مروری بر روش‌های ارتقای امنیت شبکه‌های نظارت تصویری با بهره‌گیری از بلاک‌چین

سید علی صموتی*[1] و یاسر علمی سولا[2]

[1]مدرس دانشکده شهید شمسی‌پور و دانشجوی دکتری مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی سبزوار، سبزوار، ایران
Ali.samouti@gmail.com

[2]استادیار، دانشگاه آزاد اسلامی سبزوار، سبزوار، ایران
yasser.elmi@gmail.com

چکیده

در دهه‌های اخیر، سامانه‌های نظارت تصویری گسترش فزاینده‌ای داشته که با انتشار سریع دوربین مداربسته، به‌منظور پیش‌گیری از جرم و مدیریت امکانات به کار می‌روند. فیلم‌های ذخیره‌شده در سامانه نظارت تصویری باید با آسودگی مدیریت شوند، اما گاهی اوقات فیلم‌ها به اشخاص غیرمجاز درز کرده یا توسط افراد غیر مشاهده می‌شوند و درنتیجه حریم‌های شخصی نقض می‌شوند. امروزه به دلیل افزایش تعداد جرائم، دوربین‌های مداربسته و سامانه‌های نظارت تصویری به یک ضرورت تبدیل شده‌اند؛ اما به‌دلیل ذخیره‌سازی ناامن و روش‌های اشتراک داده‌ها، دسترسی به فیلم‌های ذخیره‌شده توسط افراد غیرمجاز امکان‌پذیر می‌شود. استفاده از پروتکل‌ها و تکنیک‌های امنیتی موجود در حال حاضر چندین بار توسط مهاجمان با شکست مواجه شده است. این سامانه نیازمند یک سامانه جایگزین و یا مکمل است که نه‌تنها باید بسیار امن باشد بلکه قابلیت تغییر داده ها و تصاویر نیز ممکن نباشد. تصاویر ویدیویی ایجادشده توسط دوربین‌های نظارتی نقش حیاتی در پیش‌گیری از جرم در شهرهای هوشمند ایفا می‌کند و نیاز به یک الگو و سامانه پشتیبان برای احراز اصالت دارند. در این مقاله مروری بر روش‌ها و مقالات ارائه‌شده درزمینه کاربرد بلاک‌چین در سامانه‌های نظارت تصویری در باره امنیت تصاویر ذخیره شده، امنیت تصاویر ارسالی در شبکه های بی سیم، محرمانگی و حریم خصوصی در بازپخش ویدیو و مانیتورینگ زنده و کنترل دسترسی اپراتورها به واسطه بلاک‌چین را داریم.

واژگان کلیدی: بلاک‌چین، نظارت تصویری، حریم شخصی، کنترل دسترسی

۱- مقدمه

در دنیای امروزی شبکه‌ها در تمامی ارگان و سازمان‌های دولتی و خصوصی نفوذ کرده است و کاربران خانکی نیز از این شبکه‌ها استفاده می‌نمایند. از سویی دیگر اهمیت شبکه‌های نظارت تصویری نیز بر کسی پوشیده نیست و کاربری شبکه‌های نظارتی با اهداف کنترلی، حراستی، حفاظتی، مدیریتی و بازدارندگی نقش مهمی را در صنعت فناوری اطلاعات داشته است. [۱, ۲] در همین راستا ضبط ویدئو برای سامانه‌های امنیتی و قضایی به‌منظور بررسی پرونده‌های جنایی و حل‌وفصل اختلافات از اهمیت بسیار بالایی برخوردار است؛ زیرا این مدارک می‌تواند برای مراجع قانونی از اسناد مهم محسوب شود. بااین‌حال، ازآنجاکه این فیلم‌ها به‌واسطه‌ی تولید ابزارهای پیشرفته‌ی ویرایش در معرض دست‌کاری قرار می‌گیرند، تائید اصالت آن‌ها برای اثبات اعتبار آن در آزمایش‌ها، الزامی است. [۳] این مطلب از دیرباز موردتوجه بسیاری قرارگرفته است و قبل از ظهور بلاک‌چین با روش‌هایی نظیر الصاق نشان‌واره و یا الصاق اثرانگشت موردنقد و بررسی و پژوهش بسیاری قرارگرفته است. [۴, ۵]

سامانه نظارت تصویری و یا شبکه نظارت تصویری به‌صورت نظام‌مند شامل یک دوربین، یک بستر انتقال، یک سامانه ذخیره‌سازی و یک سامانه پخش زنده است. برای حل این مشکل، سامانهی ساخته‌شده است که کنترل دسترسی برای سامانه‌های نظارت تصویری را اعمال می‌کند، به عقیده جئونگ هنوز تحقیقات کافی برای جلوگیری از انتشار غیرمجاز تصاویر توسط مدیران برای حفظ حریم شخصی صورت نگرفته است. [۶]

سامانه‌های نظارت تصویری که به‌صورت‌های متمرکز یا نیمه‌متمرکز ارائه‌شده‌اند که با دید تمامیت (صحت) داده با نقصان مواجه هستند، بر اساس مقالات ارائه‌شده [۷, ۸] تصاویر ویدیویی ذخیره‌شده در سامانه نظارت تصویری باید با آسودگی مدیریت‌شده و به‌راحتی ذخیره و مورد بهره‌برداری قرار گیرند، اما تهدیدها و آسیب‌پذیری‌هایی برای این فیلم‌ها وجود دارد، امکان دسترسی افراد غیرمجاز به تصاویر زنده و یا آرشیوی از

*نویسندهٔ عهده‌دار مکاتبات: سیدعلی صموتی

یک‌سو و از سویی دیگر تزریق فیلم‌های جعلی در بازه زمانی خاص ممکن است علاوه بر تهدید حریم شخصی، سبب کج روی فرایندهای قضایی شود. سامانه‌های نظارت تصویری عموماً به‌صورت شکل‌های متمرکز یا نیمه‌متمرکز وجود دارد و در سامانه‌های متمرکز یک نقطه به همه گره‌ها سرویس می‌دهد و در نیمه‌متمرکز چند گره به‌صورت mirror یکدیگر قرار می‌گیرند و به‌کل مجموعه سرویس‌دهی می‌کنند. [۹, ۱۰] به‌طورکلی مشکلات سایبری که برای سامانه‌های نظارت تصویری در مجموعه‌های متمرکز یا نیمه‌متمرکز وجود دارد عبارت است از: [۱۱, ۱۲]

