مجله پژوهش های معاصر در علوم و تحقیقات
سال دوم، شماره ۲۰، اسفند ۱۳۹۹
ISSN: ۲۶۷۶-۵۷۶٤
www.jocrisar.ir

تحول در بخش امنیتی داده های ابری با کمک فناوری بلاکچین

سمیرا ندری پری [۱]

[۱] دانشجوی کارشناسی ارشد دانشگاه پیام نور تهران غرب

چکیده

رایانش ابری به عنوان یک فناوری کلیدی برای ارائه ی زیرساخت ها و نیازهای خدمات داده با هزینه ی کم و با حداقل تلاش و سطح بالای مقیاس پذیری ارائه شده است و از این رو در جنبه های مختلف صنعت فناوری اطلاعات به طور فراوان اجرا شده است. با توجه به رشد سریع رایانش ابری، هنوز هم نگرانی های امنیت اطلاعات به طور کامل رفع نشده است. نگرانی‌های امنیت اطلاعات تا حدودی مانع رشد رایانش ابری می شود که بایستی آن را حل کرد. این در حالیست که فناوری نوظهور بلاکچین به عنوان یک تکنولوژی کلیدی برای تامین امنیت به ویژه به لحاظ یکپارچگی، اصالت و محرمانه بودن ظهور کرده‌است. این مقاله به بررسی جنبه های مختلف امنیت در بلاکچین و محاسبات ابری و تجزیه و تحلیل بیشتر تحول در بخش امنیتی داده های ابری با کمک فناوری بلاکچین می پردازد.

واژه‌های کلیدی: رایانش ابری، بلاکچین، امنیت داده های ابری

مقدمه

امروزه محاسبات ابری[۱] یک امر بسیار مهم به حساب می آید که حتی استفاده از آن برای نسل آینده جهت انجام محاسبات پیش بینی شده است. در محیط محاسبات ابری، هم برنامه های کاربردی و هم منابع بر روی اینترنت به عنوان یک سرویس ارائه میشود. محیط ابری به عنوان محیطی از منابع سخت افزاری و نرم افزاری در یک مرکز داده است که سرویسهای متنوعی بر روی شبکه یا اینترنت برای برآوردن نیازهای کاربران ارائه میدهد[۱].

گسترش مدل ابری باعث شد که تجارت های مبتنی بر تکنولوژی، بیش از پیش تاثیرپذیر شوند. حرکت از سمت سرورها به سمت تفکر خدماتی، اهداف، طراحی و روش های پیاده سازی برنامه ها در دپارتمان های فناوری را تغییر داد. با این حال این پیشرفت ها مشکلات امنیتی جدیدی را به وجود آورده اند. امنیت داده به طور مداوم در فناوری اطلاعات به عنوان یک چالش مطرح بوده است و در محیط محاسبات ابری، اهمیت بسیار زیادی دارد چون داده در مکان های مختلفی حتی در سراسر جهان قرار گرفته است. حفاظت از امنیت[۲] و حریم خصوصی داده دو معیار مهم نگرانی های کاربران در فناوری ابری می باشد. مشکلات حفاظت و حریم خصوصی در معماری ابری شامل نرم افزار و سخت افزار می شود[۲].

در واقع محاسبات ابری به معنی ذخیره سازی و دسترسی به داده ها و برنامه ها روی بستر اینترنت به جای ذخیره‌سازی بر روی هارد کامپیوتر شخصی است. ابر فقط به عنوان یک استعاره برای اینترنت است. محاسبات ابری استخری از منابع محاسباتی/ذخیره سازی به اشتراک گذاشته شده است که میتواند براساس تقاضا و پیشنهادات پویا در دسترس کاربران قرار بگیرد. سرویسهای محاسبات ابر میتوانند در هر زمان و هر جایی در دسترس باشند. این خدمات توسط شرکتهای زیادی مانند گوگل (AWS) و (AZURA) مایکروسافت ارائه میشود[۳].

دلائل زیادی حاکی از این است که امنیت و اعتماد، بحرانی ترین مساله در سازمانها و موسسات مبتنی بر ابر می باشد. داده‌های ابری از این جهت که می توانند از دست بروند، لو رفته و یا مورد حمله قرار بگیرند، در معرض خطر بالایی قرار دارند. اما هیچ راه چاره ای برای بیرون آمدن از این وضعیت غیر استاندارد ندارند. کاربران ابر حتی از اینکه با چه کسانی سر و کار دارند و داده ها را با چه کسانی به اشتراک می گذارند، مطلع نیستند. همچنین شفافیت نیز در داده های ابری برای کاربران وجود ندارد[۴].

امنیت ابر که به عنوان امنیت رایانش ابری نیز شناخته می شود، شامل مجموعه ای از خط مشی ها، کنترلها، رویه ها و فناوری هایی است که برای محافظت از سیستم ها، داده ها و زیرساخت های مبتنی بر ابر با یکدیگر همکاری می کنند[۵].

با توجه به موارد گفته شده و ویژگی های بلاکچین[۳] می توان گفت که بلاکچین به عنوان یک فناوری نوظهور و جدید می‌تواند برای بالابردن اعتماد و تامین امنیت داده ها در سیستم های مبتنی بر ابر مورد استفاده قرار گیرد.

در ادامه توضیح کاملی از امنیت در داده های ابری گفته می شود. هم چنین ویژگی های بلاکچین و چالش های پیش روی سیستم های مبتنی بر ابر و در آخر، مورد استفاده ی بلاکچین اتریوم در سرویس ابری آورده می شود.

