بررسی امنیت در اینترنت اشیا با استفاده از راهکارهای تکنولوژی بلاک چین

(سید علیرضا پورشایسته فرد، کارشناس گروه امداد و پشتیبانی شبکه شرکت خدمات انفورماتیک،
(a_pourshayestefar@isc.co.ir
(مهدی امیدی، کارشناس گروه امداد و پشتیبانی شبکه شرکت خدمات انفورماتیک، m_omidi@isc.co.ir)

چکیده

اینترنت اشیا مفهومی رایانشی برای توصیف آینده‌ای که در آن اشیای فیزیکی، یکی پس از دیگری به اینترنت وصل می‌شوند و با اشیای دیگر در ارتباط قرار گرفته و با شناسه های منحصر به فرد و توانایی انتقال داده ها بر روی یک شبکه، با یکدیگر تعامل برقرار می کنند.
با رشد این شبکه، چالشهای امنیتی جدیدی بروز پیدا می‌کند که یکی از راه حل های موجود، استفاده از بلاک چین می‌باشد. این تکنولوژی تجهیزات موجود را قادر می‌سازد که از اتکاء به یک سیستم یا ابر مرکزی جهت احراز هویت و شناسایی بی نیاز شوند و با ایجاد یک شبکه مش امن، امکان برقراری ارتباط بین تجهیزات مختلف و جلوگیری از کلاهبرداری و جعل هویت را فراهم می‌سازد.

با رشد ارزها و تراکنش های رمزپایه در سال‌های اخیر، بلاک-چین ها توجه زیادی را به‌خود جلب نموده‌اند. سیستمی که بلاک چین ها پیاده‌سازی نموده‌اند، به مبارزه با متمرکزسازی منجر شده و کاربران را به پیاده‌سازی یک سیستم غیرمتمرکز و مطمئن سوق داده است. به‌علت اطمینان بالا به این سیستم، شرکت‌های بزرگی اقدام به سرمایه‌گذاری بر روی آن کرده‌اند، که در سال های آینده شاهد استفاده بیشتر از این سیستم خواهیم بود. فناوری بلاک‌چین یک دفترکل جهانی است که در اصل برای ردیابی بیت‌کوین طراحی شده است. با این حال، می‌توان آن را به گونه‌ای برنامه ریزی کرد تا هر چیزی را ردیابی کند. این به این معنی است که به کارگیری بلاک‌چین مزایای زیادی برای بهبود اینترنت اشیا در پی خواهد داشت.

در سناریوهای مختلفی که برای اینترنت اشیا مطرح است، تامین حفظ حریم خصوصی کاربران در بلاک‌چین و به صورت عمومی، راهکارها و شیوه های ارتباطی نظیر به نظیر، نقش کلیدی و مهمی را در توسعه نرم افزارهای غیر متمرکز و داده ای که بر روی میلیون ها دستگاه نصب می شود، ایفا می کند. در این مقاله سعی بر آن می شود تا به مسئله امنیت در اینترنت اشیا با استفاده از راهکارهای تکنولوژی بلاک چین پرداخته می شود.

کلمات کلیدی: اینترنت اشیا، بلاک چین، حریم خصوصی، امنیت، سیستم های غیر متمرکز

مقدمه

یکی از چالش‌های عمده‌ای که باید به منظور وارد کردن اینترنت اشیا به جهان واقعی بر طرف شود امنیت است. تهدیداتی که می تواند بر نهادهای اینترنت اشیا تأثیر گذارد متعدد هستند، مانند حملات با هدف کانال‌های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیا که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف، می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری

مکانیزم‌های امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. از جمله دو چالش مهم و پیچیده در اینترنت اشیا عبارتند از: امنیت و حریم خصوصی.

امنیت شامل دسترسی غیرقانونی به اطلاعات و حمله‌هایی است که موجب قطعی فیزیکی در قابلیت دسترسی به سرویس می-گردد. امنیت و حریم شخصی به طور گسترده‌ای از مسائل مهم در زمینه فناوری اینترنت اشیا شناخته شده اند. از یک طرف، محرمانه بودن و یکپارچگی اطلاعات منتقل شده و ذخیره شده باید تضمین گردد، و احراز هویت و مکانیزم های صدور مجوز برای جلوگیری از دسترسی ناشایست کاربران و یا دستگاه های غیر مجاز نادرست فراهم گردد. از سوی دیگر، حریم خصوصی کاربران، به عنوان توانایی پشتیبانی از حفاظت داده ها و گمنام ماندن کاربران باید به عنوان یک جنبه اساسی به ویژه در ارائه اطلاعات حساس و یا شخصی در نظر گرفته شود.
بنابراین پیشنهاد های بسیاری در این زمینه ارایه می گردد که یکی از آن ها ارایه خدمات با کنترل دسترسی می باشد که ممکن است دیدگاه مناسبی باشد اما این موضوع سبب می گردد تا با تاخیر های بالایی در شبکه مواجه شده و برخی اقدامات و خدمات را مختل نماید. برای مثال چنانچه سطح دسترسی را برای کاربرانی که خدمات امنیتی استفاده می کنند مورد نظر قرار دهیم، ممکن است با در دسترس نبودن شخص در صورت بروز مشکل، خطرات بیشتری بر این موضوع وارد گردد.