- بررسی دسترسی افراد به تصاویر ذخیره‌شده
- حفظ حریم شخصی تصاویر ذخیره‌شده و عدم سو استفاده
- شناسایی دست‌کاری دوربین از منظر پیکربندی در شبکه‌های وسیع
- شناسایی عملیات خرابکاری[1] روی دوربین
- صدور مجوز برای کاربران برای مانیتورینگ و ارائه کلید برای دسترسی به محتوای ویدیویی
- عدم امکان مدیریت رمز عبور یا کلیدها برای بازبینی تصاویر توسط اپراتورها در سامانه‌های سنتی و نیاز به استفاده به روش‌های قدیمی کنترل دسترسی نظیر RBAC
- عدم امکان پایش مدیریت دائمی کلیه دستگاه‌های منصوبِ در شبکه
- عدم امکان مدیریت احراز هویت و هدم امکان مدیریت دسترسی کاربران در شبکه‌های بزرگ MAN. CAN
- عدم امکان شناسایی ویدیوهای جعل‌شده
- نیاز به ارتقا امنیت در شبکه‌های پدر فرزندی و راهکارهای H.A

۱-۱- مفاهیم بلاک‌چین و سامانه‌های نظارت تصویری

آشنایی با مفاهیم بلاک‌چین و بیت کوین با انتشار یک مقاله توسط آقای ناکاماتو صورت گرفت قبل از ایشان درباره شبکه‌های توزیع‌شده تحقیقات متنوعی انجام‌شده بود و کلیه تحقیقات توسط آقای ناکاماتو به‌صورت یکپارچه ارائه گردید. پس‌ازآن شبکه‌های بلاک‌چین و رمز ارزها قوت گرفتند، به‌طور مثال آقای عباسی در کتاب خود آورده است که هش کش اولین بار توسط آدام بک در سال ۱۹۹۷ برای اثبات کار در کنترل هرزنامه ارائه گردید، همچنین اقدامات مشابه برای پازل‌های محاسباتی در سال ۱۹۹۲ توسط سینتیا دورک و می‌نی‌نائور صورت گرفت. [۶, ۱۳, ۱۴]

ظهور فناوری جدید بلاک‌چین، سبب شده است که بتوان در حریم خصوصی و امنیت داده‌ها تغییرات زیادی را ایجاد نمود. داده‌ها در سامانه بلاک‌چین در یک پایگاه داده خارج از سایت مدیریت و ذخیره می‌شود و نقش اصلی بلاک‌چین تائید درخواست دسترسی به داده توسط شخص و صدور مجوز برای کنترل و یا میزان دسترسی برای کاربر است. [۱۵]

بسیاری از افراد کاربری‌های بلاک‌چین را فقط در رمز ارزهای دیجیتال و یا برخی محدودتر کاربری را فقط در بیت کوین می‌دانند، اما بلاک‌چین پایه‌گذار بسیاری از کاربری‌ها و مکمل بسیاری از کاربردهای قبلی است، [۱۶, ۱۷] به‌طور مثال در [۱۸] مثالی از ارتباط بین بلاک‌چین و پزشکی ارائه گردیده است و یا ردیابی حمل مرغ با بلاک‌چین نیز به‌عنوان کاربرد دیگر تشریح گردیده است، کاربرد آموزش در بلاک‌چین نیز از عناوین دیگر این منبع است. اگرچه تعدادی از مطالعات و تحقیقات بر استفاده از فناوری بلاک‌چین در کاربردهای مختلف متمرکز هستند، اما هیچ نظرسنجی جامع و منسجمی در مورد فناوری بلاک‌چین و میزان پذیرش آن نزد مردم ازنظر فنی و کاربردی وجود ندارد. [۱۷]

۲- کاربرد بلاک‌چین در سامانه‌های نظارت تصویری

فراتر از مبحث مهم امنیت، کاربردهای متنوع دیگری از بلاک‌چین در محیط اینترنت اشیا وجود دارد که می‌تواند شامل موارد زیر بشد: [۱۹]

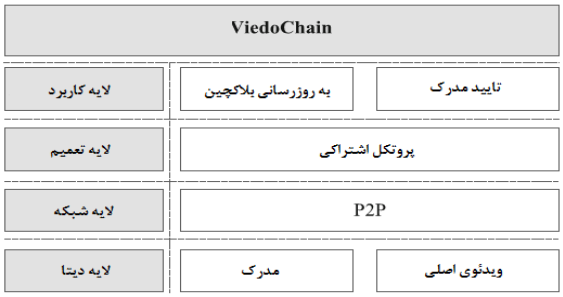
برخی از مطالعات، بلاک‌چین و تصویربرداری و الگوریتم‌های پردازش تصویر ویدیویی را ترکیب می‌کنند و کاربردهایی نظیر مبارزه با جعل ویدیو عمیق، پردازش تصویر پزشکی، رمزگذاری تصویر و مدیریت حقوق محتوای دیجیتال را به کمک بلاک‌چین ایجاد می‌کنند. [۸]

معرفی بلاک‌چین در سامانه نظارت تصویری معتبر کار ساده‌ای نیست. چالش‌هایی در این مسیر همراه است: ذخیره‌سازی اسناد و داده‌های اصلی، پروتکل اجماع ویژه، قدرت پیچیدگی داده‌ها. زنجیره ویدیویی یک نمونه از

[1] Tampering

کاربری‌های بلاک‌چین است. زنجیره ویدیویی بر اساس معماری بلاک‌چین از چهار لایه ساخته‌شده است [۲۰]

(شکل-۱): کاربردهای مهم بلاک‌چین در اینترنت اشیا



(شکل-۲): لایه‌های زنجیره ویدیویی منطبق با لایه‌های بلاک‌چین [۲۰]

