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

فرمول ۶

$$x_R = s^2 - (x_P + x_Q)$$

فرمول ۷

$$y_R = s(x_P - x_R) - y_p$$

و اگر PوQ باهم مساوی باشند از روابط ۸ تا ۱۰ استفاده می شود[14] :

فرمول ۸

$$s = \frac{3x_p^2 - a}{2y_P}$$

فرمول ۹

$$x_R = s^2 - (2x_P)$$

فرمول ۱۰

$$y_R = s(x_P - x_R) - y_p$$

در این مرحله ابتدا مرتبه خم N مشخص شده و سپس یک عدد تصادفی k طوری انتخاب می شود که $1 \leq k < N$ همچنین k وN نسبت به یکدیگر اول باشند درواقع بزرگترین مقسوم علیه مشترک آنها ۱=gcd(k,N) باشد.

دراین مرحله به محاسبه R = kG و هش[1] شناسه کاربر مورد نظر m پرداخته می شود و مقدار s از طریق فرمول ۱۱ محاسبه می شود[14]:

فرمول ۱۱

$$s = k^{-1}(m + ax) \pmod N$$

و x که سطح دسترسی کاربر می باشد هرکدام محاسبه شده و در انتها مجموعه (m, R, s) به عنوان امضای دیجیتال[2] کاربرشناخته می شود و این مجموعه دربلاکچین ذخیره می شود. مدارک الکترونیکی نیز همانند متون کاغذی نیاز به امضا دارند. این امضاها شباهت هایی با امضاهای دستی دارند. امضای دیجیتال ، طرحی برای نشان دادن درستی پیام های ارسالی است .هنگامی که یک پیام از سوی یک نفر برای دیگری ارسال می شود، گیرندۀ پیام به وسیلۀ امضای دیجیتال ، هویت فرستنده را شناسایی می کند و از اعتبار پیام مطمئن می شود. یک امضای دیجیتال از سه الگوریتم تشکیل شده است: الگوریتم تولید کلید، الگوریتم تولید امضا و الگوریتم تأیید امضا، در الگوریتم تولید کلید، گیرندۀ پیام یک کلید خصوصی تولید می کند، سپس با استفاده از کلید عمومی و متن ارسالی، امضا توسط فرستندۀ پیام تولید و در پایان، صحت امضا با استفاده از کلیدخصوصی توسط گیرندۀ پیام تأیید می شود .

از آنجا که کلید خصوصی برای رمزگشایی اطلاعات ارسالی به یک گیرنده استفاده می شود و نقش مهمی در امنیت سیستم دارد، درصورت دستیابی هکر[3] به یک بلاک باید از افشای کلید خصوصی به آسانی جلوگیری کرد که در الگوریتم های پیشین به این نکته توجه نشده است. در روش پیشنهادی ابتدا کلید خصوصی a به کمک نظریه

[1] Hash
[2] Digital Signature
[3] Hacker

آشوب[1] که حساس به عدد اولیه می باشد با یک آشوب پیش بینی نشده ای به یک مقدار نهایی تبدیل خواهد شد. کلید خصوصی a توسط معادله لجستیک نمایش داده شده در فرمول ۱۲ ، به تعداد مرتبه معادله N تکرار خواهد تا به یک عدد شبه تصادفی تبدیل شود و مقدار x_{n+1} نهایی در بلاکچین ذخیره می شود.

فرمول ۱۲

$$x_{n+1} = rx_n(1 - X_n)$$

مراحل تولید کلیدهای خصوصی و عمومی در زیر آمده است:

۱- خم بیضوی E را تحت z_p انتخاب می کنیم. تعداد نقاط در E(z_p) به عدد اول بزرگ n بخش پذیر باشد

۲- یک نقطه p را که عضو E (z_p) است و از مرتبه ی n است پیدا می کنیم.

۳- یک عدد صحیح d منحصر به فرد را در بازه ی [1 – n-1] انتخاب می کنیم.

۴- Q= d.p را محاسبه می کنیم.

۵- کلید خصوصی ما d است و کلید عمومی ما (E , p , n , Q)

برای ایجاد امضای دیجیتال مراحل زیر محاسبه می شود:

۱- یک عدد k منحصر به فرد بین بازه [1 , n-1] تولید میکنیم.

۲- K*p را محاسبه کرده که یک نقطه به مختصات (x1 , x2) می شود.

۳- r= x1 mod n . اگر r صفر بود به مرحله ی یک می رویم.

۴- S= (1/k) { h(m) + d*r} mod n را حساب می کنیم که h یک تابع hash است.

۵- اگر S=0 بود انگاه به مرحله یک میرویم.