هدف قانون امنیت، محافظت از تهدیدات است. این تهدیدات به دو دسته طبقه‌بندی می شوند که عبارتند از: تهدیدات خارجی مانند حمله مهاجمان به تشکیلات سیستم و تهدیدات داخلی مانند سوء استفاده از سیستم و یا اطلاعات. سه عامل اصلی برای حفظ امنیت وجود دارد: محرمانه بودن اطلاعات، حفظ حریم خصوصی و اعتماد. محرمانه بودن اطلاعات تضمین می کند تنها کاربران مجاز قادر به دسترسی و تغییر داده باشند، و آن شامل دو جنبه است: اول، مکانیزم کنترل دسترسی و دوم، یک فرایند احراز هویت اشیاء. اعتماد جهت اعمال قوانین امنیتی در سیستم تضمین شده است و نمونه رایج از اعتماد، گواهینامه های دیجیتال هستند. حریم خصوصی به عنوان یک کنترل دسترسی به اطلاعات شخصی تعریف شده است و نگهداری اطلاعات خاص و اطلاعات محرمانه را مقدور می سازد. ویژگی های حفظ حریم خصوصی، سری بودن، گمنامی و خلوتی آن است. بیشتر محققان در حال حاضر به دنبال افزایش و توسعه حریم خصوصی در برنامه های کاربردی هستند، فناوری‌های بهبود حریم خصوصی (PET)[1] می تواند به موضوع اشیا، تراکنش یا سیستم متمایل گردد و از آن برای محافظت از هویت در اینترنت استفاده شود. در محیط اینترنت اشیا، امنیت و حریم خصوصی برای تضمین یک تعامل قابل اعتماد بین دنیای فیزیکی و دنیای مجازی مهم هستند[۲۰].
گیبس (۲۰۰۸) حریم خصوصی را به عنوان "محدودیت دسترسی دیگران به یک شخص" تعریف می کند و اشاره می کند که این محدودیت بر اساس سه عنصر قرار گرفته است: پنهان کاری (کنترل اطلاعات)، ناشناسی (اقدام بدون توجه دیگران) و تنهایی (محدود کردن دسترسی فیزیکی به یک فرد). علاوه بر این، گیبس (۲۰۰۸) اشاره به اهمیت تعادل حریم خصوصی شخصی در برابر دیگر حقوق فردی و در برابر کالای اجتماعی جمعی دارد. حریم خصوصی افراد به طور خاص شامل آنکه (۱) افراد لازم است چه اطلاعاتی، در مورد خود برای دیگران فاش کنند، و (۲) به شدت برای خودشان حفظ کنند. با توجه به افزایش دیجیتالی شدن اطلاعات شخصی و شبکه فن آوری ها از طریق اینترنت اشیا، یک نگرانی رو به رشد وجود دارد که افراد ممکن است از عواقب قانونی مرتبط با جمع آوری داده ها از طریق اینترنت اشیاء غافل باشند. به طور خاص، اغلب دستورالعمل های نامشخصی وجود دارد.
مسائل حریم خصوصی شامل حریم خصوصی شی، حفظ حریم خصوصی مکان، و حریم خصوصی انسان است.

[1] Privacy-enhancing technologies

یافته ها نشان می دهد که (۱) برنامه های کاربردی به اندازه کافی از حریم خصوصی شخصی داده های جمع آوری شده از طریق اینترنت اشیاء محافظت نمی کند، و (۲) قوانین حفظ حریم خصوصی آینده باید پیامدهای دسترسی جهانی به خدمات اینترنت اشیاء، و حضور در همه جا و امنیت جمع آوری داده اینترنت اشیا با توجه به حریم خصوصی افراد را در نظر گیرد.
در زمینه حفظ امنیت اقدات زیر می تواند مؤثر باشد:

--رمزنگاری داده ها

--تصویب قوانین برای حفاظت از داده ها

--شناسایی فوری و حفاظت از اینترنت اشیاء در مقابل برنامه های مخرب.

بلاک چین در حال حاضر یکی از فن‌آوری‌های پرطرفدار است. در این جا سعی خواهیم کرد تا نشان دهیم در حال حاضر در حوزه امنیت و حریم خصوصی در اینترنت اشیا چه مباحثی با استفاده از بلاک چین مطرح است و همچنین کاربردها و مزایا و معایب استفاده از بلاک چین در اینترنت اشیا بیان می‌شود. همچنین در این مقاله چگونگی امنیت و حریم خصوصی را با استفاده از فناوری بلاک چین را بررسی می‌کنیم و راهکارهایی با استفاده از بلاک چین برای احراز هویت و اقداماتی که باعث بالا بردن امنیت و حریم خصوصی در اینترنت اشیا می شود را بررسی می‌کنیم و چالش های پیش رو را مشخص می‌کنیم. همچنین به مسئله احراز هویت در اینترنت اشیا پرداخته شده و راهکارهایی با استفاده از بلاک چین بیان می شود.

مرور ادبیات

طراحان بدافزار و مهاجمان سایبری امروزه نوآورانه عمل می‌کنند و به طور مداوم تلاش می‌کنند تا اقدامات موجود در زمینه امنیت را از بین ببرند (به عنوان مثال تولید نسخه های مختلف نرم افزارهای مخرب با استفاده از تغییر داده ها). اکثر رویکردهای موجود برای سیستم های تشخیص نفوذ (IDS)[۲] و سیستم های پیشگیری از نفوذ (IPS)[۳] برای شناسایی تلاش-های مجاز دسترسی و حملات ایجاد اختلال در سرویس (DDoS) طراحی شده‌اند. به عنوان مثال، Alsunbul و همکاران. [۱] سیستم دفاعی شبکه را برای شناسایی و جلوگیری از تلاش‌های دسترسی غیر مجاز، با ایجاد پویایی یک پروتکل جدید برای جایگزینی پروتکل استاندارد ارائه داد. هدف این است که تلاش های اسکن را اشتباه بگیریم. مسیر شبکه نیز به صورت دوره ای تغییر می‌کند تا از دسترسی غیر مجاز و اسکن ترافیک جلوگیری شود. با این حال، مقدار بسته تولید شده می تواند بیش از حد باشد. در روش Zitta، Neruda و Vojtech [۲]، برای امنیت شناسایی خوانندگان در RFID که با فرکانس بالا (UHF) استفاده می شود از Raspberry Pi 3 که دارای پروتکل خواننده سطح پایین (LLRP[۴]) است.

رمزنگاری یک رویکرد رایج برای ارائه محرمانه بودن اطلاعات و یکپارچگی است، مانند روش‌های چند لایه امنیتی که در منابع آمده است[۳و۴]. به طور خاص، Chang و Ramachandran [۳]، یک راه حل امنیتی چند لایه را برای محاسبات ابر ارائه دادند. اولین لایه امنیتی دیوار آتش و کنترل دسترسی است، که طوری طراحی شده تا اطمینان حاصل شود که فقط کاربران مجاز و تأیید شده می توانند به سیستم و داده دسترسی داشته باشند. لایه دوم شناسایی مدیریت و جلوگیری از نفوذ است که برای اطمینان، از شناسایی کاربر یک بار دیگر تأیید گرفته می‌شود و هر گونه فایل های مخرب شناسایی و حذف خواهند شد. لایه سوم رمزگذاری همگرا است که یک سیاست امنیتی زیاد را فراهم می کند. برای ارزیابی رویکرد پیشنهادی، نویسندگان یک آزمایش نفوذ را در ۱۰ پتا بایت داده، از مراکز داده انجام دادند. یافته های آنها نشان می دهد که زمان برای یک تلاش غیر

[2] Intrusion detection systems
[3] Intrusion prevention systems
[4] low-level reader protocol

مجاز حداقل ۱۲۵ ساعت است[۴].