یکی نکته مهم در بلاک‌چین ایجاد یک پروتکل لایه‌بندی است. درروش زنجیره ویدیویی لایه‌بندی با توجه به شکل (۲) در ۴ لایه‌ایجادشده است، در لایه دیتا لینک تمرکز روی اصل تصویر ویدیویی و مدارک آن است. در لایه شبکه، روی تعمیم شبکه بلاک‌چین و شبکه‌های توزیع‌شده تمرکز صورت گرفته است تا بتوان یک تصویر و یا داده‌های دوربین به‌واسطه آن انتقال یابد. در لایه تعمیم پروتکل‌های اشتراکی برای قرارداد هوشمند روش‌هایی بیان‌شده است تا گام اول اجماع صورت پذیرد و درنهایت در لایه کاربرد، با استفاده از PoS[1]تائید تصویر یا مدارک دوربین صورت پذیرد و بلوک نهایی شود. [۲۰]

از سویی دیگر در [۲۱] اهمیت نظارت تصویری در مراکز تجزیه‌وتحلیل نظارت تصویری یا SAC[2] بسیار مهم اشاره‌شده است و این مراکز در گزند تهدیدهایی نظیر جعل، تغییر و وقفه هستند و احتمال نشت اطلاعات بسیار بالا است. مراکز سنتی به‌هیچ‌عنوان تضمینی در صحت داده و یا تغییر داده را ندارند و فقط در تحقیقات علمی به آن اشاره‌شده و به هیچ صورت به‌عنوان یک فناوری به بازار عرضه نشده است. سامانه‌های نظارت تصویری سنتی برای اشتراک‌گذاری و حفظ حریم شخصی یا SePriS[3] هیچ مصونیتی ندارند. در [۲۱] مکانیسم‌هایی برای SePriS به روش بلاک‌چین اشاره‌شده است؛ که بر مبنای قراردادهای هوشمند و رمزگذاری فریم‌ها بر اساس DAB[4] و تبدیل کسینوسی گسسته پایه‌گذاری شده است. [۲۱]

در سامانه‌های بلاک‌چین و ترکیب آن با سامانه‌های نظارت تصویری می‌توان تصاویر را رمزینه کرد و مدیریت کلید (گذرواژه کاربران و یا کلیدهای مربوط به دوربین‌ها در بستر https) را به‌واسطه مدیر سامانه انجام داد. این کار بااعتبار سنجی روی دیتا بیس مرکزی و توزیع آن در شبکه توزیع‌شده صورت می‌گیرد. سامانه نظارت تصویری مبتنی بر بلاک‌چین می‌تواند به‌طور امن دسترسی افراد خارجی و مدیران داخلی را مدیریت کندو یا مدیریت کاملی بر روی موجودیت‌ها داشته باشد. همچنین، مدیریت رکورد هدف که آیا صدور ویدیو به‌خوبی مدیریت می‌شود، امکان‌پذیر است. [۷] راه‌کارهای دیگر ارائه‌شده روشی مقرون‌به‌صرفه برای احراز هویت داده‌ها برای دوربین‌های نظارت تصویری است که می‌تواند برای اینترنت اشیا در یک شهر هوشمند بسط داده شود. [۸]

درروش ذخیره‌سازی تصاویر ویدیویی سنتی هیچ تضمینی وجود ندارد که فیلم ویدئویی به‌دست‌آمده به‌صورت دیجیتالی دست‌کاری نشده باشد. این امر مستلزم راه‌کاری است که بتواند اثبات‌کننده‌ی یکپارچگی اطلاعات نظارت تصویری ردوبدل شده بین دستگاه‌ها باشد تا لایه‌های مختلف و ارگان‌های متفاوت بتوانند بر اساس میزان اهمیت و اعتماد موردنیاز از آن بهره‌برداری نمایند و برای توسعه و دوری از سامانه‌های متمرکز می‌توان از الگوریتم‌های اجماع در روش‌های توزیع‌شده اشاره کرد. [۲۲] ازآنجاکه فیلم‌های آرشیوی سامانه‌های نظارت تصویری به‌واسطه‌ی تولید ابزارهای پیشرفته‌ی ویرایش در معرض دست‌کاری هستند، تائید اصالت آن‌ها برای اثبات اعتبار آن در مجتمع‌های قضایی یا اداری، الزامی است. [۳]

سامانه نظارت تصویری به‌عنوان عضوی از ابزار اینترنت اشیا و شهر هوشمند محسوب می‌شود همواره بحث امنیت سایبری و محافظت و صیانت از داده‌ها یک

[1] Proof of Stake
[2] surveillance analytics centers centers
[3] Privacy-preserving Stored surveillance video sharing
[4] Digital audio broadcasting

امر محب است و برای بهبود این روش از بلاک‌چین استفاده‌شده است تا بتوان سامانه‌های نظارت تصویری را اثربخش نمود به‌طور مثال یک روش ارائه‌شده استفاده از اترنیوم است که برای مقابله با DDOS و حمله انکار توزیع‌شده روش‌هایی ارائه‌شده است که شبیه‌سازی آن در سال ۲۰۱۸ صورت گرفت. این روش بلاک‌چین می‌تواند برای سامانه‌های نظارت تصویری پرکاربرد باشد. [۴, ۸]

اینترنت اشیا نیز می‌تواند از بلاک‌چین برای اطمینان از صحت داده‌های موجود در کسب‌وکار استفاده نماید. به دلیل محدودیت‌های رایج موجود در نودهای اینترنت اشیا، استفاده از یک شبکه کاملاً امن بلاک‌چین درزمینهٔ IoT عمومی در حال حاضر نمی‌تواند عملی باشد. بااین‌حال، برخی از کاربردهای مانند شبکه‌های هوشمند، ITS، بهداشت الکترونیکی، بیمه که بر اساس محیط‌های قرارداد هوشمند است، ممکن است قابلیت‌های کافی برای پشتیبانی از قابلیت P2P و شبکه‌های توزیع‌شده را در برداشته باشد. این بدان معنی است استفاده از بلاک‌چین برای پیام‌های پشتیبانی، شناسایی، جستجوی تراکنش‌ها، فراخوانی، همگام‌سازی و اشتراک‌گذاری، می‌تواند به پهنای باند کمتر نیاز داشته و صحت داده تحویلی را در یک شبکه بسیار بزرگ تضمین نماید. سطوح مختلف نیازهای عملیاتی موردنظر برای کاربران در این رویکردها عبارت‌اند از: بلاک‌چین های انتها به انتها، سطح تجزیه‌وتحلیل یا ذخیره‌سازی، سطح ورود و خرج، سطح سایت، سطح دستگاه. [۱۹]