۶- امضای پیام M عبارت است از یک جفت عدد صحیح (r , s)

[1] Chaos Theory

۴. یافته‌های پژوهش

برای ارزیابی روش احراز هویت، هر یک از فرآیندهایی که در این فرآیند انجام می شود به طور جداگانه بررسی می شود تا زمان پردازش مورد نیاز برای هر یک از این قسمت ها بررسی شود. در جدول زیر زمان هر محاسبه و فرآیند در اجرای الگوریتم بر حسب واحد ثانیه نمایش داده شده است:

Process	Sec	Percentage
hi	0.001552267	0.081%
IDi	0.000340767	0.01778%
ki	0.002676633	0.13968%
li	0.0033637	0.17554%
m	0.0000779	0.00406%
mk	0.000219867	0.01147%
PKi	0.224936767	11.7388%
Ppub	0.204789233	10.6873%
ri	3.95667E-05	0.00206%
Ri	0.2230888	11.6423%
si	5.02667E-05	0.00262%
τ	0.0000748	0.00390%
ti	3.99E-05	0.00208%
Ti	0.227536567	11.8745%
xi	0.0000318	0.00165%
ایجاد امضا	0.893106466	46.60 %
تایید امضا	1.023071467	53.40 %
کل زمان محاسبات	1.916177933	100 %

در ادامه روشی ارائه می شود که زمان اجرای این محاسبات را کاهش داده و در نتیجه زمان کل الگوریتم تولید امضا کاهش می یابد. در الگوریتم ارائه شده، متن پیام ورودی را از ورودی گرفته و در متغیری مانند پیام ذخیره می کنیم.

```
message=char(input('Enter your message: ','s'));
```

در مرحله ی بعد عددی اول مثل m را از ورودی گرفته و $p=2^m$ را محاسبه می کنیم.

```
m=input('Emter m:');
p=power(2,m);
```

سپس با توجه به فرمول زیر نقاط روی خم بیضوی را بدست می آوریم:

$$(y^2 + xy) \bmod p = x^3 + a * x^2 + b$$

با این شرایط که a , b اعدادی بین ۰ تا p-1 هستند. نقاط بدست آمده از فرمول بالا را در مجموعه ای به نام G ذخیره می کنیم. تعداد نقاط بدست آمده در خم بیضوی را در متغیری به نام N ذخیره می کنیم.

محاسبه ی کلید خصوصی :

برای بدست آوردن کلید خصوصی یک عدد تصادفی بین ۱ تا N بدست می آوریم به عنوان مثال در این الگوریتم عدد تصادفی بدست آمده را در متغیری به نام point قرار داده ایم. سپس در مجموعه G نقطه ای را که در مکانی برابر با محل نقطه قرار دارد به عنوان کلید خصوصی انتخاب کرده و با نام P ذخیره می کنیم.

```
point=floor(rand()*N)+1;
P=[1,2];
P(1,1)=G(point,1);
P(1,2)=G(point,2);
```

محاسبه ی کلید عمومی:

برای بدست آوردن کلید عمومی، یک عدد تصادفی بین ۱ و N-1 بدست می آوریم. برای مثال در این الگوریتم عدد تصادفی به دست آمده را در متغیری به نام id قرار داده ایم. سپس این عدد به دست آمده را در مختصات نقطه P ضرب می کنیم نقطه جدید به دست آمده R نامیده می شود و کلید عمومی الگوریتم به دست می آید.

```
id=randi(N-2,1,1)+1;
R1=P(1,1)*id;
R2=P(1,2)*id;
```

در مرحله بعد پیام ورودی ذخیره شده در متغیر message را به تابع هش می فرستیم و خلاصه پیام را در متغیری به نام e ذخیره می کنیم. در این الگوریتم از تابع هش استفاده شده است. می توانید پارامترهای ورودی تابع هش را در زیر مشاهده کنید:

```
v1=hex2dec('cbbb9d5dc1059ed8');
v2=hex2dec('629a292a367cd507');
v3=hex2dec('9159015a3070dd17');
v4=hex2dec('152fecd8f70e5939');
v5=hex2dec('67332667ffc00b31');
v6=hex2dec('8eb44a8768581511');
v7=hex2dec('db0c2e0d64f98fa7');
v8=hex2dec('47b5481dbefa4fa4');
e=mod(HASH512(v1,v2,v3,v4,v5,v6,v7,v8,message),N);
```

در تابع هش ابتدا متن ورودی به کد اسکی تبدیل می شود سپس این کدها باید به ۱۰۲۴ بیت تبدیل شوند. به این ترتیب ابتدا کدهای اسکی به دست آمده برای متن اصلی به باینری تبدیل می شوند. اگر این کدهای تبدیل شده کمتر از ۸۹۸ بیت باشند، بیت های اضافی را به کد تبدیل شده به باینری اضافه می کنیم تا تعداد بیت ها به ۸۹۸ بیت برسد. برای افزودن بیت های اضافی، ابتدا یک عدد ۱ و سپس ۰ وارد می کنیم تا به بیت ۸۹۸ برسیم. با تبدیل طول متن ورودی به یک عدد باینری ۱۲۷ بیتی، بیت های باقی مانده را که ۱۲۷ بیتی هستند، بدست می آوریم.