---

[۱] Cloud Computing

[۲] Security

[۳] Block Chain

۲. متن اصلی

امنیت به مجموعه ای از تدابیر، روشها و ابزارها برای جلوگیری از دسترسی و تغییرات غیر مجاز در نظامهـای رایانه ای و ارتباطی اطلاق میشود. وظیفه ی امنیت اطلاعات در رایانش ابری، اعمال مجموعه ای از فرایند های کسـب و کـار بـرای محافظـت از دارایی های اطلاعات است. موارد سه گانه حفظ درستی، محرمانگی و دسترس پذیری از مفاهیم اصلی امنیت اطلاعات است. امنیت در رایانش ابری زیر مجموعه ای از امنیت کامپیوتری، امنیت شبکه و در حالت کلی تر امنیت اطلاعات به حساب می آید. این مفهوم شامل مجموعه ای از سیاستها، تکنولوژیها و کنترلها جهت محافظت از داده ها، برنامه ها و زیرساختهای امنیتی در محاسبات ابری اسـت. امنیـت داده و حفـظ محرمانگی، دو عامل اساسی درباره فن آوری ابری است. مباحث امنیت و محرمانگی داده ها هم به سخت افزار و هم به نـرم افـزار در معمـاری ابری ارتباط دارد. حفاظت از حریم و افشای داده ها، برای سازمان هایی که قصد مهاجرت داده های خود به سمت سرویس های ابری را دارنـد از اهمیت شایانی برخوردار می باشد. رایانش ابری در واقع یک الگوی اصلی است که دسترسی به یک استخر مشترک از منابع محاسبات را برای کاربر ابری به صورت "بر حسب تقاضا " و یا "پرداخت بر اساس مصرف " فراهم می کند. ارائـه دهنـدگان خـدمات بایسـتی تضـمین کننـد زیرساخت آنها ایمن بوده و اپلیکیشن ها و داده های مشتری ایمن می باشند. این اقدام با اجرای سیاست ها و مکانیسم های امنیتی محقق می گردد و تهدیدات امنیتی مثل امنیت فیزیکی، امنیت اطلاعات، بازیابی داده ها، کنترل دسترسی کاربر توسط ارائـه دهنـده، وقفـه در سـرویس دهی، بازیابی داده ها و نیز ارائه ی راهکارهایی برای مقابله با هر یک است. رایانش ابری مزایای متعددی از نظر هزینه های سرمایه گذاری و صرفه جویی در هزینه های عملیاتی برای کاربران و سازمان ها ارائه می دهد. با وجود چنین مزایایی، موانعی وجود دارد که استفاده از رایانش ابری را محدود می کند. امنیت موضوع مهمی است که همیشه در نظر گرفته شده است. فقدان این ویژگی حیاتی منجر به تـاثیر منفـی ایـن الگـوی محاسباتی شده و در نتیجه ضررهای شخصی، حقوقی و مالی را در پـی دارد [۶] .

۲-۱ سرویس های ابری

سرویس های ابر به سه گروه تقسیم می شوند:

۱- زیرساخت به عنوان سرویس Infrastructure as a service(IaaS)

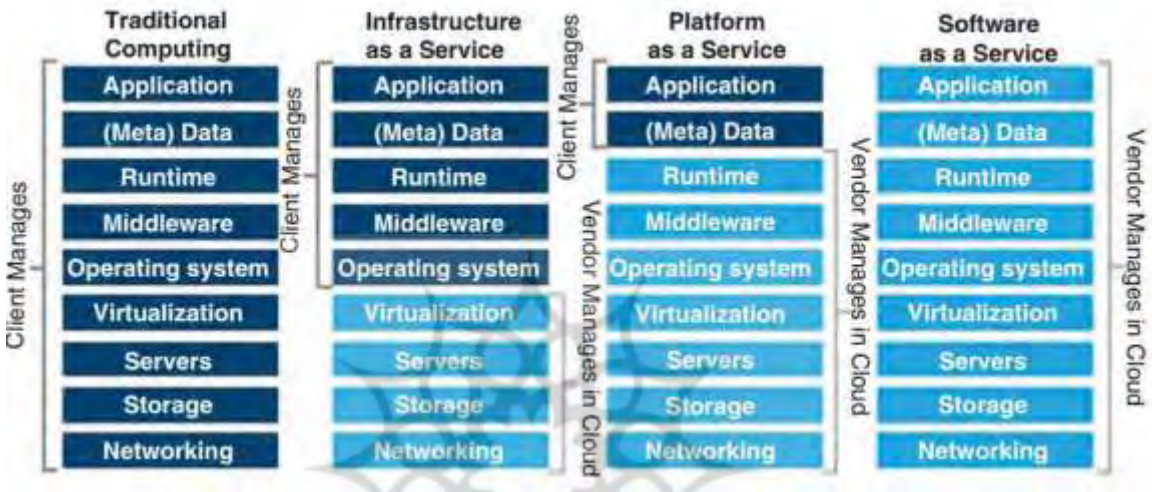
۲- سیستم عامل به عنوان سرویس platform as a service(PaaS)

۳- نرم افزار به عنوان سرویس Software as a service(SaaS)

IaaS مسئولیت مدیر سخت افزار، شبکه و دیگر سرویس ها را به عهده دارد. PaaS سیستم عامل و پلتفرم برنامه ها را حمایت می کند و SaaS همه چیز را حمایت می کند. سرویسهای ابر را می توان به سه صورت ارائه کرد: ابر خصوصی، ابر

عمومی و ابر ترکیبی[۳]. ابر عمومی میتواند در دسترس هر شخصی باشد، ابر خصوصی خدمات را به مجموعه کاربران دارای مجوز ارائه میدهد و ابر ترکیبی، ترکیبی از دو ابر عمومی و خصوصی است.

یک سرور ابر یک سرور منطقی باز است که یک میزبان میسازد و به عنوان یک ابر محاسباتی از طریق اینترنت ارائه میشود. سرورهای ابر یک عملکرد مشابه مانند قابلیتهای یک سرور معمولی ارائه میدهند. در هر حال آنها از راه دور و توسط یک ارائه دهنده خدمات ابر به یک ابر باز دسترسی دارند. یک سرور ابر به عنوان یک سرور مجازی خصوصی شناخته میشود. یک سرور ابر به عنوان یک زیرساختار است که به عنوان سرویس ارائه میشود (IaaS) و مدل اصلی سرویس ابر است. مقایسه محاسبات سنتی با مدلهای مختلف سرویس ابر در شکل ۱ نشان داده شده است [۷].



شکل ۱: مقایسه محاسبات سنتی با انواع مدل سرویس ابر[۷].

۲-۲ ضرورت سرویس ابر

برخی از الزامات مهم ابر که می تواند الگوهای طراحی مختلف ابر را تحت تاثیر قرار دهند در ادامه آورده شده اند:

۱. مقیاس پذیری:[۴] شبکه ابری با استفاده از سرویس های ابر، میلیون ها کاربر یا گره را اداره می کند. معماری سخت‌افزار از نظر اندازه انعطاف پذیر است.

۲. کشش:[۵] سیستم زنجیره بلوکی پرکارآمد می تواند حجم کار را با تخصیص و تخصیص زدایی منابع در یک مد برنامه ریزی شده اصلاح کند، به طوری که در هر نقطه از زمان تمام منابع موجود الزامات فعلی را تا بالاترین سطح امکان پذیر برآورده می‌کنند.

۳. حریم خصوصی:[۶] همه کاربران باید کنترل مؤثری بر داده هایشان داشته باشند و سیستم نیز باید از آن محافظت کند.