۲-۱- چالش‌های امنیتی ازنظر سامانه‌های نظارتی

مشخصاً سامانه‌های نظارت تصویری تحت شبکه عامل بازدارنده و محافظ مایملک در تأسیسات صنعتی و منازل است. در ده سال اخیر این سامانه‌ها با پیشرفت شگرفی روبرو شده‌اند، اما این پیشرفت سبب شده است که حملات و تهدیدهای متنوعی در کمین این سامانه‌ها قرار بگیرند. [۱۰] بنابراین، دسترسی غیرمجاز به این سامانه‌ها پیامدهای جدی امنیتی را به همراه خواهد داشت. در سامانه‌های سنتی برای سامانه‌های متمرکز روش‌هایی برای امن سازی ارائه‌شده است، اما بسیاری از این روش‌ها نمی‌تواند سبب تضمین تمامیت (صحت) داده شود. [۱۲]

به‌طور مثال یکی از نگرانی‌های اصلی دست‌کاری پیکربندی دوربین و یا تغییر زاویه دید تک دوربین در یک شبکه بسیار بزرگ است و ممکن است دوربین منصوبه در یک منطقه حساس باشد. مشخصاً بسیاری از شبکه‌های نظارت تصویری دارای هزاران دوربین است و دست‌کاری یک دوربین در زمان مربوطه یا فی‌الفور مشخص نخواهد شد؛ و ممکن است مدیریان و سرپرستان از آن تغییر در زمان مقتضی اطلاعی پیدا نکنند و در همان زمان سرپرستان و تکنسین‌های خرابکار خواهان خرابکاری و آسیب‌رسانی به سامانه باشند. این اقدامات مخرب و دست‌کاری‌ها ممکن است تأثیرات منفی داشته باشد: تغییر صحنه‌های موردنظر و نقض حریم شخصی همسایگان و یا تغییر فوکوس دوربین می‌تواند آسیب‌پذیری سامانه را افزایش و استحکام سامانه را کاهش دهد. ممکن است یک نصاب به دلایل نامعلوم خواهان خرابکاری باشد و پس از تحویل پروژه به نحوی پیکربندی دوربین را تغییر دهد و نیاز است که در شبکه فردی که پیکربندی را تغییر داده است مشخص شود، به کمک بلاک‌چین می‌تواند عدم انکار را در این مورد کاهش داد. [۱۶]

در حال حاضر معماری بسیاری از سامانه‌های نظارت تصویری به‌صورت متمرکز و یا نیمه‌متمرکز می‌باشد. در حالت نیمه‌متمرکز چند سرور به‌صورت افزونه یا آینه‌ای باهم کار می‌کنند. در حالت متمرکز در صورت ازکارافتادن سامانه مرکزی، کل سامانه دچار اختلال خواهد شد، ولی در سامانه‌های نیمه‌متمرکز تا حدی مشکل از کار فتادن سامانه یا Sigle point of failure برطرف گردیده است، اما با ظهور شبکه‌های توزیع‌شده و شبکه‌های بلاک‌چین افق جدیدی برای کاربری و بهینه‌سازی شبکه‌ها ایجادشده است تا در صحت و تمامیت داده بتوان اعتماد بیشتری داشت. [۱, ۲]

در سامانه‌های متمرکز یا نیمه‌متمرکز تهدیدهای مختلفی از دید مثلث امنیت یا CIA وجود دارد و برای برخی از آن‌ها در روش‌های متمرکز راه‌کارهایی عرضه‌شده است. [۱۲, ۲۳]. یکی دیگر از مشکلات ذخیره‌سازی، در سامانه‌های پدر-فرزندی است و در این سامانه‌ها که چند سرور در لایه‌های مختلف قرار می‌گیرد، از صحت ذخیره‌سازی و عدم‌تغییرپذیری آن باید اطمینان حاصل نمود. [۲۰]

آقای چریسن واکاس برای تضمین قابلیت اعتماد ضبط تصاویر ذخیره‌شده، روش استفاده از دفتر توزیع‌شده برای داده‌های ویدیویی را ارائه کرده است که به مراجع قضایی اجازه می‌دهد تا تغییر اطلاعات را تائید کند. در این روش ضمن کنترل و احراز هویت دوربین و عملکرد آن

نظیر (مانند پلاک خوانی)، به کمک بلاک‌چین امنیت را بالاتر برده و جعل ویدیویی را کاهش داده است. [۸]

ازآنجاکه سامانه‌های نظارت تصویری با آنالاتیک همگام شده‌اند و هوشمند سازی به‌عنوان جزئی از این سامانه‌ها محسوب می‌شود و آلارم های تولیدشده از این سامانه‌ها بسیار کلیدی و حیاتی است، مدیریت صحت و تمامیت داده‌ها اهمیت بالایی دارد، مشکلات مختلفی ازجمله مسأله محافظت از حریم شخصی و یا محافظت از تغییر داده ممکن است در این مسیر چالش‌هایی را ایجاد نماید، لذا نیاز است که در برابر حملات جعل و تحریف مقاوم بوده و برای محیط‌های نظارت هوشمند چندرسانه‌ای مبتنی بر هوش مصنوعی مناسب باشد. برای پردازش امن ویدئو دوربین مداربسته مبتنی بر بلاک‌چین، داده‌ها نباید درروند انتقال از بین بروند و یا استریم ویدیو اصلی آسیب ببیند. علاوه بر این، داده‌های ویدئویی دوربین مداربسته اندازه و حجم بسیار بالایی دارد و برای همگام‌سازی به پهنای باند گسترده‌ای نیاز دارد؛ بنابراین نیاز است که راه‌کار دیگری غیر از ارسال همه تصاویر یا بخشی از تصاویر در نظر گرفته شود؛ بنابراین، حتی هنگامی‌که مقدار زیادی از داده‌های ویدئویی با استفاده از روش‌های مختلف به‌صورت هم‌زمان تکثیر می‌شوند باید الگویی تهیه شود و داشتن حداقل پهنای باند و پردازش مؤثر، یکی از الزامات مهم به شمار می‌رود. [۲۴]