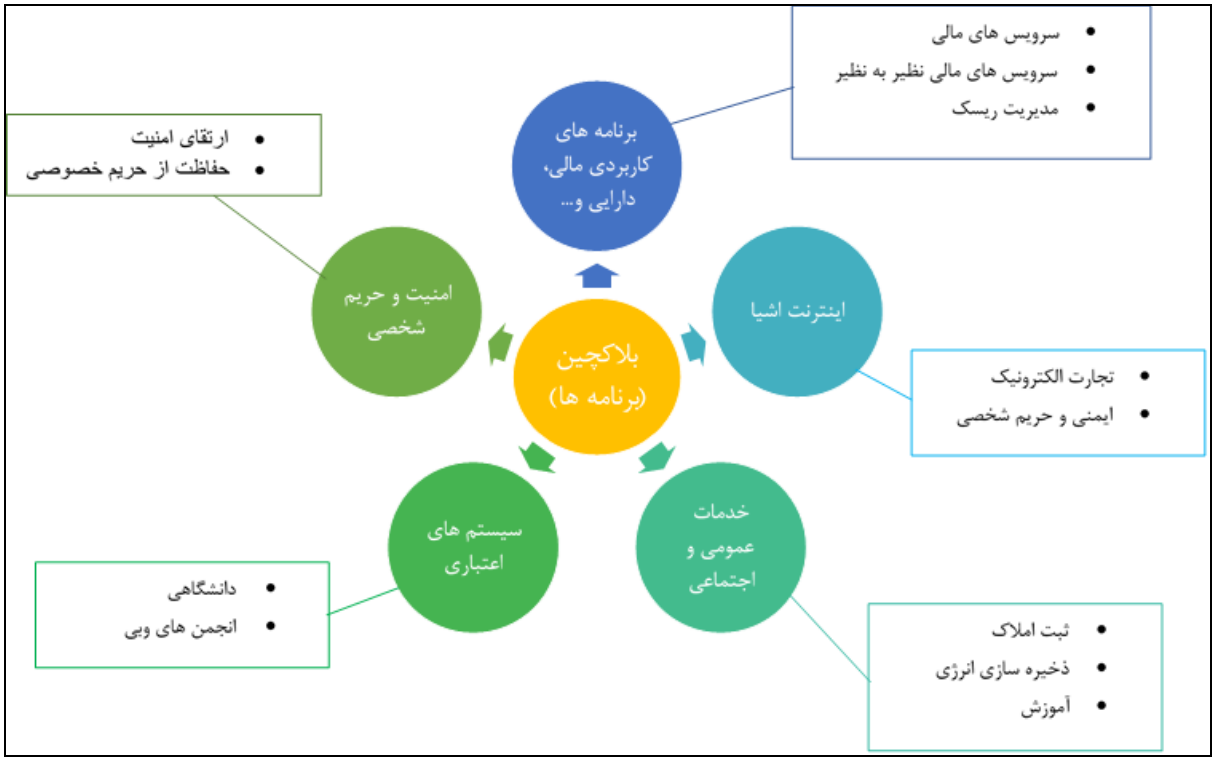
Jin، Tomoishi و Matsuura [۵]، روش پیشرفته تأیید هویت شبکه مجازی (VPN) را با استفاده از سیستم موقعیت یابی جهانی (GPS) ارائه دادند. روش پیشنهادی محافظت از حریم خصوصی در دستگاه های تلفن همراه را فراهم می کند. در اینجا، یک مشتری VPN، به جای ارسال مقدار خام، اطلاعات هش، از اطلاعات جغرافیایی را ارسال می کند، بنابراین، حفاظت از اطلاعات موقعیت جغرافیایی حریم خصوصی مشتری حفظ می شود. به جای ارائه مختصات GPS فقط، اطلاعات یک منطقه برای تأیید هویت برای هر مشتری ارائه می شود. نقشه های گوگل برای بررسی میزان خطا از مختصات جغرافیایی مشتری منطقه مورد نظر استفاده شده است، و نتایج ارزیابی نویسندگان، میزان دقت ۹۹,۲۹

افزایش زیاد استفاده از پهنای باند در بلاک چین سبب کاهش این مقدار در استفاده دستگاه ها در شبکه اینترنت اشیا خواهد شد.

کاربرد ها و نرم افزار های مختلفی برای فناوری بلاک چین وجود دارد که در این تحقیق به بررسی خلاصه ی چند برنامه ی کاربردی می پردازیم:

برنامه های کاربردی (دارایی، مالی و سرمایه گذاری) بلاک چین
اینترنت اشیا
خدمات عمومی و اجتماعی
سیستم اعتباری
امنیت

همچنین در شکل ۱ دامنه ی کاربردهای بلاک چین را نشان می دهیم.



شکل ۱- دامنه کاربرد بلاک چین

۱. برنامه های کاربردی مالی و دارایی

سرویس های مالی

سرویس های مالی با درجه ی اهمیت بسیار بالایی از سیستم های بلاک چین مانند بیت کوین (ناکاموتی ۲۰۰۸ و Hyperledger 2015) [۸]، تاثیر زیادی بر خدمات مالی و تجاری سنتی داشته است. همچنین بلاک‌چین‌ها پتانسیل زیادی در ایجاد اختلال در بانک را دارند. تکنولوژی بلاک چین می تواند در بسیاری از مناطق از جمله در پاکسازی و حل و فصل دارایی های مالی استفاده شود. علاوه بر این یکی از موارد واقعی کسب و کار، تامین مالی و مشتقات آن است که بلاک چین می تواند در کاهش این هزینه ها کمک نمایند[۹]. (Morini, 2016)

ریسک‌های استفاده از بلاک چین توجه شرکت‌های نرم افزاری بزرگ را در تنظیم چشم اندازهای بلند مدت خودت جلب کرده است. (azure 2016[۱۱] و IBM 2016[۱۰]). در تحول سازمانی علاوه بر تکامل خدمات مالی و سرویس های تجاری، بلاک چین می‌تواند به سازمان‌های سنتی کمک کند تا تغییرات سازمانی را به صورت موازی کامل کند. برای مثال شرکت‌های خدماتی پستی را در نظر بگیرید، از آنجایی که شرکت های پست سنتی به عنوان یک واسطه ی ساده بین تجار و مشتری عمل می‌کنند، تکنولوژی بلاک چین و ارزهای رمزنگاری شده می تواند به سازمان های تولید کننده کمک کند تا نقش ساده‌ی خود را با ارائه‌ی خدمات جدید مالی و غیرمالی گسترش دهند. مشخص شده است که در شرکت های پستی می توانند postcoin خود را از طریق تبدیل بیت کوین صادر نمایند[۱۲]. (jaag 2016).

بازار مالی نظیر به نظیر

بلاک چین می تواند به ساخت بازار مالی نظیر به نظیر در یک راه مطمئن و ایمن کمک کند. همچنین در اینترنت اشیا، شبکه ارتباطی برای ارتباط دستگاه های مختلف بر اساس مدل نظیر به نظیر پیاده سازی شده است.