---

[۴] Scalability

[۵] Elasticity

[۶] Privacy

۴. منابع محاسباتی بی نهایت:[۷] سرویس های تأمین کننده از ابر نیاز به برنامه ریزی قبلی توسط کاربران ندارند.
۵. قیمت گذاری:[۸] کاربرد و خدمات مختلف در ابر در هزینه ها متفاوت بوده و پرداخت بستگی به بهره برداری از منابع دارد.
۶. بهره برداری:[۹] منابع، با اجازه دادن به بهترین بهره برداری ممکن، می توانند به طور موثر دوباره پیکربندی شوند.
۷. بهره وری هزینه:[۱۰] خدمات ابر در سراسر اینترنت بر اساس نیاز کاربر نهایی است. این کار هزینه کلی نگهداری و عملیات نرم افزار را کاهش خواهد داد.
۸. عملکرد:[۱۱] به طور کلی، ارزیابی ها از نظر کارایی برنامه ها و عملکردهایی که بر روی سیستم ابری در حال اجرا هستند، کمی می شوند.
۹. انعطاف پذیری:[۱۲] قابلیت به اشتراک گذاری فایل ها یا خدمات از طریق اینترنت تحت انعطاف پذیری قرار می‌گیرد. ابر انعطاف پذیری را تا حد بیشتری برای کاربران فراهم می کند[٤].

۳-۲ مشکلات سرویس های ابر

با توجه به مزایای زیادی که برای سرویسهای ابر در نظر گرفته شده است، این سیستم ها مشکلات زیادی دارند. بر اساس یک نظرسنجی که توسط موسسه گارتنر انجام شده: بیش از ۷۲ ٪ از کارکنان فنی تصور میکنند که دلیل اصلی این که سرویسهای محاسبات ابری مورد استفاده قرار نگرفته است امنیت اطلاعات و مسائل مربوط به حفظ حریم خصوصی است[8].

برخی از ریسکهای این حوزه در ادامه بیان شده است:

۱. قابلیت اعتماد به اینترنت: یک مسئله اصلی در اجرای ابر، اینترنت است. سرعت اینترنت عامل اصلی در ارائه خدمات توسط ارائه دهندگان سرویسهای ابر است و ارتباط سرویسهای تجاری و مالی با پایین بودن سرعت اینترنت ممکن است دچار مشکل شدیدی شوند.
۲. وابستگی به تامین کننده: مشتریان به صورت روزانه به ارائه دهندگان سرویسهای فناوری اطلاعات وابسته میشوند. پشتیبانی و نگهداری عواملی است که مشتری را جذب میکند و استفاده از منابع را به صورت گسترده ای افزایش میدهد و بیشتر به ارائه دهنده وابسته میگردد از این رو باید مسائل قانونی و نظم دهنده در بحث ابر مورد توجه قرار گیرد.
۳. محل قرارگیری اطلاعات: وقتی اطلاعات بر روی ابر انتقال داده میشود، ارائه دهنده آن را روی اینترنت بارگذاری میکند و اگر محل قرارگیری این داده ها مشخص نشود، کاربر اطلاعات خود را از دست میدهد و متضرر خواهد شد.
۴. دسترسی کاربران: کنترل دسترسی یک نگرانی بزرگ در سرویسهای ابر است تا داده ها مورد حمله ی داخلی از سوی ارائه دهندگان سرویس ابر قرار نگیرند.

---

[۷] Infinite Computing Resources

[۸] Pricing

[۹] Utilization

[۱۰] Cost Efficiency

[۱۱] Performance

[۱۲] Flexibility

۵. رعایت مقررات: مسئولیت اطمینان از امنیت و یکپارچگی داده ها بر روی کاربر ابر است؛ هر چند که توسط ارائه‌دهندگان ارائه میشود. از این رو مشتری باید اطمینان حاصل کند که ارائه دهندگان قادر به رعایت مقررات و پیگرد قانونی خطرات هستند.

۶. تفکیک داده: وقتی که کاربر اطلاعات را در ابر ذخیره میکند، این ریسک بوجود میآید که اطلاعات کاربر در میان داده های مشتری دیگر ذخیره شود. ممکن است که رمزگذاری در هنگام اجرا، جابه جایی و حتی استراحت صورت گیرد و هر چند رمزگذاری موثر است، ولی در دسترس بودن یک خطر است[۸].

۷. بازیابی: بازیابی یک عامل کلیدی در استفاده از سرویس ابر است. شاید کاربران بدانند اطلاعات آنها کجا قرار دارد، اما هیچوقت نمیدانند که از نظر فیزیکی کجا قرار دارد و در برابر تهدیداتی مانند آتش، سیل، بلایای طبیعی و غیره قرار دارد و از این رو امکان آسیب دیدن محل قرارگیری فیزیکی داده ها وجود دارد.

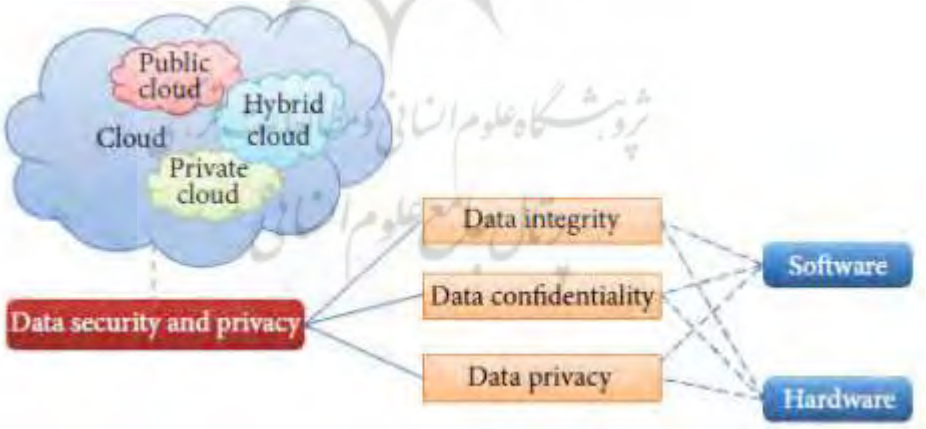
۸. پشتیبانی تحقیقاتی: در صورت نقض امنیتی دسترسی به داده ها معمولا دشوار است؛ زیرا مشتریان چندگانه معمولا در کنار هم قرار دارند و اطلاعات مشتری ممکن است در سرورهای مختلف و مراکز مختلف پخش شود؛ بنابراین انجام تحقیقات دشوار است.

۹. ماندگاری طولانی مدت: ماندگاری اطلاعات یک ریسک است که مشتری باید با آن روبرو شود. ارائه دهندگان میتوانند از این تجارت خارج شوند و مشتری نیز باید آن را ترک کند.

۱۰. دزدی اکانت یا سرویس: کاربران بوسیله پسورد به اکانت خود دسترسی دارند، بنابراین گذرواژه ها سوء استفاده میشوند. زمانی که اکانت به سرقت میرود، کاربران غیرمجاز میتوانند به اطلاعات مشتریان دسترسی داشته باشند[۸].