دوربین‌های مداربسته و بلاک‌چین چالش‌ها و مشکلاتی نیز دارد، به‌طور مثال برخی از چالش‌ها عبارت‌اند از: فقدان حریم خصوصی، مدل امنیتی، مقیاس‌پذیری محدود، هزینه بالا، مرکزیت پنهان، عدم انعطاف‌پذیری و اندازه بحرانی. همچنین از محدودیت‌های غیر فنی بلاک‌چین می‌توان به فقدان پذیرش قانونی و اعتماد کاربران اشاره کرد. [۱۴, ۱۸, ۲۵, ۲۶]

یکی از کاربردهای دوربین مداربسته در ارسال تصویر، ماسک کردن بخشی از تصویر است تا حریم شخصی همسایگان حفظ شود و این امر در لایه خود دوربین صورت می‌گیرد و سبب می‌شود اصالت تصویر از بین برود و در صورت نیاز به بخشی از تصویر ماسک شده هیچ راهی وجود ندارد، اما به کمک روش درخت مرکل می‌توان روی فریم اصلی ماسکی را ایجاد نمود و اصل تصویر ذخیره شود و برای بازپخش لایه‌های مختلف ماسک شده روی تصویر اصلی اضافه شود. [۲۴]

استریم های مختلفی برای سامانه‌های نظارت تصویری وجود دارد و پروتکل‌های متعددی مورداستفاده قرار می‌گیرد. مقاله‌ی خوان بنت در مورد کاستی‌های استفاده فعلی از Http و خدمات وب ارائه‌شده توسط آن و چگونگی بی‌ربط بودن آن به‌زودی در آینده، در مورد انتقال و پخش پرونده‌های بزرگ بحث نموده است. Http برای فایل‌های کوچک مناسب است و هنگام انتقال تعداد زیادی از آن‌ها هزینه بسیار کمتری صرف می‌شود، اما وقتی صحبت از داده‌های بسیار بزرگ‌تر می‌شود، کار کمی سخت است. [۱۵]

مقاله‌ای از اریک ال پیزا، جوئل ام کپلان، لزلی د کندی و اندرو ام گیلچریست در مورد موضوعات نظارت بر دوربین مداربسته و اقدامات ایمنی کافی در موارد اضطراری در مناطق خاصی از نیوآرک، نیوجرسی، بررسی‌هایی انجام داده است. در این مقاله به دو مانع اصلی یعنی نسبت زیاد تعداد دوربین‌ها به هر اپراتور و مکانیسم عکس‌العمل متفاوت پلیس و واکنش وی برای هر رویداد، پرداخته‌شده است. روش‌های موردبحث و استفاده یک آزمایش مبتنی بر منطقه و طراحی بلوک است. این آزمایش توسط تیم و مقامات پلیس بر اساس مناطقی که دوربین‌های مداربسته در آن‌ها مستقرشده‌اند طراحی‌شده است. در این تحقیق، استفاده‌ی ترکیبی از این مکانیسم‌های فنی و فیزیکی در مقایسه با استقرار مستقل دوربین مداربسته یک موفقیت بزرگ بوده و به‌طور مؤثر از وقوع جرم به‌ویژه در سناریوهای خیابانی جلوگیری می‌کند. [۱۵]

۲-۲- تعریف بلاک‌چین بادید سامانه‌های نظرات تصویری

بلاک‌چین از دو کلمه بلوک و زنجیر تشکیل‌شده است، در حقیقت این فناوری مجموعه‌ای از بلوک‌ها است که به یکدیگر متصل شده‌اند. در بلاک‌چین اطلاعات در بلوک‌ها قرار می‌گیرند و باهم به‌صورت زنجیره مرتبطی شوند. بلاک‌چین یک نوع سامانه ثبت اطلاعات، گزارش‌ها و یا تراکنش‌ها است. [۱۳] در کتاب آقای خوانساری عنوان‌شده است که ایده‌های شبکه‌های نظیر به نظیر، معماری محاسباتی هش، سازوکار توافق، تکثیر ماشین حالت و طرح‌های پول الکترونیکی در اختراع بلاک‌چین نقش اساسی داشته‌اند. [۲۶] از یک دیدگاه، دو روش برای تعریف بلاک‌چین عنوان‌شده است: ۱- بلاک‌چین به‌عنوان یک ساختار داده، ۲- بلاک‌چین به‌عنوان یک الگوریتم، [۱۸, ۲۵, ۲۶]

آقای زیبین جینگ معتقد است، فناوری بلاک‌چین زمانی محبوبیت خود را به دست آورد که افراد در سراسر

جهان شروع به استفاده از بیت کوین کردند. فناوری‌هایی مانند بلاک‌چین در دنیایی پر از مهاجم و حملات مخرب که سعی در استفاده از روزنه‌ها و رخنه‌ها در سامانه‌های موجود دارند، نقشی حیاتی دارند. [۱۵]

۲-۳- مزایا و معایب بلاک‌چین بادید سامانه‌های نظارت تصویری

مزایای سامانه‌های توزیع‌شده در کتاب [۲۵] عنوان‌شده است که از آن موارد می‌توان به این موارد اشاره کرد: قدرت پردازش بالاتر، کاهش هزینه‌ها، قابلیت اعتماد بیشتر و توانایی توسعه و ارتقا طبیعی (خود به خودی) عنوان گردیده است.