مدیریت ریسک

چارچوب مدیریت ریسک در تکنولوژی های مالی (FinTech) از اهمیت بسیار بالایی برخوردار است و می تواند با ترکیب با بلاک چین امکانات بهتری ارائه شود و از آن در مدیریت ریسک سرمایه گذاری در سناریو های بورس اوراق بها دار و زنجیره تامین استفاده نمود.

۲. اینترنت اشیا

اینترنت اشیا یکی از بزرگترین امیدهای فناوری اطلاعات و ارتباطات می باشد و در آن مشخص شده است همه اشیا به صورت هوشمند با یکدیگر در ارتباط باشند و به اینترنت متصل گردند تا کاربران بتوانند از خدمات مختلف آن استفاده نمایند که این خدمات عبارتند از:

- خانه های هوشمند
- سلامت هوشمند
- صنایع هوشمند

- مدیریت انرژی و امنیت هوشمند
- و...

فناوری بلاک چین می تواند اینترنت اشیا را به صورت بالقوه بهبود بخشد.

کسب و کارهای الکترونیکی

در یک مدل جدید کسب و کار IOT[5] تجارت الکترونیک را به گونه ای ارائه می دهد که دراین معاملات اموال هوشمند بر اساس قرار گرفتن در بلاک چین انجام پذیرد. در این مدل شرکت‌های مستقل موجود به عنوان یک نهاد معامله گر غیر متمرکز به ثبت رسیده که افراد می توانند اطلاعات حسگر ها را بدون دخالت هیچ شخص ثالثی از طریق سکه های بدست آوری شده معامله کنند.

امنیت و حریم خصوصی

یکی از دغدغه های مهم در صنعت IOT حفظ امنیت و حریم خصوصی می باشد که بلاک چین توانسته است در بهبود حریم خصوصی در برنامه های IOT کمک به حفظ حریم شخصی کند. در یک سیستم ابری می توان پیشنهاد داد که یک معماری خاصی طراحی گردد تا افراد با استفاده از بلاک چین بتوانند به صورت غیر متمرکز به ایجاد یک شبکه توزیع دستگاه پرداخته و در این روش از هیچ شخص ثالثی استفاده ننمایند.

۳. سرویس های عمومی و اجتماعی

بلاک چین می تواند استفاده های گوناگونی در سرویس های عمومی و اجتماعی داشته باشد که نمونه هایی از آن در زیر اعلام می شود.

ثبت املاک

یکی از خدمات کاربردی در بخش عمومی ثبت املاک می باشد که در آن اطلاعات زمین مانند وضعیت فیزیکی و حقوق مربوط به آن می‌تواند بر روی بلاک‌های زنجیره‌ای ثبت و منتشر شود. علاوه بر این هرگونه تغییر در آن مانند انتقال زمین، ایجاد وام مسکن می‌تواند بر روی بلاک‌ها ثبت و مدیریت شود و می تواند خدمات عمومی را بهبود بخشد.

ذخیره سازی انرژی

بلاک‌چین‌ها می‌تواند در انرژی‌های سبز نیز استفاده شوند. Gogerty و Zitoli پیشنهاد کرده‌اند که انرژی خورشیدی می-تواند برای تشویق استفاده کنندگان از انرژی‌های تجدید پذیر استفاده گردد. به طور خاص شرکت‌های تولید کننده انرژی

[5] Internet of things

خورشیدی واحد ارزی‌ای به نام solacoin را در قبال تولیداتشان دریافت می نمایند[۱۳].

آموزش

بلاک‌چین در اصل برای فعال کردن معاملات ارز در محیط های بی اعتماد طراحی شده است؛ بنابر این در بحث آموزش چنانچه بخواهیم از این قابلیت بلاک‌چین استفاده نماییم می‌توان در بازارهای آموزش آنلاین از آن استفاده کرد. معلم‌ها به عنوان تولید کننده‌های بلاک و دانش آموزان به عنوان سکه در نظر گرفته می‌شوند. بلاک چین می‌تواند در سایر خدمات عمومی مانند ثبت ازدواج، ثبت اختراعات و سیستم های پرداخت مالیات استفاده شود. در سرویس‌های عمومی جدید که از بلاک‌چین استفاده می‌شود از امضای دیجیتال در دستگاه های همراه استفاده می گردد که از آن به عنوان مهر و امضای فیزیکی استفاده می گردد. بنابر این می‌توان حجم زیادی از پرونده‌ها را به صورت مجازی ذخیره کرد.

۴. سیستم اعتباری

در معاملات تجاری در جامعه اعتبار افراد یکی از ارکان مهم در معاملات می‌باشد و اعتبار یک شخص بر اساس گزارش‌های معاملات قبلی خود در جامعه محاسبه می شود. برای مثال در تجارت الکترونیکی افراد به صورت جعلی از سوی مشتریان دیگر خدمات ثبت نام را انجام داده و شهرت بالایی پیدا می‌کند، بنابراین بلاک چین به صورت بالقوه می توان این مشکل را برطرف سازد.

دانشگاه

اعتبار برای دانشگاهیان بسیار مهم می باشد. (Sharples & Domingue, 2015[۱۴]) برای نگهداری و اعتبار آموزشی یک سیستم توزیع مبتنی بر بلاک‌چین را ارائه دادند در ابتدا هر موسسه و هر دانشجو می‌توانند از ارز اعتبار آموزشی یک پاداش اولیه بدست آورند. یک موسسه می‌تواند به کارمندانش با استفاده از انتقال رکوردهای اعتباری پاداش دهد. از زمانی که تراکنش ها بر روی بلاک‌چین ذخیره می‌شوند تمام تغییرات اعتبارات به راحتی قابل کشف و ردیابی می‌باشند.

انجمن های وبی

توانایی ارزیابی اعتبار یک عضو در جامعه‌ی وب بسیار مهم می‌باشد. یک مدل پیشنهادی بر مبنای بلاک‌چین اینگونه است که اگر مشتری با سرویس موافقت کند گزارش امضا خواهد شد و مایل است بازخورد خوبی را دریافت نمایند. پس ازامضای کوپن به سرویس دهنده باید ۳ امتیاز از پرداخت را به عنوان هزینه‌ی رای گیری دریافت نماید که جهت جلوگیری از حمله‌ی Sybil انجام می شود. یک بلاک چین جدید برای ذخیره ی میزان اعتبار (ارزش صفر یا یک) از معاملات کامل ایجاد می‌گردد به عنوان مثال در خصوص به اشتراک گذاری فایل موجودیت A یک فایل را به واحد B ارسال می کند؛ پس از دریافت فایل B یک شماره از فایل را برای تایید هویت ارسال می کند سپس کاشف ها (miners) با Bو A تماس می‌گیرند تا تایید کنند معامله بدون هیچ مشکلی صورت پذیرفته است و از آنجا که معاملات در بلاک‌چین ذخیره می‌شوند هر گونه مداخله و تغییر در پرونده ها غیر ممکن خواهد شد.