۱۱. انتقال داده ها: یک مشکل قابل توجه در هنگام انتقال داده از یک مکان به مکان دیگر بوجود میآید. تمام اطلاعات در ابتدا با یک سازمان خاص در یک مکان خاص ذخیره میشوند. اما برخی از تامین کنندگان ممکن است موقعیت اطلاعات را از یک مکان به مکان دیگر به دلیل شرایط اجتناب ناپذیر تغییر دهند. اما ممکن است محل داده ها در قرارداد خودشان مشخص شده باشدکه این باعث خطر در حرکت داده ها میشود[۸].

شکل ۲، نمایی از ساختار امنیت داده در محاسبات ابری را نمایش می دهد[۲].



شکل ۲: ساختار امنیت داده در محاسبات ابری[۲]

۲-۳-۱ چالش های امنیتی

در محاسبات ابری، کاربران از مکان دقیق اطلاعات حساس خود مطلع نیستند، زیـرا ارائـه دهنـدگان سـرویس ابر مراکز داده در مکان های توزیع شده جغرافیایی نگهداری می شوند که منجر به چندین چالش و تهدید امنیتی مـی شـود. در روش‌های سنتی: تکنیک های امنیتی مانند فایروال ها، نرم افزارهای ضد ویروس مبتنی بـر میزبـان و سیسـتم هـای تشـخیص نفـوذ و سیستم های مجازی به علت گسترش سریع تهدیدات از طریق محیط مجازی در امنیت کافی نیستند.

۱. تهدیدها و خطرات محاسبات ابر

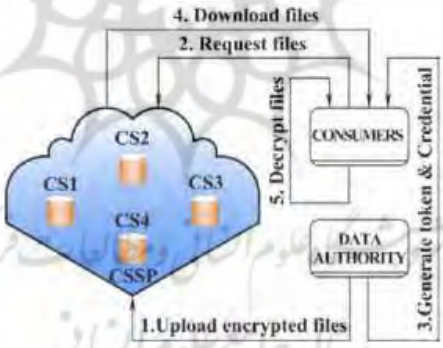
در میان تمام خطرات و تهدیدهای شناسایی شده برای سرویس ابر، نقض داده ها (اطلاعات) به عنوان بالاترین مسـئله ی امنیت که نیاز به آدرس دارند، در نظر گرفته شده است.

۲. امنیت در رمزنگاری

اسـتفاده از ابرهـای عمـومی منجر به چندین خطر امنیتی می شود. محرمانه بودن و یکپارچگی داده ها یکی از بزرگترین خطرات ناشی از نگرانی های جدی است. شکل۳ معماری یک ابر رمزگذاری شده را که توسط کامارا در سال ۲۰۱۰ ارائه شده است را به وضوح نشان می‌دهد این شـامل سه پایه اساسی می شود:

اداره داده (صاحب داده ها) مصرف کننده داده هـا و ارائـه دهنـده سـرویس[۱۳](CSP) ، مجـوز داده و فایـل هـای رمزگذاری شده را بارگذاری کرده و مصرف کننده یا کاربر از ابر دسترسی به فایل ها را تأیید می کند. سپس فایل مورد درخواست را می توان با استفاده از نشانه ها و اعتبار های مناسب دانلود کرد. اینها توسط اشخاص صورت میگیرد.

چالش های مختلف امنیتی در سطح ارتباطات، محاسبات و موافقت نامه های سطح خدمات[۱۴]هستند [۶].



شکل۳- معماری رمزنگاری ابر[۶]

شکل ۴ درخت امنیتی و الزامات امنیتی اولیه را نشان می دهد. درست همانطور که امن بودن ریشه ی درخت در خاک منافع حاصل از آن را تضمین می کند، چالش های مشخص شده در ریشه نیز بایستی به درستی حل شوند تا یکسری مسائل تضمین شوند. پروتکل های (TLS[۱۵]) و (SSL[۱۶]) که در لایه ی حمل و نقل هستند و به ترتیب، امنیت لایه و سوکت امن را

---

[۱۳] Cloud Service Provider

[۱۴] *Service-level agreement*

[۱۵] *Transport Layer Security*

[۱۶] Secure Socket Layer

نشان می دهند، برای انتقال امن داده های نشان داده شده با تنه ی درخت نشان داده می شود. چالش های امنیتی مشخص شده در درخت امنیتی بر مبنای سه نهاد اساسی طبقه بندی شده اند کـه در ۴ شـکل نشـان داده شده اند. این سه سطح عبارتند از: ارتباط، محاسبات و توافق سطح خدمات. همانطور که قبلا بیان شده است، نمودار شـکل ۵ طبقه بندی سه سطح چالش امنیتی را مشخص می‌کند. مسائل امنیتی در هر سطح نیز با وضوح بیشتر نشان داده شـده اسـت. در ادامه طبقه بندی مسائل امنیتی مربوط به سه سطح عنوان شده آورده می شود.

۱-سطح ارتباطات

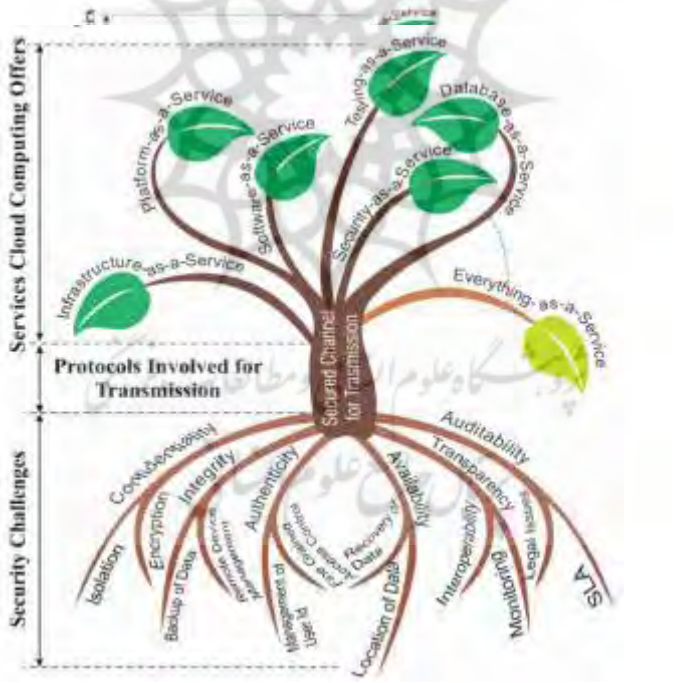
مسائل مربوط به سطح ارتباط به عنوان یک نتیجه از به اشتراک گذاری منابع مشترک، زیرساخت ها و غیره، در میان ماشین‌های مجازی ایجاد می شود. امنیت در برابر حملات شناسایی شده بر اساس سطح ارتباطات در ادامه آورده شده اند:

الف) امنیت در سطح شبکه

ویژگی های کلیدی که باید در سطح شبکه مورد توجه قرار گیرند، محرمانه بودن و یکپارچگی داده ها هستند. در حقیقت تمامی مسائل مربـوط بـه امنیت در سطح شبکه هستند.