همچنین معایب این سامانه‌ها هزینه سربار هماهنگی یا همکاری بین بخش‌های مختلف، هزینه سربار ارتباطات، وابستگی به شبکه، پیچیدگی بالای برنامه (ازنظر ساختار الگوریتم) و مسائل امنیتی است. [۱۸, ۲۶]

در بحثی دیگر مزایا و قابلیت‌های مهم بلاک‌چین با عناوین ذیل عنوان‌شده‌اند: تمرکززدایی، شفافیت و اعتماد، تغییرناپذیری، دسترس‌پذیری بالا، امنیت بالا، ساده‌سازی الگوهای فعلی تسریع معاملات، صرفه‌جویی در هزینه‌ها. همچنین بر اساس همین کتاب مشکلات بلاک‌چین مقیاس‌پذیری، سازگاری، تنظیم مقررات، نو پا بودن فناوری و حریم خصوصی عنوان‌شده است. [۲۶]

سامانه‌های نظارت تصویری متمرکز دارای نقص‌ها و آسیب‌پذیری‌هایی است. فیلم‌های دوربین مداربسته برای تحقیقات قانونی ضروری است، در این راستا، فناوری بلاک‌چین برای این کاربرد در دو سال گذشته، بسیار موردتوجه قرارگرفته است و کاربرد قرارداد هوشمند و سامانه‌های نظارت تصویری موردتوجه محققین قرارگرفته است. بر این اساس یکی از محدودیت‌ها برای پیاده‌سازی سامانه نظارت تصویری و بلاک‌چین پهنای باند و حجم داده‌های تصاویر است.

یک روش پیشنهادی قبل از خروج از دوربین این است که هش داده‌های ویدیو را برای اطمینان از یکپارچگی و تمامیت محاسبه می‌کند. پس‌ازآن، هش در یک پلتفرم مبتنی بر بلاک‌چین ذخیره می‌شود که تشخیص دست‌کاری در ویدئو را امکان‌پذیر می‌کند. این جریان مداوم به‌طور کارآمد تقسیم می‌شود تا دارای مقدار هش دوره‌ای باشد و بدین ترتیب خطر پاک شدن یا تغییر فیلم در صورت خرابی دستگاه را به حداقل برساند؛ اما مشکل ترافیک و حجم پردازنده‌ها و افزایش نیاز مصرف پردازش از مشکلات مهم به شمار می‌رود. [۳]

۲-۴- سازوکار فنی بلاک‌چین و ارتباط با سامانه‌های نظارت تصویری

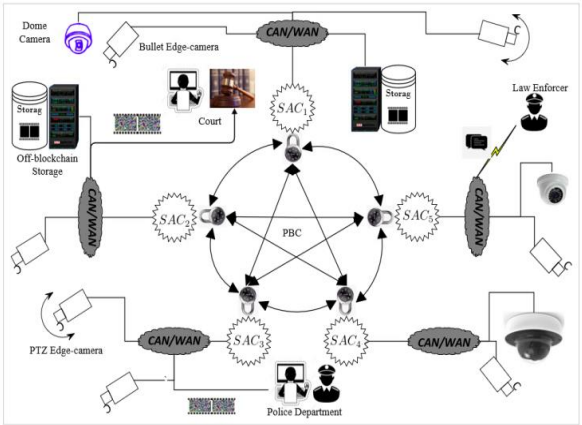
مطابق با تعریف بلاک‌چین که زنجیره بلوک‌ها نامیده می‌شود، یک بلوک درواقع مجموعه‌ای از تراکنش‌ها است که به شکل منطقی در یک واحد بسته‌بندی و سازماندهی‌شده است. یک تراکنش می‌تواند ثبت یک رویداد مثلاً تراکنش مالی و یا ذخیره‌سازی مدت‌زمانی از یک فیلم دوربین مداربسته باشد. یک بلوک از یک تعداد تراکنش ساخته‌شده است و اندازه آن بسته به طراحی بلاک‌چین دارد و می‌تواند متفاوت باشد. حلقه اول زنجیر جنسیس بلوک یا بلوک آغازین نام دارد و دستی نام‌گذاری می‌گردد. ساختار و بنای هر بلوک بر اساس نظر سازنده آن است که معمولاً سرایند بلوک شامل اشاره‌گر به بلوک قبلی، مهر زمانی، نانس، ریشه درخت مرکل تراکنش‌ها و بدنه بلوک است، البته مؤلفه‌های دیگر نیز می‌تواند در این سازوکار نقش داشته باشد. [۲۶]

یکی از موارد مهم برای سازوکار بلاک‌چین تفاهم و یا اجماع است. مفهوم اجماع بدان معناست که کلیه گره‌ها برای رسیدن به توافق نهایی با یکدیگر مباحثه کرده و به توافق برسند. در روش‌هایی نظیر متمرکز یا نیمه‌متمرکز بین دو گره اجماع به‌راحتی صورت می‌گیرد اما نکته مهم در شبکه توزیع‌شده است که تعداد مشخص و یا نامشخص گره به شبکه اضافه‌شده است. برای رسیدن به توافق در این حالت نیاز به یک روشی مشابه یک چالش پرسش و پاسخ است و نتیجه اجماع فرایند توزیع‌شده است. در یک الگوریتم توافق نیازمندی‌های اساسی همچون توافق، خاتمه، صحت، تحمل‌پذیری خطا و یکپارچگی وجود دارد. برخی از روش‌هایی که برای چالش اجماع وجود دارد عبارت‌اند از: اثبات کار، اثبات سهم، اثبات سهم نیابتی DPoS، اثبات زمان سپری‌شده، اثبات سپرده PoD، اثبات اهمیتPoI ، اثبات هم‌پیمان، اثبات فعالیت PoA، اثبات ظرفیتPoC ، اثبات ذخیره‌سازی PoS. [۱۴, ۱۸, ۲۶]

مقاله‌ای از آندره بیندر و ایوان کوتولیاک نیز کار و اهمیت شبکه‌های ارائه‌ی محتوای ویدیویی را به‌طور واضح توضیح داده است. این سامانه در لایه کاربرد معماری شبکه فعالیت می‌کند و به ارائه داده‌های دیجیتالی مانند فیلم‌ها و عکس‌ها به بسیاری از نقاط انتهایی بدون هیچ‌گونه تغییر در ساختار اصلی شبکه کمک می‌نماید. در