در مرحله بعد کل پیام به بلوک های ۶۴ بیتی تقسیم می شود. تعداد این بلوک ها را در متغیری به نام N1 قرار می دهیم. سپس برای هر بلوک ۶۴ بیتی موارد زیر را انجام می دهیم:

آرایه ای با ۸۰ خانه به نام w تعریف می کنیم. هر خانه از این نمایش ۶۴ بیت است. بنابراین، بیت های بلوک اول تا N1 را در خانه های اول تا N1 از w قرار می دهیم. پس از به دست آوردن تمام ۸۰ خانه w، مقدار هر خانه را تغییر می دهیم. در نهایت با ادغام متغیرهای H1 به H7، خلاصه پیام ورودی را بدست می آوریم.

در مرحله بعدی الگوریتم امضای دیجیتال به دنبال عددی می گردیم که اگر در یکی از اعداد ۱ تا N-1 ضرب شود، باقیمانده تقسیم صحیح برابر با ۱ می شود. پس از یافتن چنین عددی، آن را در آن ذخیره می کنیم. متغیری به نام la. سپس این عدد را در فرمول زیر قرار دهید تا مقدار s1 بدست آید:

$$S1 = la * (e + id * U) \bmod N$$

شبه کد بدست آوردن عدد la را در زیر مشاهده می کنید:

```
for k=1 to N-1
     if(mod((k*nr),N)==1)
       la=k;
     end if
end for
```

مقدار S1 همان امضای پیام ما خواهد بود که در آخر آن را به عددی در مبنای ۱۶ تبدیل کرده و به انتهای پیام می چسبانیم.

۲-۴ خطرات و حمله های احتمالی به امضای دیجیتال

در شبکه هایی که به شکل بی سیم با هم در اتباط هستند به دلیل فضای باز ارتباطی و رسانه ی انتقالی که به شکل امواج محیط است، کاربران مهاجم و یا نفوذگران می توانند به شبکه نفوذ کنند و داده ها را دستکاری کنند. وجود یک کلید قوی و با تعداد کاراکترهای مناسب می تواند از داده ها در برابر برخی حملات در شبکه حفاظت کند که در ادامه انواع حملاتی که در شبکه می تواند رخ دهد معرفی شده اند :

- **حمله Key-Only**

در این حمله، دشمن فقط کلید عمومی امضاکننده را می‌داند و بنابراین فقط می‌تواند اعتبار امضای پیام‌هایی که به او داده شده را بررسی کند.

- **حمله Known Signature**

دشمن کلید عمومی امضاکننده را می‌داند و جفت‌های پیام / امضا را که توسط امضاکننده انتخاب و تولید شده است، دیده است. این حمله در عمل امکان پذیر است و بنابراین هر روش امضایی باید در برابر آن ایمن باشد.

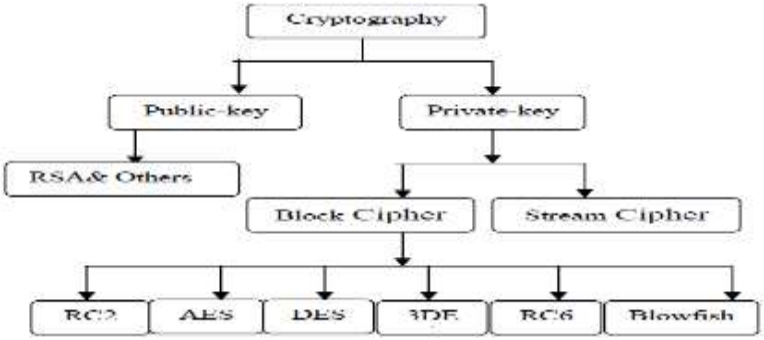
- **حمله Chosen Message**

دشمن مجاز است از امضاکننده بخواهد تعدادی پیام را به انتخاب خود امضا کند. انتخاب این پیام ها ممکن است به امضاهایی که قبلا گرفته شده است بستگی داشته باشد. این حمله ممکن است در بیشتر موارد غیرعملی به نظر برسد، اما با رعایت قانون احتیاط، روش امضایی که در برابر آن ایمن باشد ترجیح داده می شود.