ب) امنیت در سطح برنامه

برنامه های کاربردی برای جلوگیری از هدف مهاجمان برای به دست گرفتن کنترل آنها با تـلاش خود برای تغییر فرصت ها نیاز به امنیت دارد. شکل ۴ نمایی از درخت امنیتی است[۶].



شکل ۴- درخت امنیتی[۶]

شکل ۵- طبقه بندی امنیت موضوع[۶]

ج) امنیت در سطح میزبان

تهدید میزبان که در برنامه های کاربردی کار می کنند در سطح سیستم عامل قرار می گیرند. تهدیدات اصلی میزبان عبارتند از

•ویروس ها، اسب های تروجان و کرم ها؛

•پروفایل

•شکسته شدن رمز عبور؛

•ردیابی؛

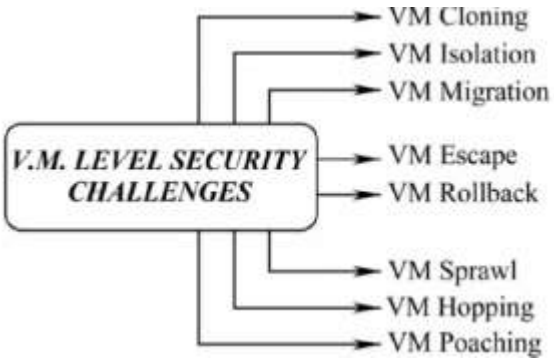
•خود داری از خدمات؛

•دسترسی غیرمجاز.

۲-سطح محاسباتی

پیاده سازی مفهوم مجازی سازی در ابر یکی از بزرگترین چالش های محاسباتی است.

برخی از کلاس های مشترک مجازی سازی، مجازی سازی برنامه، مجازی سازی دسک تاپ، مجازی سازی شبکه، سرور و مجازی سازی ماشین هستند. شکل ۶ چالش های امنیتی این سطح را نشان می دهد[۶].



شکل ۶ – چالش های امنیتی سطح VM [۶]

۳-توافقات سطح سرویس(SLA)

خدمات توسط ارائه دهندگان، به مصرف کنندگان با SLA مناسب ارائه می شود. نهادهـای اساسـی رمزگـذاری ابـر مسـئولیت حفظ SLA را دارند. تامین منابع در هر زمان بستگی به پهنای باند مورد نیاز، CPU، حافظه و مدیریت کلید در میان دیگران دارد. استفاده از SLA کمک می کند تا کیفیت خدمات در سطح قابل قبولی ارائه شود. SLA شامل تعریف قرارداد، مذاکره، نظارت و اجرای آن است. تعریـف قـرارداد و مـذاکره، منافع و مسئولیت هر طرف را مشخص می کند. نظارت و اجرای اعتماد بین مصرف کننده و ارائه کننده ایجـاد مـی کنـد[۶].

۲-۴ بلاکچین

تکنولوژی بلاکچین بوسیله ی بیت کوین به جهان معرفی شد. بیت کوین یک ارز دیجیتال رمزنگاری شده ی همتا به همتا است که ناکاماتو در سال ۲۰۰۸ آن را توسعه داد. در سیستم بیت کوین بلاکچین سیستم پرداخت را پشتیبانی می کند و کامل کننده ی ارز دیجیتال است. همچنین ایمن و توزیع شده هستند[۹].

فناوری بلاکچین نرم افزاری با منبع باز[۷]است که ایجاد یک پایگاه داده عمومی بزرگ، غیرمتمرکز و امن که حاوی سوابق مرتب شده و سازماندهی شده در ساختار یک بلوک است را میسر میکند. شبکه بلاکچین را میتوان به عنوان ستونی عظیم از اطلاعات در بلوکهایی که در طول زمان ایجاد میشوند، در نظر گرفت که کار تبادل اطلاعات بین کاربران (تراکنشها) را در یک دفتر کل عمومی مدیریت میکند. کاربران از یک زیرساخت راهنمای همگانی (PKI[۸]) استفاده می کنند که شامل دو راهنما است: عمومی و خصوصی. راهنمای خصوصی آن چیزی است که شناسایی هویت کاربر در شبکه را میسر میکند، در حالی که راهنمای عمومی حاوی آدرسی است که کاربر را به شناسه ورودی برای دسترسی به داده های بلاکچین، مرتبط میکند. از طریق راهنمای خصوصی میتوان یک یا چند راهنمای عمومی را بدست آورد، اما از طریق راهنمای عمومی نمیتوان به راهنمای خصوصی دست یافت. این امر از طریق عملیات رمزنگاری نامتقارن بر اساس یک منحنی بیضوی بدست می آید و این یکی از جنبه هایی است که به سیستم امنیت میبخشد. تراکنشها عبارتند از راهنمای عمومی فرستنده و راهنمای عمومی دریافت کننده و همچنین مقدار اطلاعاتی که منتقل میشود. این تراکنشها در یک چارچوب زمانی متغیر(۱۰ دقیقه) در مورد بیت کوین انجام میگیرد و همراه با تمام تراکنشهای ساخته شده دیگر، بلوکی جدید نوشته میشود[۱۰].

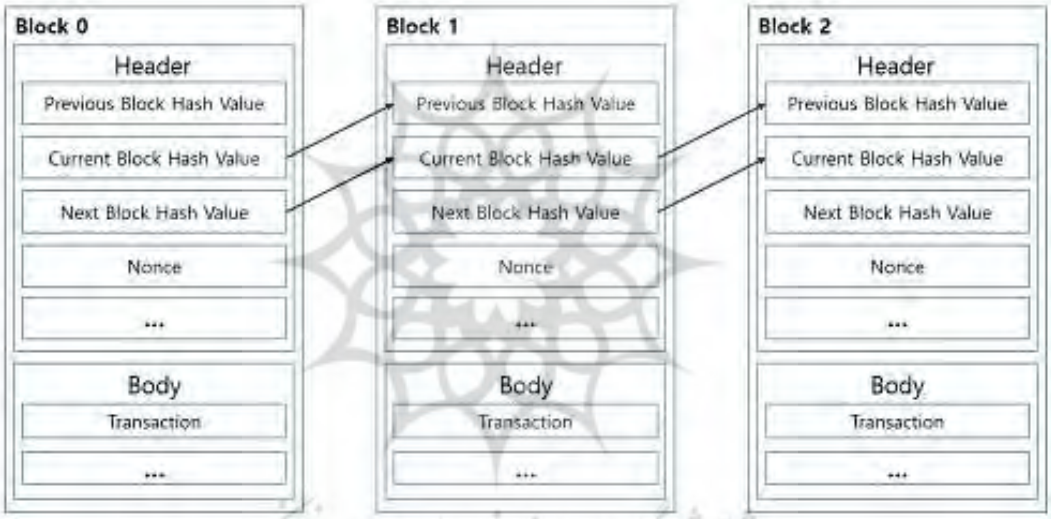
بلوک جدید با بلوک درج شده قبل از خود لینک میشود و این فرآیندی است که بایستی پشت سر هم تکرار شود. هنگامی که نوشتن شش بلوک پایان می‌یابد، از آن پس هر تراکنشی برای هر منظور و مقصودی که به وجود آید، تراکنشی دائمی و پایدار خواهد بود. بنابراین هر بلوک حاوی اطلاعاتی درباره تمام تراکنشهایی است که به وجود آمده اند و پیشینه آن به زمان پیدایش این زنجیره برمیگردد و این یکی از جنبه هایی است که باعث ثبات اطلاعات موجود میشود. بلوکهای حاوی اطلاعات با استفاده از کامپیوترهای خود اعضای شبکه بلاکچین که هم کاربر و هم نگهدارنده کل سیستم هستند به صورت دیجیتالی در بین گره‌ها (کاربران) ذخیره میشوند و داده های مربوط به تمام تراکنشهای انجام گرفته در زمان حال و گذشته در بین گره ها