این راستا، سامانه پیشنهادی نظارت مؤثر بر زیستگاه و قابلیت ردیابی را برای کشاورزان ارائه می‌دهد و می‌تواند درزمینه‌ُهای دیگر مانند مدیریت گلخانه، مدیریت انبار و غیره نیز به کار گرفته شود. [۱۵]

مدل تعامل بلاک‌چین-کاربر (Blockchain-user) سه لایه مهم شامل لایه کاربرد، لایه دیتا و لایه حسگر را معرفی می‌کند. لایه کاربرد شامل برنامه‌های کاربری است که توسط کلاینت‌ها و مدیران شبکه اجرا می‌شود. کاربران می‌توانند با استفاده از مرورگرهای وب یا برنامه‌های کاربری، داده‌ها را انتخاب کرده و بازیابی کنند. تبادل داده‌ها در لایه میانی رخ می‌دهد که از بلاک‌چین تشکیل‌شده است. لجر توزیع‌شده به‌عنوان نقطه احراز هویت و تأیید داده‌ها و متادیتاهای دوربین‌های نظارتی عمل می‌کند. قوانین مختلف و قراردادهای هوشمند نیز بر روی این لایه اجرا می‌شوند. این قوانین باید هماهنگ با کاربران، مراجع نظارتی و ارائه‌دهندگان زیرساخت‌ها تدوین شود؛ بنابراین تعهدات مبتنی بر قرارداد هوشمند، مانند معاملات داده‌ها و دارایی‌های فیزیکی، به دلیل اعتماد متقابل به بلاک‌چین قابل تسویه است. لایه حسگر شامل سنسورهای تصویر یا دستگاه‌های نظارتی است که همان دوربین‌های مداربسته هستند. بلاک‌چین به‌منزله‌ی ستون فقرات در برخی از سامانه‌ها پیشنهادشده است. این برنامه بدون نیاز به‌واسطه به دلیل قابلیت‌های قرارداد P2P و هوشمند کار می‌کند. علاوه بر این، اعتماد در میان ذینفعان همواره الزامی نیست؛ زیرا فناوری پلتفرم دفتر توزیع‌شده، ویژگی‌های رمزگذاری و ردیابی کامل هر بلوک را ارائه می‌دهد. [۸]

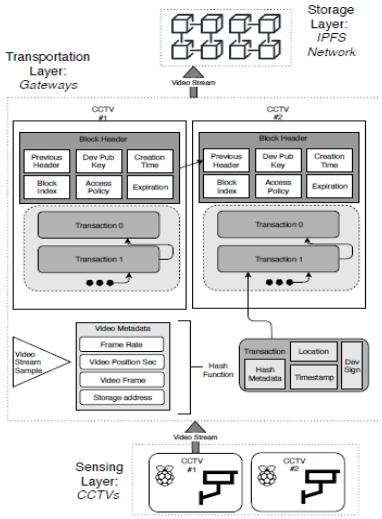


(شکل-۳): معماری روش حفظ حریم شخصی و امنیت در شبکه بلاک‌چین برای دوربین نظارت تصویری [۲۱]

شکل (۳) نحوه ذخیره فیلم‌های نظارتی را نشان می‌دهد. دسترسی ایمن توسط کاربران مجاز با استفاده از PBC مبتنی بر رویکرد را می‌توان به کمک آن پیاده‌سازی نمود. در درجه اول، اداره پلیس، دادگاه‌ها به تصاویر دسترسی دارند و کاربران ویدیوهای نظارتی ذخیره‌شده برای اهداف تحقیقاتی و پزشکی قانونی یا به‌عنوان شواهدی علیه جنایتکاران در دادگاه‌های حقوقی می‌توانند ارجاع دهند و ادله عدم‌تغییر را داشته باشند. شبکه بلاک‌چین می‌تواند توسط سازمان‌های بالادستی مدیریت شود. می‌توان اصل فیلم را نیز ذخیره نمود. یک ابر ذخیره‌سازی خارج از بلاک‌چین، ده مرحله انجام می‌شود درخواست‌کننده، گره‌های BC و ذخیره‌سازی خارج از بلاک‌چین. هر یک از مراحل در مقاله [۲۱] به‌طور کامل اشاره‌شده است.

روش دیگری برای محافظت داده‌ها توسط درخت مرکل اشاره‌شده است. این روش به‌صورت درختواره بر اساس مرکل هش اصلی را حساب می‌کند. هش ها برای داده‌های متادیتا به کار می‌رود؛ اما بلاک‌چین مبتنی بر Merkle-Tree از کنترل نسخه برای فایل داده‌های ویدیویی دوربین مداربسته پشتیبانی نمی‌کند. بااین‌حال، در محیط دوربین مداربسته، مدیریت نسخه‌های مختلف مانند Privacy Masking موردنیاز است تا بتوان ماسک زنی را به‌صورت لایه‌ای انجام داد. ازاین‌رو، یک روش پیکربندی Merkle-Tree جدید برای نظارت بر دوربین مداربسته موردنیاز است. در [۲۴] روش جدیدی ارائه‌شده است که امکان همگام‌سازی ایمن متادیتا و ویدئوی موردنیاز برای نظارت تصویری دوربین مداربسته را فراهم می‌کند. فناوری پیشنهادی مبتنی بر فناوری بلاک‌چین با استفاده از فناوری SM-Tree که فناوری موجود Merkle-Tree را بهبود می‌بخشد، دارای ویژگی‌هایی از قبیل پیشگیری از جعل ویدئو، کاهش پهنای باند، محافظت از حریم خصوصی اشیا و هماهنگ‌سازی کارآمد و ایمن ابر داده‌ها برخوردار می‌باشد در همین مقاله روش ماسک زنی چندگانه تصویر برای فریم‌های متعدد پیشنهادشده است. [۲۴]

در شکل (۴) چگونگی تشکیل بلوک متادیتا دوربین و تصاویر در کنار هم نشان داده‌شده است. دوربین‌ها در لایه دوربین اقدام به تشکیل بلوک می‌نمایند و برای بلاک‌چین ارسال می‌کنند. یکی از مشکلات این روش نیاز به پشتیبانی سامانه توسط سازندگان است. سازندگان دوربین به دلیل آنکه محدودیت پردازشگر دارند، معمولاً کیفیت تصویر را اولویت قرار می‌دهند و نمی‌خواهند کیفیت تصویر فدای روش‌هایی نظیر این روش شود و شاید در حاضر مورد استقبال سازندگان قرار نگیرد.