۵. امنیت و حریم خصوصی

ارتقای امنیت

ما با گسترش روز افزون تلفن همراه و خدمات مربوط به آنها مواجه هستیم که سبب می گردد آسیب پذیری به آنها بیشتر شده بنابراین تعدادی از فیلترهای ضد تروجان برای شناسایی فایل‌های مشکوک از طریق الگوهای تطبیق پیشنهاد می‌شود که یک سرور مرکزی برای ذخیره و بروز رسانی الگوهای ویروس وجود دارد این اقدامات برای ورود مهاجمان همچنان آسیب پذیر می‌باشد. بلاک‌چین به طور بالقوه می‌تواند به بهبود امنیت شبکه های توزیع کمک نماید. چارلز یک محیط جدید anti-malware به نام BitAd را پیشنهاد کرد که در آن کاربران می توانند الگوهای ویروس را در بلاک چین توزیع نمایند. بنابراین می‌توانند سرعت اسکن را بهبود بخشیده و قابلیت اطمینان خطا را افزایش دهند. فناوری های بلاک‌چین در جهت بر قراری زیرساخت های امنیتی بسیار مورد استفاده قرار می گیرند برای مثال زیرساخت های کلید عمومی PKI[۶]

حفاظت از حریم خصوصی

علاوه بر خطرات موجود بر روی امنیت شبکه ممکن است افراد اطلاعات شخصی خود را بر روی تلفن های همراه یا شبکه ی های اجتماعی ذخیره نمایند برای مثال فیس بوک بیش از ۳۰۰ پتابایت اطلاعات شخصی را از ابتدا جمع‌آوری کرده است که این اطلاعات در سرور مرکزی ذخیره می گردد که بسیار مستعد حملات سایبری می‌باشند. بنابر بلاک‌چین جهت بهبود امنیت داده‌های حساس می‌تواند مورد استفاده قرار می‌گیرد. یک سیستم مدیریت اطلاعات شخصی غیر متمرکز می تواند مالکیت کاربر را نسبت به داده‌های خود تضمین نماید که این موضوع از طریق بلاک‌چین قابل پیاده سازی می باشد. بنابراین بلاک-چین از طریق غیر متمرکز کردن داده‌ها به ایمن سازی داده‌های حساس می پردازد که سبب می گردد:

مالکیت داده حفظ شود.

شفافیت داده ها و قابلیت اطمینان ایجاد شود و کنترل دسترسی دقیق ایجاد گردد.

چالش‌های بلاک‌چین و بررسی آن‌ها

در ادامه به بررسی مشکلات و چالش‌های مطرح شده در زمینه امنیت بلاک‌چین پرداخته می‌شود. همچنین راهکارهایی که می‌توان از طریق آن مشکلات را برطرف کرد نیز بیان می‌شود.

امنیت

امروزه تراکنش‌ها به صورت سراسری انتشار پیدا می کنند اما معمولا در اغلب برنامه‌های کاربردی رمزنگاری نشده‌اند. اگر این داده یک داده شخصی باشد، مثلاً داده‌های مربوط به مسایل مالی و یا پزشکی، باعث می‌شود که این داده‌ها به رگولاتوری‌ها رود و مشکلاتی را به وجود آورد. یک راهکار برای جلوگیری از این مشکل این است که داده ها را به صورت رمزنگاری شده در

[۶] زیرساخت کلید عمومی

بلاک‌چین قرار دهیم که این خود منجر به بروز مشکلات دیگری می‌شود. اگر کلید مربوط به اطلاعات شخصی که رمزنگاری با آن انجام گرفته از بین برود، ممکن است داده به درستی بازگردانده نشود. بنابراین، اگر یک کلید دزدیده و منتشر شود، تمام داده ها برای همیشه در بلاک‌چین به صورت رمزگذاری شده باقی می‌ماند چون داده ها نمی‌توانند اصلاح و یا تغییر کنند. به علاوه بلاک‌چین می‌تواند در بهبود استراتژی‌های دفاعی در امنیت سایبری مخصوصاً در زمینه شناسایی و دسترسی کمک کند.

حمله‌های MITM[7]

حمله مرد میانی به این معنی است که بتواند یک گواهی شناسایی (CA[8]) معتبر ایجاد کند تا کاربران بتوانند با یک کلید عمومی جعلی (تعویض کلید عمومی با یک کلید جلی) کار کنند. در این صورت می‌تواند به اطلاعات حساس به صورت رمزگشایی شده دست یافت. در رویکرد بلاک‌چین که در آن کاربران کلید عمومی خود را در بلاک‌هایی که به صورت عمومی انتشار یافته است قرار می‌دهند. اطلاعات در گره‌های شرکت کننده به همراه لینک‌های ارتباطی به بلاک قبلی و بعدی آن در بلاک‌چین توزیع می‌شود. این باعث می‌شود که کلید عمومی تغییر ناپذیر گردد و کار برای هکرها برای ایجاد و انتشار کلید جعلی بسیار سخت می‌شود. بعلاوه تنها نقطه شکست، یعنی CA، در بلاک‌ها توزیع شده است به این معنی که خیلی سخت می شود سیستم را از کار انداخت.

خرابکاری داده ها

از آنجایی که هر تراکنش امضا شده و در میان تمامی بلاک‌های گره‌ها توزیع شده است، عملاً بدون داشتن دانش کافی در مورد شبکه‌ای که در آن بلاک چین وجود دارد، دستکاری داده‌ها غیر ممکن است. می‌توان با زدن یک مثال مفهوم زیر را تشریح کرد، مثلاً هیچ کس نمی تواند ثابت کند که در جام جهانی ۱۹۹۸، ایران در جام جهانی، آمریکا را شکست نداده است، زیرا این به یک دانش عمومی تبدیل شده است و در بین مردم گسترده شده است. در مراقبت های پزشکی و بهداشتی، بلاک-چین می‌تواند در رسیدگی‌های دنباله دار غیرقابل تغییر، نگهداری و حفظ آزمایشات پزشکی و اطمینان از یکپارچگی داده‌های بیمار به اشتراک گذاشته شده در محیط های پزشکی مختلف کمک بسیار زیادی کند.