---

[۷] *Open Source*

[۸] *Public Key Infrastructure*

ذخیره میشود[۱۱]. بلاکچین توسط سیستمی از گره ها (کاربرها) نگهداری میشود که به آن ماینینگ (استخراج) میگویند. در ماینینگ، گره ها با یکدیگر رقابت میکنند تا یک مشکل ریاضیاتی را توسط تکنیک هش حل کنند و راه حل آن در متوسطی از زمانی ثابت (در مورد بیت کوین، در ۱۰ دقیقه) به دست میآید. گره ای (کاربری) که این مشکل را در زمان کمتری حل کند، اثبات کار (work-of-proof) میشود و در واقع همان کسی خواهد بود که بلوک بعدی زنجیره را برای کسب پاداش، خواهد نوشت. این همان سیستمی است که در شبکه توسط گره ها برای انجام و تأیید تراکنشها مورد استفاده قرار میگیرد و در قبال انجام این کار، اجرتی کوچک نیز از کاربر دریافت میکند. دستیابی به اثبات کار، نیاز به مقدار زیادی تلاش محاسباتی و مصرف بالایی از انرژی دارد و این یکی از عواملی است که سیستم را ارزشمند میکند. یکی از مزایای اصلی سیستم گواهی بلاکچین این است که توسط خود کاربران به شکلی نامتمرکز نگهداری میشود، بنابراین نیازی به سازمانی برای ذخیره سازی ندارد. بلاکچین به شکل ساخت یافته اطلاعات را به صورت یک پایگاه داده توزیع شده در خود ذخیره می کند. در شکل ۷ ساختار اتصالات بلاکچین نمایش داده شده است. هر بلوک ساختاری متشکل از هدر و بدنه دارد و داده های بلوک ها به کمک روش فهرست[۱۹]جستجو می شوند. اگرچه بلوک حاوی هش بلوک بعدی نیست، اما به عنوان تمرین به آن اضافه می شود[۱۲] .



شکل۷: ساختار اتصالات بلاکچین[۱۲]

۱-۴-۲ انواع بلاکچین

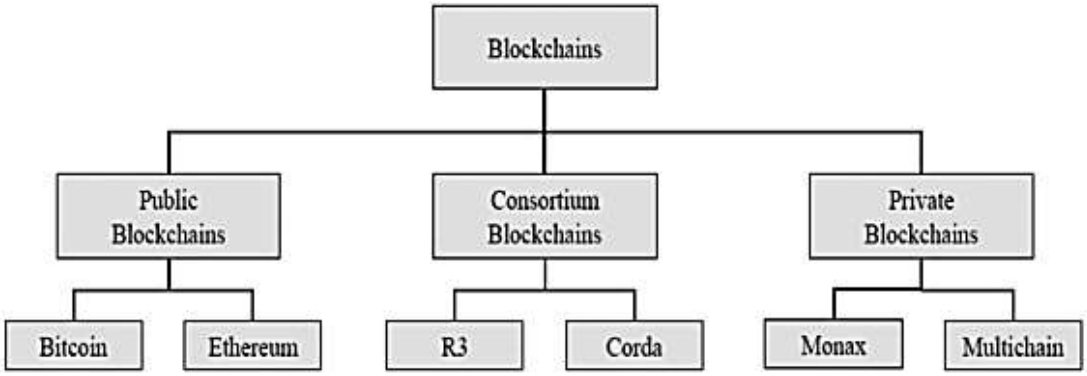
بلاکچین سه نوع مختلف را ارائه میدهد مانند عمومی ، خصوصی و کنسرسیوم که در شکل ۸ نشان داده شده است.

عمومی: یک بلاکچین عمومی یک دفتر کل قابل مشاهده برای هر نفر در اینترنت است و هر کس میتواند آن را تایید کند و یک بلوک به بلاکچین اضافه کند.

خصوصی : بلاکچین خصوصی فقط به افراد خاص در سازمان اجازه تایید و اضافه کردن بلوک را میدهد اما هر شخص در اینترنت میتواند به طور کلی مشاهده کند.

[۱۹] Indexed method

کنسرسیوم: در اینجا فقط یک گروه از سازمانها (مانند بانک) میتوانند یک تراکنش را تایید یا اضافه کنند، اما دفتر کل میتواند برای گروه انتخابی باز یا محرمانه باشد.



شکل۸: انواع مختلف بلاکچین[۳]

۲-۵ ضرورت استفاده از بلاکچین

بلاکچین یک تکنولوژی در پایگاه داده جهانی است که هر کسی هر کجا با اتصال به اینترنت میتواند از آن استفاده کند. برخلاف یک پایگاه داده سنتی که متعلق به یک مرکز است مانند بانکها و دولت، بلاکچین به هیچ کس تعلق ندارد. بلاکچین اطلاعات را در کل شبکه و میان گره ها ذخیره میکند. فقط غیرمتمرکز نمیکند بلکه آنها را توزیع هم میکند. پس تقلب در سیستم با اسناد جعلی، معاملات و دیگر اطلاعات غیرممکن خواهد شد. هر گره در شبکه میتواند یک کپی محلی از سیستم بلاکچین را که به طور دوره ای آپدیت میشود ذخیره کند تا گره ها یک مقدار هماهنگ داشته باشند. یک بلاکچین یک محاسبات توزیع شده و پلتفرم ذخیره سازی اطلاعات است که چندین گره را که به هم اعتماد ندارند را قادر میسازد تا یک تصمیم بگیرند. ایراد سیستم مرکزی در این است که یک نقطه شکست دارد. در سیستم غیرمتمرکز چندین نقطه ی مختصات وجود دارد که بر یک نقطه شکست غلبه میکنند. هر کاربر نماینده یک نقطه ی اتصال در روش توزیع شده است هر گره شامل یک کپی از لیست بلاکچین است که به طور منظم آپدیت میشود[۳].