- **حمله Man-in-the-middle**

در این حمله فرد با سوء استفاده از موقعیت در هنگام تبادل کلید عمومی، کلید عمومی خود را جایگزین کرده و برای گیرنده ارسال می کند و به این ترتیب بدون اطلاع فرستنده و گیرنده می تواند به پیام ها دسترسی داشته باشد.

بنابراین برای افزایش امنیت پیام ها و امضای الکترونیکی اسناد، رویکرد دیگری که می توان در نظر گرفت این است که پس از تولید چکیده پیام، چکیده با استفاده از یکی از روش های رمزگذاری رمزگذاری شده و مقدار خروجی رمزگذاری می شود. آن را به انتهای متن اضافه کنید. در این تست از روش های رمزگذاری AES، DES، DES۳، RC2، RC6 و Blowfish استفاده کرده ایم که در ادامه نتایج این تست ها را مشاهده خواهید کرد.



نتایج آزمایشات

در این آزمایش از یک پردازنده لپ تاپ i5core با فرکانس ۲.۵ گیگاهرتز استفاده کردیم که اطلاعات به دست آمده را در آن ذخیره می کنیم. در این آزمایش‌ها، فایل‌هایی با حجم ۳۲۱ کیلوبایت تا ۷.۱۳۹ مگابایت را رمزگذاری می‌کند.

برخی از معیارهای مهم برای ارزیابی کارایی الگوریتم های رمزنگاری عبارتند از:

۱. زمان رمزنگاری
۲. زمان پردازش CPU
۳. سیکل های ساعت CPU و توان باتری

زمان رمزگذاری مقدار زمانی است که یک الگوریتم رمزنگاری برای تولید یک متن رمزی از یک متن ساده نیاز دارد. زمان رمزگذاری برای محاسبه کارایی یک روش رمزگذاری استفاده می شود و سرعت رمزگذاری را نشان می دهد. عملکرد روش رمزگذاری با تقسیم تعداد کل بایت های رمزگذاری شده متن اصلی بر زمان رمزگذاری محاسبه می شود. زمان پردازش CPU زمانی است که یک CPU به تنهایی مسئول پردازش محاسبات خاصی است که بار CPU را منعکس می کند. هر چه زمان CPU بیشتر در فرآیند رمزگذاری استفاده شود، بار CPU بیشتر می شود. چرخه های ساعت CPU اندازه گیری است که نشان می دهد چقدر توان CPU در طول پردازش عملیات رمزنگاری مصرف شده است. هر چرخه CPU مقدار کمی انرژی مصرف می کند.

آثار زیر عبارتند از:

• مقایسه ای بین نتایج روش های مختلف رمزگذاری و رمزگشایی از نظر زمان رمزگذاری در دو روش مبتنی بر کدگذاری پایه ۱۶ و پایه ۶۴ انجام شده است.

• تحقیقی در مورد تأثیر تغییر اندازه بسته های داده بر مصرف باتری در طول اجرای هر یک از الگوریتم های رمزگذاری متقارن انتخاب شده انجام شده است.

• تحقیق در مورد تأثیر تغییر اندازه انواع داده ها – مانند متن یا سند یا تصویر – بر مصرف باتری، برای هر الگوریتم رمزگذاری انتخاب شده.

• تحقیقی در مورد تأثیر تغییر اندازه کلید بر مصرف باتری بر روی الگوریتم های رمزگذاری متقارن انتخاب شده انجام شده است.

نتایج شبیه سازی

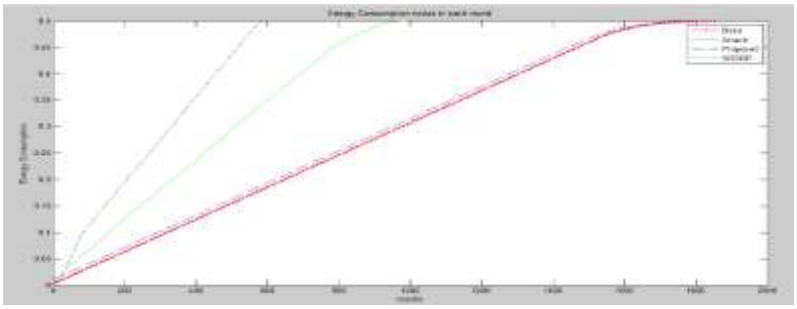
تاثیر تغیر اندازه بسته های داده الگوریتم رمزنگاری بر مصرف باتری

زمان رمزگذاری به منظور محاسبه کارایی یک روش رمزگذاری محاسبه می شود و سرعت عملیات رمزگذاری را نشان می دهد. عملکرد روش رمزگذاری با تقسیم تعداد کل بایت های رمزگذاری شده متن اصلی بر کل زمان رمزگذاری آن الگوریتم محاسبه می شود. با افزایش کارایی، مصرف باتری عملیات رمزگذاری کاهش می یابد.