حملات DDOS

در علم رایانه، حملات ایجاد اختلال در سرویس (DOS) یا حملات ایجاد اختلال در سرویس توزیع شده (DDOS)، تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجازش می‌باشد. اگرچه منظور از حمله DOS و انگیزه انجام آن ممکن است متفاوت باشد، اما به طور کلی شامل تلاش برای قطع موقت یا دائمی یا تعلیق خدمات یک میزبان متصل به اینترنت است. اهداف حمله DOS معمولاً سایت‌ها یا خدمات میزبانی وب سرور با ویژگی‌های مناسب مانند بانک‌ها، کارت-های اعتباری و حتی سرورهای ریشه را هدف قرار می‌دهند. یکی از روش های معمول حمله شامل، اشباع ماشین هدف با درخواست‌های ارتباط خارجی است به طوری که ماشین هدف، نمی‌تواند به ترافیک قانونی پاسخ دهد یا پاسخ ها با سرعت کم داده می‌شوند یا در دسترس نمی‌باشند. چنین حملاتی منجر به سربار زیاد سرور می‌شوند. حمله DOS کامپیوتر هدف را وادار به ریست شدن یا مصرف منابع‌اش می‌کند، بنابراین نمی‌تواند به سرویس‌های مورد نظرش سرویس بدهد و همچنین سیاست

[7] Man in the middle
[8] Certificate authority

های مورد قبول فراهم کنندگان سرویس های اینترنتی را نقض می کنند. در صورتی که خدمات میزبانی وب بر اساس بلاک-چین باشد، می‌توان گفت که حملات به سختی منجر به موفقیت می‌شوند. زیرا زیرساخت خدماتی وب سرور به صورت سیستم‌های توزیعی هستند و داده ها و همچنین ورودی داده‌ها را نمی‌توان با توجه به ماهیت بلاک چین تغییر داد[۲۲].

حریم خصوصی

همواره بخاطر داشته باشید که جهت حفظ حریم خصوصی، مسئولیت انجام اقدامات درست با خود شماست. تکنولوژی بلاک چین یک نمونه عالی برای امنیت (حداقل از نظر غیر قابل تغییر بودن) و حریم خصوصی است. در حالی که ممکن ست یک تراکنش مقاوم در برابر تغییر ایجاد شود، این معامله را می توان در تمام گره‌های شبکه مشاهده کرد. تحقیقات گسترده ای در حریم خصوصی و تراکنش های خصوصی در حال انجام است که می توان از آن ها برای رای گیری‌ها، تراکنش‌های ناشناس و مزایده ها استفاده کرد.

چالش ها

اگرچه فناوری‌های بهبود حریم خصوصی نیز وجود دارند، ولی هنوز هم ابردادهایی[۹] تولید می کنند. تجزیه و تحلیل آماری "برخی" اطلاعات نشان می‌دهد، حتی اگر داده‌ها به صورت رمزگذاری شده باشند، برای مثال، تشخیص الگو امکان پذیر است. علاوه بر این، مقیاس پذیری یک چالش در حال ظهور است، زیرا پیاده‌سازی روند اجماع در حال حاضر بیش از حد هزینه دارد. اگر ارز یا هر مقدار دیگر در یک برنامه مبتنی بر بلاک‌چین معامله شود، تراکنش‌ها باید از سرعت بسیار بالاتری برخوردار شوند. Ethereum در حال حاضر قادر به انجام ۲,۸ تراکنش در ثانیه است، در حالی که بیتکوین قادر است حدود ۳,۲ تراکنش در ثانیه انجام دهد. به دلیل فرایند اجماع پیچیده برای هر تراکنش (در حال حاضر اثبات کار یا اثبات سهام) حمله دیگری که باید در ذهن داشته باشید، حمله□51 یا «Attack Majority Hash Rate» است. اگر یک سازمان یا فرد دارای ۵۱

داده‌ها جلوگیری شود. بنابراین، تجهیزات و تمهیدات جدیدی برای سیستم‌های پیاده‌سازی شده‌ی کنونی باید بکار گرفته شود. در این قسمت به بررسی نیازمندی‌های جدید امنیتی در حوزه احراز هویت با استفاده از بلاک چین پرداخته می‌شود.

احراز هویت غیرمتمرکز

احراز هویت غیر متمرکز، جایگزین نام کاربری و پسورد و استفاده از تولید کلید و گواهی SSL در سمت کلاینت شده است و از رمزنگاری منحنی بیضوی(ECC[11]) برای تولید کلید استفاده می‌کند. این دقیقا همان پروتکلی است که در بلاک‌چین مورد استفاده قرار گرفته است [۱۵] و [۱۶] . این روش رمزنگاری باعث حذف شدن یک پایگاه داده مرکزی برای نگه داری اطلاعات کاربران می شود و هکرها نمی توانند موردی برای ایجاد اختلال در داده‌ها شوند. پسورد کاربرد در این نوع احراز هویت، تنها برای ماشین مورد استفاده کاربر استفاده می شود تا بتواند به کلید خصوصی آن دست یابد. کلید خصوصی هرگز از طریق شبکه یا سرویس دهنده، نشان و یا در دسترس قرار نمی‌گیرد و نمی‌تواند بین سرویس دهنده و سرویس گیرنده بیش از یک کانال جانبی مبادله شود. این پروتکل احراز هویت بر اساس تایید هویت غیرقابل انکار با استفاده از امضاهای دیجیتال بر اساس کلیدهای عمومی استوار است. یک کاربر زمانی تایید می‌شود که پیام یا تراکنش آن، با یک کلید خصوصی تأیید شده است. در نتیجه هرکسی که دسترسی به کلید خصوصی دارد مالکیت اطلاعات را دارد و هویت دقیق مالک مشخص نیست.

احراز هویت بی نام و بدون پسورد

احراز هویت بدون رمز عبور برای سال‌هاست که یک روش ایده آل برای امنیت است. در این روش، راه‌های زیادی برای رسیدگی به احراز هویت و شناسایی کاربران وجود دارد، مانند احراز هویت مبتنی بر بیومتریک، PKI و QRCodeها. با این حال، این سه روش به یک پایگاه داده‌ی شناسایی یک سازمان مرکزی متصل شده و ناشناس نیستند. به تازگی، شناسایی مبتنی بر بلاک‌چین یک راه حل برای جایگزینی نام کاربری و رمز عبور با احراز هویت و کنترل دسترسی امن ارائه داده است. این سیستم شناسایی، مشابه سایر ارزهای دیجیتالی مبتنی بر بلاک‌چین مانند بیت کوین است. تراکنش با هر سیستم آنلاین یک شماره شناسای امن (SIN[12])دارد[۱۷]. یک SIN، دارای شناسه رکورد منحصر به فرد است که توسط آن هویت شناخته می‌شود و هیچ زیرساخت متمرکز یا نهاد و سازمانی لازم ندارد. هویت در SIN امن و تحت کنترل کامل مالک است. SIN می‌تواند طیف کاملی از نیازهای هویت و احراز هویت را پشتیبانی کند.