۲-۶ چالش های بلاکچین

مقاله ای در سال ۲۰۱۹ توسط مهنتا[۱] و همکاران ارائه شد که در آن در مورد چالشهای اجرای بلاکچین و ارتباط آن با مسائل امنیت و حریم خصوصی بحث میکند و مروری سیستماتیک بر مقاله های حوزه های مختلف بلاکچین دارد[۷]. همچنین در کار

[۱] Mohanta

انجام شده [۴] چندین چالش امنیتی در مورد امنیت بلاکچین گزارش شده است که عبارتند از: توافقنامه Blockchain[۲۱] ، امنیت معاملات[۲۲]، امنیت کیف پول[۲۳] و امنیت نرم افزار.[۲۴]

۲-۷ مورد استفاده از بلاکچین در سیستم های ابری

همانطور که گفته شد، امروزه حجمه ی روزافزونی از داده ها، به خدمات ابری، برون سپاری می شوند و نیاز به محاسبات ابری روز به روز در حال افزایش است[۱۳]. به منظور تضمین امنیت و محرمانگی داده، این داده ها اغلب بر روی سرورهای ابری، در حالت رمز-متن ذخیره سازی می شوند. هنگامی که یک کاربر، درخواست دستیابی به داده های رمزنگاری شده را دارد، یک کلید دست یابی که توسط شخص ثالث توزیع می شود، مورد نیاز است. با این وجود در صورتی که شخص ثالث، مطمئن نباشد، امنیت سیستم، مورد تهدید قرار می گیرد. جهت رویارویی با این مساله، در مقاله در دست، یک چارچوب ذخیره سازی ابری جدید امن، با کنترل دسترسی، از طریق استفاده از فناوری بلاک چین اتریوم[۲۵] پیشنهاد می کنیم. طرح جدید ما ترکیبی از رمزنگاری مبتنی بر خصیصه سیاست رمز-متن و بلاک چین اتریوم (CP-ABE) می باشد. چارچوب ذخیره سازی ابری، پیشنهادی غیرمتمرکز بوده است یعنی هیچ گونه شخص ثالث مطمئنی، در سیستم وجود ندارد.

طرح ما سه ویژگی اصلی دارد:

در وهله اول، به دلیل اینکه فعالیت بلاک چین اتریوم، استفاده شده است، مالک داده می تواند رمز-متن داده ها را از طریق قراردادهای هوشمند، در یک شبکه بلاک چین ذخیره سازی کند. در وهله دوم، مالک داده می تواند بازه های دسترسی معتبر، برای استفاده از داده را به گونه ای قرار دهد که رمز-متن را تنها بتوان در طول این بازه های دسترسی معتبر، رمزگشایی کرد. در نهایت به دلیل اینکه خلق و ایراد هر قرارداد هوشمند را می توان در بلاک چین، ذخیره سازی کرد، بنابراین کاربرد ردیابی آن، حاصل می شود. تحلیل امنیت و آزمایشات نشان می دهد که طرح ما اِعمال پذیر است.

در این طرح، از قرارداد هوشمند[۲۶] برای ذخیره اطلاعات مربوط به پرونده رمزگذاری شده استفاده خواهیم کرد. از همه مهمتر، کاربران داده و دارندگان داده از قراردادهای هوشمند اتریوم[۲۷] جهت ذخیره و بازیابی داده های متن-رمز برای اجرای الگوریتم‌های رمزگذاری و رمزگشایی استفاده می کنند. هر تماس قراردادی در بلاکچین ثبت می شود[۹].

---

[۲۱] Blockchain Agreement

[۲۲] Transactions Security

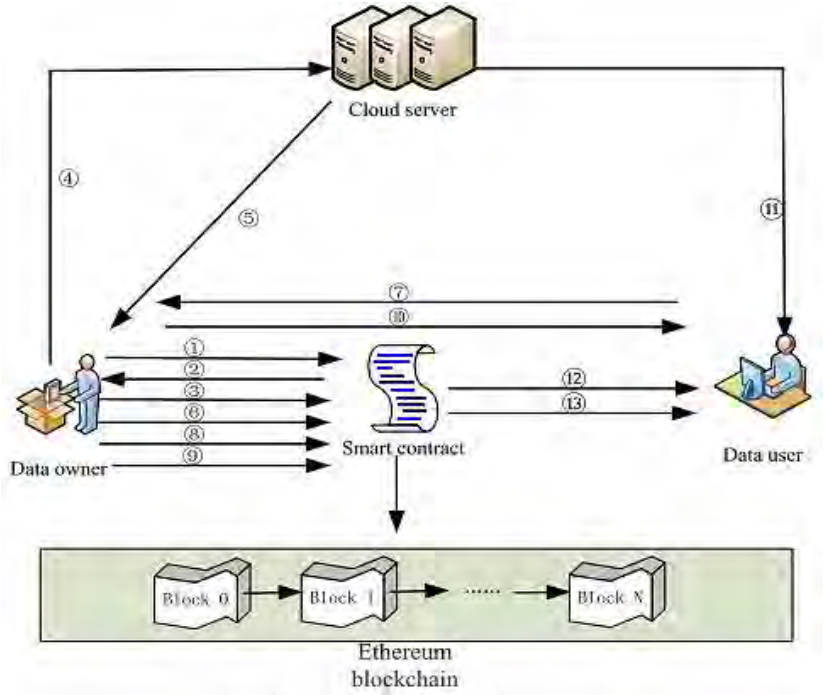
[۲۳] Wallet Security

[۲۴] Software Security

[۲۵] Ethereum

[۲۶] Smart Contract

[۲۷] Ethereum



شکل ۹– مدل سیستم[۹]

بنابراین، اطلاعات منتقل شده بین کاربران داده و صاحبان داده ها دستکاری نمی شوند.

چهار موجودیت در طرح وجود دارد، یعنی سرور ابر، بلاک چین اتریوم، دارنده داده و کاربر داده.

سرور ابری: مسئول ذخیره فایلهای رمزگذاری شده بارگذاری شده توسط دارندگان داده ها است.

بلاکچین اتریوم: قراردادهای هوشمند را در اتریوم قرار می دهد، قراردادهای هوشمندی که مربوط به رابط های ذخیره داده و دریافت داده هستند.

دارنده داده[۲۸](DO): مسئول ایجاد و استقرار قراردادهای هوشمند، بارگذاری پرونده های رمزگذاری شده، تعریف سیاست‌های کنترل دسترسی، اختصاص مجموعه ویژگی ها و تعیین دوره های دسترسی معتبر به کاربران داده است.