Process	Sec
hi	0.000556821
IDi	0.0002321501
ki	0.001623547
li	0.0023254
m	0.0000685
mk	0.0001254177
PKi	0.02425876
Ppub	0.10452178
ri	3.975863E-04
Ri	0.1652478
si	5.02497E-04
τ	0.0000752
ti	3.86E-05
Ti	0.127532478
xi	0.0000316
ایجاد امضا	0.003106325
تایید امضا	1.022035877
کل زمان محاسبه	1.71617652

تاثیر تغیر نوع داده در الگوریتم رمزنگاری بر روی مصرف انرژی

برای محاسبه مصرف انرژی، پس از اتمام شبیه سازی، میانگین مصرف انرژی محاسبه شده و در شکل ۱-۴ نشان داده شده است.



شکل ۱-۴متوسط مصرف انرژی شبکه در هر دور

همانطور که در شکل ۱-۴ نشان داده شده است، میانگین مصرف انرژی برای حالت حمله بیشتر از سایر حالت ها است. این باعث کاهش طول عمر شبکه در حالت حمله می شود. زیرا گره های شبکه با ارسال پیام های hello متوالی انرژی زیادی در شبکه مصرف می کنند. علاوه بر این، روش ایمن به دلیل اینکه توانایی تشخیص صحیح گره های مخرب و حذف آنها را دارد، مصرف انرژی دستگاه های اینترنت اشیا را کاهش می دهد. روش پیشنهادی نسبت به روش اصلی توانایی بسیار بهتری در شناسایی پیام های مخرب دارد و این به بهبود عملکرد این روش کمک می کند.

۵. نتیجه‌گیری

جنبه‌های حقوقی امضای الکترونیک

اینکه چه چیزی می تواند به عنوان امضای الکترونیکی مورد استفاده قرار گیرد یک موضوع حقوقی است، زیرا پردازش فنی اطلاعات یا داده ها زمانی می تواند به عنوان امضا استفاده شود که قانون چنین اعتبار و مجوزی به آن بدهد. بنابراین

بعد از اینکه علوم کامپیوتر توانست امضای الکترونیکی ایجاد کند و امنیت آن را حداقل به اندازه امضای دست نویس تضمین کند، نوبت به علم حقوق می رسد که به مسائل حقوقی خود عمل کند. بنابراین در مورد امضای الکترونیکی ابتدا نگاه ها به جنبه های اجرایی، فنی و امنیتی آن معطوف شده و سپس به جنبه های حقوقی و حقوقی می رسد.

ماهیت امضای الکترونیکی

قبل از ظهور امضای الکترونیکی، برای واگذاری اسناد و اقدامات به افراد، از مهر و امضای دست نویس استفاده می شد و به جز ممنوعیت استفاده از مهر در چک، هر دو کاربرد و ارزش یکسانی دارند. در مورد چک ماده ۳۱۱ قانون تجارت می گوید چک باید به امضای صادرکننده برسد. بنابراین بسیاری از حقوقدانان معتقدند قانونگذار صدور چک را فقط از طریق امضای صادرکننده پذیرفته است و با توجه به صراحت ماده ۳۱۱ قانون تجارت که در مهر ذکر نشده است، نمی توان از مهر در مهر استفاده کرد. صدور چک به این دلیل که قانونگذار برای صدور چک افراد بی سواد را نخواسته است و ثانیاً ماده ۲۲۳ قانون تجارت در مورد برات علاوه بر امضاء مهر را نیز معتبر می داند اما در ماده ۳۱۱ ق.م. قانون گفت، هیچ اشاره ای به مهر نشده است. بنابراین صدور چک فقط با امضا امکان پذیر است و این امضا باید دست نویس باشد یعنی امضای شخصی که مهر شده برای صدور چک معتبر نیست. بنابراین این موضوع که امضای الکترونیکی در مهر یا امضای دست نویس در خصوص صدور چک الکترونیکی - به عنوان یکی از روش های پرداخت در قراردادهای الکترونیکی - درج می شود، اهمیت می یابد.

برخی از حقوق دانان امضای الکترونیکی را در ردیف مهر قرار داده اند، زیرا از نظر ماهیت با امضای دست نویس متفاوت است و بیشتر شبیه مهر است. امضای الکترونیکی چیزی نیست جز یک سری فرمول های ریاضی که توسط مقامات گواهی امضا تایید می شود و به افراد داده می شود و اگرچه امضا نامیده می شود اما به این دلیل که توسط شخص ثالث تولید شده و به افراد اختصاص داده شده است و فقط به افراد اختصاص داده شده است. از آنها به شکلی استفاده کنید که در تحلیل حقوقی در ردیف مهر قرار می گیرند.