استفاده از SIN امن تر از به اشتراک گذاشتن کلید جلسه در یک پروتکل شناسایی سازمانی است. SIN می‌تواند به طور آشکار برای همه به اشتراک گذاشته شود، به عنوان کلید خصوصی مربوطه در سمت سرویس گیرنده نگه داشته شده و هرگز در سراسر شبکه، منتقل نمی‌شود و همچنین با هیچ یک از موجودیت‌ها به اشتراک گذاشته نمی‌شود. در طول فرآیند تأیید هویت، سرویس دهنده، با تایید امضای دیجیتالی خود در مقابل کلید عمومی به اشتراک گذاشته شده از سوی کاربر و SIN به اشتراک گذاشته شده قبلی، شناسایی می‌شود.

این نشان می‌دهد که شماره یکبار مصرف تایید شده۱۳ بزرگتر از SIN شماره یکبار مصرف قبلی است تا از حمله‌ی بازپخش یا تکرار[14] جلوگیری کند. حمله بازپخش یکی از انواع حملات تحت شبکه است که در آن یک انتقال داده‌ی معتبر با انگیزه‌ی

[11] Elliptic curve cryptographic
[12] Secure Identity Number
[13] Signed nonce: NONCE

بدخواهانه یا کلاه برداری تکرار می‌شود یا به تاخیر می‌افتد. سپس درخواست کاربر را تایید می کند. مزیت استفاده از SIN در شناسایی قابلیت انتقال آن است، به این معنی که هویت یکسان را می‌توان در دستگاه های متعدد بدون افشای اعتبار و کلیدهای جلسه استفاده کرد.

بدون تک نقطه خرابی سیستم

تک نقطه خرابی یا نقطه تکی شکست[15] که به اختصار SPOF نام دارد به قسمتی از یک سیستم می‌گویند که اگر خراب شود، کل سیستم دچار مشکل و توقف می شود. بلاک چین یک تکنولوژی ذخیره سازی داده های توزیع شده و غیر متمرکز است که یک لیست به طور مداوم از سوابق دستور داده شده را نگه می‌دارد. این ریسک‌هایی را که با داده‌هایی که به طور مرکزی نگه داشته می‌شوند را حذف می‌کند و همچنین آسیب پذیری در مقابل هکرهای شبکه یا نقطه شکست را کاهش می-دهد. هر سرور بلاک چین که برای اهداف کاوش[16] استفاده می‌شود دارای یک کپی از بلاک چین است. کیفیت داده ها توسط تکرار پایگاه داده‌های عظیم حفظ می‌شود و از نظر رمزنگاری مورد اعتماد است. بلاک‌چین که در سیستم احراز هویت استفاده می شود یک هویت دیجیتالی محرمانه را به طور بالقوه برای کاهش اثربخشی حملات فیشینگ ایجاد می‌کند. ماهیت غیر متمرکز کل شبکه بلاک‌چین باعث می شود که زیرساخت ها، درخواست های بیش از حد را ناکام کنند. از این رو، به عنوان روش احراز هویت، که بر اساس تکنولوژی بلاک‌چین است، می تواند نسبت به حملات DDoS ایمن باشد[۲۲].

جلوگیری از سرقت داده ها

افزایش میزان حوادث هک و سرقت اطلاعات موجب ایجاد نارضایتی از دسترسی به اطلاعات حساس، به ویژه داده‌های مالی از جمله حساب‌های بانکی، کارت های اعتباری و پرونده های پزشکی است. Petland ، استاد دانشگاه MIT، بلاک چین را برای ساخت Enigma [۱۸]،کشف کرده است، که به طور بالقوه اجازه می دهد پایگاه های داده اطلاعات حساس را نگهداری کنند و آنها را پردازش کنند بدون اینکه کاربران خرابکار و هکرها بخواهند آن ها را در معرض خطر بگیرند. Enigma یک شبکه نظیر به نظیر است و کاربران مختلف برای ذخیره سازی و اجرای محاسبات روی داده ها میتوانند به آن متصل شده و همچنین داده ها کاملا خصوصی هستند. تکنولوژی بلاک چین به طور کامل از سرقت داده ها جلوگیری نمی کند، این تکنولوژی باعث می شود که سخت‌تر بتوان سیستم را از کار انداخت. مجموعه زیرساخت پیاده سازی این تکنولوژی، حفظ حریم خصوصی، امنیت و آزادی انتقال اطلاعات را بهبود می‌بخشد.

سوابق غیر قابل تغییر

فن‌آوری بلاک‌چین نوع جدیدی از پایگاه داده است که می‌تواند به طور مستقیم توسط یک گروه از کاربران بدون نیاز به یک مدیریت مرکزی، بر خلاف پایگاه های داده SQL یا NoSQL، اطلاعات به اشتراک گذاشته می‌شود. بلاک چین نوعی از پایگاه داده توزیع شده است که لیستی از پرونده های مرتب شده که آن ها را بلاک می‌نامند را حفظ می‌کند. هر بلاک حاوی یک نشانه زمانی[17] و یک پیوند به بلاک قبلی است [۱۶]. سوابق به طور محاسباتی نمی‌توانند رزرو و یا جابه جا شوند، در

[14] Replay attack
[15] Single Point Of Failure
[16] Minning
[17] Timestamp

صورتی که امکان دارد تا از تراکنش‌ها از اقدامات جعلی یا سرقت محافظت شود. با استفاده از قوانین هش و بلاک[۱۹] ، داده ها زمانی که در بلاک‌چین نوشته می‌شوند، نمی‌توانند تغییر کنند. هیچ کدام از کاربران و یا حتی مدیران نمی‌توانند زنجیره های موجود را در بلاک‌چین از بین ببرند و یا آن‌ها را تغییر دهند. هر کپی از بلاک‌چین، در شبکه همانند هم هستند و اجماع در بلاک چین توسط پروتکل مبتنی بر اثبات کار صورت می‌گیرد. پروتکل اثبات کار[۱۸] که پایه و مبنای محبوب ترین و رایج ترین ارزهای دیجیتال مانند بیت کوین است، یک سیستم استخراج و مبتنی بر قدرت محاسباتی کامپیوتر است که کاربران مشارکت کننده لازم است مسائل ریاضیاتی دشوار را برای تعیین اعتبار تراکنش ها حل کنند. شبکه های بزرگ رمزنگاری مانند بیت کوین الگوریتم اثبات کار را بنیان کار خود قرار داده اند، زیرا این به نامتمرکز بودن قدرت و کنترل روی توزیع و پیاده سازی تغییرات عمده اقتصادی و فنی در شبکه می‌انجامد. در این سیستم هر کامپیوتر با انجام محسابات هر تراکنش مقداری بیت کوین به عنوان پاداش دریافت می‌کند.