کاربر داده[۲۹](DU): دسترسی به یک فایل رمزگذاری شده ی ذخیره شده در سرور ابری را دارد و هنگامی که مجموعه ویژگی‌های آن ساختار جاسازی شده در متن رمز داده شده را راضی می کند، می تواند رمز دریافت شده را رمزگشایی کند تا کلید محتوای رمزگشایی فایل رمزگذاری شده را بدست آورد.

مراحل اجرای فازهای الگوریتم مربوط به شکل فوق همراه با نتایج بدست آمده و تجزیه و تحلیل آنها در کار [۹] آورده شده است که نشان دهنده ی تاثیرگذاری مطلوب بلاکچین بر روی ابر می باشد. در ادامه موارد استفاده ی بلاکچین برای امنیت ابر توضیح داده می شود.

الف) دفترچه باز[۳۰]

[۲۸] Data Owner(DO)

[۲۹] Data User(DU)

[۳۰] Open Ledger

برای هر کاربر، فضای ذخیره سازی ابری که توسط بلاکچین استفاده می شود قابل دسترسی و باز است و کاربر می تواند انواع خدمات ارائه شده توسط ابر از جمله توافق نامه های سطح خدمات (SLAs) را مشاهده کند.

ب) دفتر توزیع شده[۳۱]

همه نسخه های دفتر به خوبی همگام سازی شده اند و همه کاربران ابر می توانند نسخه یکسان / نسخه دفتر را مشاهده کنند. این دفتر شامل سابقه خدمات مورد استفاده توسط هر کاربر ابری و به طور کلی شامل استفاده از خدمات، خط مشی‌ها و SLA ها است. این همان شفافیت است.

ج) قرارداد هوشمند غیر متمرکز[۳۲]

در بلاکچین یک قرارداد هوشمند مدت دار، نرم افزاری است که شرایط و ضوابط قرارداد را حفظ، تأیید و اجرا می کند. بلاکچین همراه با فناوری های قرارداد هوشمند اعتماد و شفافیت بیشتری را فراهم می‌کند. قراردادهای هوشمند در بلاکچین ذخیره شده اند که همه کاربران ابر هم نسخه ای از آن را دارند. تمام معاملات قراردادی به ترتیب زمانی در بلاکچین برای دسترسی در آینده همراه با سیر حسابرسی کامل وقایع ذخیره می شوند. اگر هر طرفی بخواهد قراردادی را در مورد بلاکچین تغییر دهد، سایر کاربران ابر می توانند آن را شناسایی و از آن جلوگیری کنند.

۴. نتیجه گیری

در این مقاله، ساختار کلی سیستم ابر و بلاکچین مورد بحث قرار گرفته است. بعلاوه، ویژگیهای سرویس ابر، ضرورت استفاده از آن و چالش های امنیت آن آورده شده است. همچنین در مورد بلاکچین نیز ضرورت استفاده از آن و چالش ها و مزایای آن بررسی شده است. بر اساس این تجزیه و تحلیل، مشخص شده است که بلاکچین می تواند یک ابزار مناسب و قدرتمند برای تأمین امنیت در محیط محاسبات ابری باشد. علاوه بر این، این مقاله پیاده سازی های مختلف بلاکچین موجود برای امنیت ابر را بررسی کرد. امید است با توجه به نیاز به رشد سرویسهای ابری بتوان بلاکچین را در تمامی سرویسهای ابری کاربردی کرد و از ویژگی امنیت بالای بلاکچین در تمامی سرویس های ابری بهره برد.

مراجع

1. Leavitt, N. (2009),"*Is cloud computing really ready for prime time?*", Computer, vol. 42, no. 1, pp. 15– 25.

۲.ریاحی، ا. (۱۳۹۵). "ارائه ی راهکارهای امنیت داده در محاسبات ابری"، دومین کنفرانس بین المللی مدیریت و فناوری اطلاعات و ارتباطات.

۳. جوادی، ج و خانجانی، ع. (۱۳۹۸). "مقایسه بلاکچین در اینترنت اشیا و محاسبات ابری"، اولین کنفرانس بین المللی توانمندسازی کسب و کارهای فناورانه و راهکارهای پیشرفت در تکنولوژی و مهندسی، تهران، ۲۹ آذر.

[۳۱] Distributed Ledger

[۳۲] Decentralized Smart Contract

۴. Gupta, A. and Tabrez, Sh. And Alam, Sh. And Shuaib, M. (2019). "*Cloud Computing Security using Blockchain*", JETIR June, Volume 6, Issue 6.

۵. نخعی، م. (۱۳۹۹). " شرحی بر امنیت سیستم ابری" اولین کنفرانس علمی پژوهشی مکانیک، برق،کامپیوتر و علوم مهندسی، باکو، آذربایجان، ۱۳ شهریور.

۶. سلیقه، ف و دشتی، س. ا. (۱۳۹۸). " بررسی مسائل امنیتی و چالش های جدید رایانش ابری"، هفتمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، موسسه کومه علم آوران دانش، بابل، مرداد.

۷.Aslanpour, M.S. and Mehta, H. and Stankovski, V. and Garraghan, P. and Mishra, S. and Kaila, S. and Sehgal, B. and Pervaiz, H. and Jain, U. and Singh, M. and Smirnova, D. and Tuli,Sh. And Lindsay, D. Vijay Singh, K. Singh, I. and Xu, M. and Tuli, Sh. And Singh Gill, S. (2019). "*Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution*", Vision, doi: https://doi.org/10.1016/j.iot.2019.100118 Trends and Open Challenges, Internet of Things.

8. Kumar, M.and Hukam, Kh. Saini, Ch. (2019). "*Review on Security Challenges of Cloud Computing*", International Conference on Advancements in Computing & Management (ICACM).

9. WANG, S.H. and WANG, X. and ZHANG, Y. (2019). "*A Secure Cloud Storage Framework With Access Control Based on Blockchain*", IEEE, 23 July.

۱۰. غفاری، م و تاجفر، ا. ه. (۱۳۹۹)، "تاثیر بلاکچین بر واقعیت افزوده در پزشکی"، چهارمین کنفرانس ملی پژوهش‌های کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی.

۱۱. حسن پور عسکری، ع و احمدی نیا، م. (۱۳۹۷)، "فناوری بلاکچین و کاربرد آن در حوزه ی پزشکی"، فصلنامه ی پژوهش‌های کاربردی در فنی و مهندسی.

۱۲ . Park, J. H. and Park, J. H. (2017). "*Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions*", Journal of Symmetry, MDPI, September.

13. Pavithra, S. and Ramya, S. and Prathibha, S. (2019). "*A Survey On Cloud Security Issues And Blockchain*", 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, India, 21-22 Feb.