طبق ماده ۷ قانون تجارت الکترونیکی ایران، «هرگاه قانون، وجود امضاء را لازم بداند، امضای الکترونیکی مکفی است» یعنی امضای الکترونیکی هر ماهیتی که داشته باشد (مهر، امضاء یا ماهیت دیگر) از نظر قانون جایگزین امضاء دست‌نویس با آثار حقوقی مشابه شده است.

پذیرش قانونی امضای الکترونیک

به موازات گسترش و پذیرش مبادلات الکترونیکی، موج قانون گذاری در این زمینه نیز در سال های اخیر (بین سال های ۱۹۹۶ تا ۲۰۰۱ میلادی) چشمگیر بوده است. اکثر کشورهایی که به قانونی کردن تجارت الکترونیک روی آورده اند، یکی از مهم ترین مسائلی که با آن مواجه بوده اند، پذیرش امضای الکترونیکی بوده است. در حال حاضر اکثر این کشورها بدون تردید این نوع امضا را به عنوان یکی از اقدامات با همان آثار حقوقی امضای دستی پذیرفته اند. در برخی کشورها حتی قوانین و لوایح مستقلی برای امضای الکترونیکی وضع شده است. در اسپانیا «قانون امضای الکترونیکی اسپانیا» در سال ۱۹۹۹ و در آلمان «قانون امضای الکترونیکی» در سال ۲۰۰۰ تصویب شد، اما اکثر کشورها در قوانین مربوط به مبادلات و ارتباطات الکترونیکی امضای الکترونیکی را ارائه کرده اند. اولین قانون در مورد امضای الکترونیکی در "قانون یکسان معاملات الکترونیکی" ایالت "یوتا" در ایالات متحده تصویب شد. سنگاپور در سال ۱۹۹۸ میلادی در «قانون معاملات الکترونیک سنگاپور» و کانادا در «قانون تجارت الکترونیکی یکنواخت» در سال ۲۰۰۰ میلادی امضای

الکترونیکی را پذیرفته اند. حتی کشور انگلستان نیز که نظام حقوقی آن بر پایه حقوق عرفی (قانون عرف) بنا شده است نیز ناگزیر به وضع قانون در این زمینه بوده است. زیرا طبق دستورالعمل شماره ۳۱ / ۲۰۰۰ اتحادیه اروپا که بر برخی از جنبه های حقوقی تجارت الکترونیک نظارت می کند، کشورهای عضو موظف هستند که نظام های حقوقی خود ضمانت تشکیل قراردادها از طریق واسطه های الکترونیکی و سایر الزامات آن را داشته باشند. در همین راستا در سال ۲۰۰۲ انگلستان نیز «مقررات امضای الکترونیکی» را تصویب کرد. در فرانسه اگرچه قانون خاصی در این زمینه تصویب نشده است، اما در سال ۲۰۰۰ میلادی مطابق دستورالعمل مذکور ماده ۱۳۱۶ قانون مدنی فرانسه به منظور پذیرش امضای الکترونیکی و تشخیص اسناد الکترونیکی به عنوان مدرک معتبر اصلاح شده است.

در قوانین و سازمان‌های بین‌المللی، همانطور که قبلاً گفته شد، دستورالعمل‌ها و دستورالعمل‌های آنها مقرراتی را در مورد امضای الکترونیکی وضع کرده‌اند. از جمله می توان به دستورالعمل امضای الکترونیکی اتحادیه اروپا مصوب ۱۹۹۹ و همچنین قانون نمونه آنسیترال امضای الکترونیکی مصوب ۲۰۰۱ اشاره کرد. ایران نیز به صراحت امضای الکترونیکی را در قانون تجارت الکترونیک خود به رسمیت شناخته است. طبق ماده ۷ قانون فوق الذکر: «هرگاه قانون وجود امضا را ایجاب کند امضای الکترونیکی کافی است».

گسترش تجارت الکترونیک مستلزم تضمین اعتبار و امنیت آن توسط سیستم های حقوقی است. یکی از مهمترین ابزارهای اعتبارسنجی مبادلات الکترونیکی، پذیرش امضای الکترونیکی و تامین الزامات فنی آن است. در حال حاضر امضای الکترونیکی به عنوان یکی از اقدامات با آثار حقوقی مشابه امضای دستی مورد پذیرش قانونی نظام های حقوقی جهان (از جمله ایران) قرار گرفته و جایگاه خود را در اثبات دعوا تثبیت کرده است. امضای الکترونیکی از نظر آثار حقوقی با سایر امضاهای دست نویس تفاوتی ندارد، یعنی اگر امضای الکترونیکی دارای تمام شرایط فنی لازم و تضمین امنیت آن توسط علم کامپیوتر باشد، اعتبار و جایگاهی مشابه با دست نوشته خواهد داشت. امضاء در اثبات دعوی می توان آن را به عنوان دلیل در دادخواست یا دفاع ذکر کرد.