جمع‌بندی

هر روز تهدیدات امنیتی سایبری ظهور می‌کنند، در حالی که تهدیدات قدیمی هنوز در اطراف هستند و منتظر است تا بار دیگر مورد سوء استفاده قرار گیرند. تکنولوژی بلاک چین هنوز نتوانسته است که هدف نهایی در امنیت سایبری را مهیا کند، اما یک ابزار قدرتمند است که می تواند سیستم ها را تقویت کند که به سختی از کار بیافتند و یا از بین بروند. بلاک چین نقاط قوت زیادی داردکه در طی این مقاله به آن اشاره شده است. اگر سیستمی به صورت متمرکز با یک نقطه شکست باشد، به راحتی می‌توان آن را از کار انداخت. اگر تراکنش ها با سرعت زیاد و امنیت بالا نیاز باشد، بلاک چین میتواند این نیازها را برآورده کند. بلاک چین یک فن‌آوری است که در شبکه های هوشمند نظیر اینترنت اشیا کاربردهای زیادی دارد و می‌توان از آن در سیستم‌های مالی استفاده کرد.

این مقاله مشکلات امنیتی مشترک مربوط به احراز هویت در بلاک چین و همچنین راهکارهای جلوگیری از دسترسی های غیر مجاز در اینترنت اشیا را با تکنولوژی بلاک چین بررسی می‌کند. اگرچه این محدودیت ها مورد توجه قرار گرفته اند، و در شبکه های بزرگ مانند اینترنت، به طور فزاینده ای استفاده می‌شوند، ولی همواره در یک محیط بزرگ داده ها، آسیب پذیری های امنیتی رایج است. در حال حاضر که نیازهای امنیتی بیشتر مورد نیاز است، مقیاس‌های استفاده از داده ها و ادغام داده‌ها به سرعت در حال افزایش است. فن آوری بلاک‌چین، که ابتدا توسط بیت کوین معرفی شد، یک راه حل مقیاس پذیر برای بسیاری از مسائل امنیتی مشترک که در مواجهه با کلان داده ها مطرح است، ارائه می‌دهد. تکنیک های احراز هویت موجود با استفاده از سیستم های متمرکز، می توانند داده های بزرگ را بسیار در معرض خطرات و آسیب پذیرهای امنیتی قرار دهند. اکثر پروتکل های تأیید هویت بهینه شده که در محیط های توزیعی استفاده می شوند، باید از زیرساخت های غیر متمرکز که مقیاس پذیر و قابل اطمینان هستند استفاده کنند. بنابراین، پیشنهاد استفاده از مزایای فن‌آوری بلاک چین می تواند برای تقویت سیستم های امنیتی، از جمله تأیید اعتبار و مجوز دسترسی به داده ها، موثر واقع شود. چیزی که نیاز جدی درآن حس می‌شود این است که بتوان به یک سیستم احراز هویت جدید و چارجوب شناسایی جدید بر پایه تکنولوژی بلاک‌چین دست یافت.

[18] Proof of work protocol

منابع

[1] S. Alsunbul, P. Le, J. Tan, B. Srinivasan A network defense system for detecting and preventing potential hacking attempts 2016 International Conference on Information Networking (ICOIN) (2016), pp. 449-454 Kota Kinabalu.
[2] T. Zitta, M. Neruda, L. VojtechThe security of RFID readers with IDS/IPS solution using Raspberry Pi 2017 18th International Carpathian Control Conference (ICCC) (2017), pp. 316-320 Sinaia
[3] V. Chang, M. RamachandranTowards achieving data security with the cloud computing adoption framework IEEE Trans. Serv. Comput., 9 (1) (Jan.-Feb. 1 2016), pp. 138-151
[4] K. El Makkaoui, A. Ezzati, A. Beni-Hssane, C. MotamedCloud security and privacy model for providing secure cloud services 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech) (2016), pp. 81-86
[5] Y. Jin, M. Tomoishi, S. MatsuuraEnhancement of VPN authentication using GPS information with geo-privacy protection 2016 25th International Conference on Computer Communication and Networks (ICCCN) (2016), pp. 1-6 Waikoloa, HI
[6] A. Merlo, M. Migliardi, E. SpadaciniBalancing delays and energy consumption in IPS-enabled networks 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA) (2016), pp. 267-272 Crans-Montana
[7] A. Keshri, S. Singh, M. Agarwal, S.K. NandiyDoS attacks prevention using IDS and data mining 2016 International Conference on Accessibility to Digital World (ICADW) (2016), pp. 87-92 Guwahati
[8] hyperledger. Hyperledger project. https://www.hyperledger.org/, 2015.
[9] Massimo Morini. From‌ blockchain hype‌ to a real business case for financial markets. Social Science Research Network, 2016.
[10] Ibm blockchain. http://www.ibm.com/blockchain/, 2016.
[11] azure. Microsoft azure: Blockchain as a service. https://azure.microsoft.com/en-us/solutions/blockchain/, 2016.
[12] Christian Jaag, Christian Bach, et al. Blockchain technology and cryptocurrencies:Opportunities for postal financial services. Technical report, 2016.
[12] Nick Gogerty and Joseph Zitoli. Deko: An electricity-backed currency proposal. Social Science Research Network, 2011.
[14] Mike Sharples and John Domingue. The blockchain and kudos: A distributed system for educational record, reputation and reward. In Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), pages 490‌ت496, Lyon, France, 2015.
[15] G. Wood, ب‌Ethereum: A secure decentralised generalised transaction ledger,پ Ethereum Proj. Yellow Pap., vol. 151, 2014.
[16] S. Nakamoto, ب‌Bitcoin: A peer-to-peer electronic cash system,پConsulted, vol. 1, no. 2012, p. 28, 2008.
[17] ب‌Identity protocol v1 - Bitcoin Wiki.پ[Online]. Available: https://en.bitcoin.it/wiki/Identity_protocol_v1. [Accessed: 14-Jan- 2017].
[18] G. Zyskind, O. Nathan, and A. Pentland, ب‌Enigma: Decentralized Computation Platform with Guaranteed Privacy,پArXiv Prepr. ArXiv150603471, 2015.

[19] ب Hash-based message authentication code, پ Wikipedia. 14-Jan-2017.
[20] Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology. , pp. 33-48, 2015.
[21]M. Atzori, ب Blockchain Technology and Decentralized Governance: Is the State Still Necessary? پ SSRN Electronic Journal, pp. 1 ت 37, 2015.
[22]M. Pilkington, ب Blockchain technology: Principles and applications, پ pp. 1 ت 39, Sep. 2015.