پیشنهادات

استراتژی توزیع شده دارای مزایای کاهش میزان ترافیک تحت نظارت و افزایش ظرفیت پردازش است. با این حال، پیاده سازی یک سیستم تشخیص حمله در مناطق مختلف شبکه به دلیل مشکلات مدیریتی چالش برانگیز است. به عنوان یک پیشنهاد می توان برای کارهای آتی موارد زیر را مد نظر قرار داد:

- از روش های توزیع شده برای تشخیص حمله در شبکه استفاده کرد.
- از تئوری های معماری مثل اندازه گیری قابلیت اطمینان سیستم های تشخیص در مواجهه با تهدیدات شدید استفاده کرد.
- می توان در کارهای آتی از ارزیابی مدل یادگیری عمیق و ایجاد پیش بینی ها استفاده کرد.

منابع و ماخذ

[1] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. Kwak, “The internet of things for health care: A comprehensive survey,” IEEE Access, vol. 3, pp. 678–708, 2015.
[2] V. A. Thakor, M. A. Razzaque, and M. R. A. Khandaker, “Lightweight cryptography algorithms for resource constrained IoT devices: A review, comparison and research opportunities,” IEEE Access, to appear, 2021.
[3] Zemrane, H.; Baddi, Y.; Hasbi, A. Comparison between IOT Protocols: ZigBee and WiFi using the OPNET Simulator. In Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications, Rabat, Morocco, 24–25 October 2018; pp. 1–6
[4] Ray, P.P.; Agarwal, S. Bluetooth 5 and Internet of Things: Potential and architecture. In Proceedings of the International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 3–5 October 2016; pp. 1461–1465.
[5] Wang, Y.; Chen, C.; Jiang, Q. Security Algorithm of Internet of Things based on ZigBee Protocol. Clust. Comput. 2019, 22, 14759–14766.
[6] Al Enany, M.O.; Harb, H.M.; Attiya, G. A Comparative Analysis of MQTT and IoT Application Protocols. In Proceedings of the International Conference on Electronic Engineering (ICEEM), Menouf, Egypt, 3–4 July 2021; pp. 1–6.
[7] Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A survey of LoRaWAN for IoT: From Technology to Application. Sensors 2018, 18, 3995.
[8] Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. 2017, 4, 1125–1142.
[9] Capkun, S.; Buttyan, L.; Hubaux, J.P. Self-organized Public-key Management for Mobile Ad hoc Networks. IEEE Trans. Mob. Comput. 2003, 2, 52–64
[10] Delavar, M.; Mirzakuchaki, S.; Ameri, M.H.; Mohajeri, J. PUF-based Solutions for Secure Communications in Advanced Metering Infrastructure (AMI). Int. J. Commun. Syst. 2017, 30, e3195.
[11] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135, pp. 62–75, Jun. 2019.
[12] A. Brock, D. Braden, and J. M. Day, “Holochain - A Framework For Distributed Applications,” US Patent US20 200 389 521A1, Dec., 2020. [Online]. Available:https://patents.google.com/patent/US20200389521A1/en
[13] Abbas Yazdinejad, Reza M. Parizi, Ali Dehghantanha, Qi Zhang, Kim-Kwang Raymond Choo. (2020). An Energy-efficient SDN Controller Architecture for IoT Networks with Blockchain-based Security. IEEE TRANSACTIONS ON SERVICES COMPUTING
[14] Al-Absi, M.A.; Al-Absi, A.A.; Fu, R.; Kim, K.H.; Lee, Y.S.; Lee, B.G.; Lee, S.G.; Lee, H.J. Secure and Efficient High Throughput Medium Access Control for Vehicular Ad-Hoc Network. Sensors 2021, 21, 4935.
[15] Meshram, C.; Ibrahim, R.W.; Deng, L.; Shende, S.W.; Meshram, S.G.; Barve, S.K. A Robust Smart Card and Remote User Password-based Authentication Protocol using Extended Chaotic Maps under Smart Cities Environment. Soft Comput. 2021, 25, 10037–10051.
[16] Srinivas, J.; Das, A.K.; Wazid, M.; Vasilakos, A.V. Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System. IEEE Internet Things J. 2021, 8, 7727–7744.
[17] Velliangiri, S.; Manoharn, R.; Ramachandran, S.; Venkatesan, K.; Rajasekar, V.; Karthikeyan, P.; Kumar, P.; Kumar, A.; Dhanabalan, S.S. An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography. IEEE Trans. Ind. Inform. 2022, 18, 6494–6502.
[18] Xu, X.; Zhao, H.; Yao, H.; Wang, S. A Blockchain-Enabled Energy-Efficient Data Collection System for UAV-Assisted IoT. IEEE Internet Things J. 2020, 8, 2431–2443.
[19] Vivekanandan, M.; Sastry, V.N.; Srinivasulu Reddy, U. BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology. Peer-to-Peer Netw. Appl. 2021, 14, 403–419.
[20] Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A.K. Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET. IEEE Trans. Netw. Sci. Eng. 2022, 9, 1346–1358.
[21] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, ‘‘Blockchain in healthcare

applications: Research challenges and opportunities,'' J. Netw. Comput. Appl., vol. 135, pp. 62–75, Jun. 2019.
[22] A. Brock, D. Braden, and J. M. Day, ''Holochain—A framework for distributed applications,'' U.S. Patent 2020 389 521 A1, Dec. 16, 2020. [Online]. Available: https://patents.google.com/patent/US20200389521A1/en
[23] K. Janjua, M. A. Shah, A. Almogren, H. A. Khattak, C. Maple, and I. U. Din, ''Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies,'' Electronics, vol. 9, no. 7, p. 1172, Jul. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/7/1172
[24] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, ''CT-GAN: Malicious tampering of 3D medical imagery using deep learning,'' in Proc. 28th USENIX Conf. Secur. Symp., 2019, pp. 461–478.
[25] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, ''Adversarial attacks on medical machine learning,'' Science, vol. 363, no. 6433, pp. 1287–1289, 2019.
[26] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin, ''A retrospective impact analysis of the WannaCry cyberattack on the NHS,'' NPJ Digit. Med., vol. 2, pp. 1–7, Oct. 2019.
[27] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, ''Bubbles of trust: A decentralized blockchain-based authentication system for IoT,'' Comput. Secur., vol. 78, pp. 126–142, Sep. 2018. [Online]. Available: ttp://www.sciencedirect.com/science/article/pii/S0167404818300890
[28] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K.-R. Choo, ''Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks,'' IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1120–1132, Apr. 2021.
[29] E. Harris-Braun, N. Luck, and A. Brock. (2018). Holochain: Scalable Agent-Centric Distributed Computing. [Online]. Available: https://github.com/Holochain/holochain-proto/blob/whitepaper/holochain.pdf
[30] R. T. Frahat, M. M. Monowar, and S. M. Buhari, ''Secure and scalable trust management model for IoT P2P network,'' in Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), May 2019, pp. 1–6.
[31] A. K. M. N. Islam, M. Mäntymäki, and M. Turunen, ''Why do blockchains split? An actor-network perspective on Bitcoin splits,'' Technol. Forecasting Social Change, vol. 148, Nov. 2019, Art. no. 119743. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0040162518319711
[32] What is HoloFuel Holo FAQ. Accessed: Jan. 27, 2022. [Online]. Available: https://holo.host/faq/what-is-holo-fuel/
[33] (Jul. 2019). Holo-Host/Holofuel-Model. Accessed: Jul. 24, 2018. [Online]. Available: https://github.com/Holo-Host/holofuel-model
[34] Holochain Think Outside the Blocks—Scalable Distributed Computing. Accessed: Jan. 27, 2022. [Online]. Available: https://holochain.org/
[35] The (Re) Distributive Enterprise. Accessed: Jan. 27, 2022. [Online]. Available: https://www.nextblockgroup.com/the-re-distributive-enterprise
[36] D. Diojdescu, ''The city as a collaborative commons. The state of the art of codesigning digital ledger technologies for commons and common good,'' Univ. Torino, Turin, Italy, Tech. Rep. UIA01-051, 2018.

Providing a new approach to send and store information in the Internet of Things for use in smart homes

Abstract

With the expansion of the Internet, the use of devices that are equipped with the Internet increased in homes, so that these devices received information from the environment with the help of their sensors, and after processing an event in the environment was executed or a decision was made. It led to the emergence of smart homes. But since these sensors had access to people's personal data, users' privacy was compromised. Therefore, various methods have been provided to create security in these networks. Many of these presented methods are based on traditional encryption, but these methods are not effective in distributed environments such as the Internet of Things. Therefore, in this research, we will present a Holochain-based solution to maintain data security and user privacy in Internet of Things networks.

Keywords: Sending, storing, information, Internet of things, smart homes.