(شکل-۴): چگونگی ایجاد تراکنش‌های ویدیویی متادیتا [۲۲]

۳- راه‌کارهای ارائه‌شده توسط بلاک‌چین برای امنیت شبکه‌های نظارت تصویری

در مقالات مختلف روش‌های مختلفی را برای کاربرد بلاک‌چین در سامانه‌های نظارت تصویری ارائه داده‌اند که در این بخش به معرفی برخی از آن‌ها می‌پردازیم:

۳-۱- ارائه راه‌کار برای جلوگیری از تغییر و انحراف پیکربندی دوربین

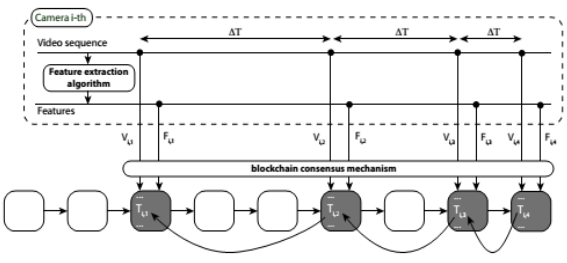
یکی از نگرانی‌ها در سامانه‌های نظارت تصویری جلوگیری از دست‌کاری سامانه‌های نظارت تصویری است. یکی از راهکارهای ارائه‌شده blocksee است که به‌طور مشترک قابلیت اطمینان و تغییرناپذیری، پیکربندی دوربین و فیلم‌های نظارتی را فراهم می‌کند و گزارش این رویدادها را در صورت وقوع، به‌راحتی در دسترس کاربران مجاز قرار می‌دهد. BlockSee با ردیابی پیکربندی دوربین، از طریق تجزیه‌وتحلیل فتوگرامتری سبک فریم‌های دوربین در زمان تحویل به کاربر نهایی، یا به هنگام انجام دست‌کاری‌های احتمالی توسط خرابکاران، می‌تواند چنین مسائلی را ردیابی کند. [۱۶]

قبل از روش block see، گریپ برای دوربین‌های داشبورد ماشین‌ها با استفاده از هش و رمزنگاری، تمامیت داده را تضمین کرد و الگوریتمی را ارائه داد تا صحت تصاویر ذخیره‌شده تضمین شود و دست‌کاری آن‌ها صورت نپذیرد تا در صورت نیاز برای بازبینی پلیس اعتبار سنجی تصویر امکان‌پذیر باشد. همچنین هلمین و هوس، الگوریتم‌های هش را برای یکپارچگی و تمامیت ارائه داد تا بتوان تصاویر را روی شبکه بلاک‌چین ذخیره نمود. [۱۶]

درروش Blocksee دو گام تعریف‌شده است، در گام اول تقسیم‌بندی صورت می‌گیرد و فریم‌های ویدیویی را تقسیم‌بندی می‌کند و به‌واسطه آن پس‌زمینه و پیش‌زمینه تشخیص داده می‌شود و در گام دوم استخراج ویژگی و استنباط تنظیمات صورت خواهد پذیرفت. در این روش سه سطح مختلف دوربین‌ها، گره‌ها و هسته اصلی بلاک‌چین تعریف می‌گردد. این سامانه به‌صورت مجوز دار است که در آن تنها گره‌هایی که به یک لیست سفید تعلق دارند می‌توانند هش های بخش‌های ویدئویی را در بلاک‌چین و همچنین متادیتای آن‌ها (موقعیت و جهت دوربین، برای بازیابی سریع داده‌ها) اضافه نمایند. [۱۶]

وقتی تکنسین‌ها دوربین‌ها را نصب یا نگهداری می‌کنند، ممکن است تغییراتی در تنظیمات آن اعمال کنند. نصب کنندگان و تکنسین‌ها همواره نمی‌توانند مورد اعتماد باشند و ممکن است به‌عمد دوربین‌ها را با تنظیمات دلخواه خود و گاه همراه با تخلف تنظیم کرده و پس‌ازآن، با نسبت دادن تنظیمات مخرب قبلی، از این اقدام غیرقانونی خود شانه خالی کنند. همان‌طور که در BlockSee پیشنهادی ارائه‌شده است، حتی پاسخگویی ساده در این سامانه‌ها نیز یک هدف ارزشمند است. هرگونه تغییر غیرقابل پاسخگویی یا غیرمجاز در تنظیمات دوربین به‌طور دائمی در بلاک‌چین ثبت می‌شود و به‌موقع می‌توان با آن مقابله نمود. [۱۶]

اعتبار بلوک‌ها توسط یک تعامل هوشمند BlockSee بررسی می‌شود. باید توجه داشت، داده‌هایی معتبر هستند که توسط یک دوربین تائید (امضا) شوند. جریان‌های ویدیویی بدون امضا توسط BlockSee پردازش نمی‌شوند زیرا معتبر نیستند. همچنین فریم‌هایی که از دوربین‌های قدیمی وارد می‌شوند نیز نمی‌توانند وارد BlockSee شوند، زیرا با آن سازگاری ندارند شکل ۵ این روش و فریم‌ها و هش های دوربین‌ها در بازه زمانی مشخص را نشان می‌دهد در این بلوک‌ها کلیه تغییر تنظیمات نیز ثبت خواهد شد. [۱۶]



(شکل-۵): الگوی ارتقا امنیت برای جلوگیری از چرخش دوربین یا تغییر پیکربندی [۱۶]

۳-۲- راه‌کارهایی برای جلوگیری از نقض حریم شخصی

فناوری بلاک‌چین اساساً یک بانک اطلاعاتی غیرمتمرکز، مشترک و تغییرناپذیر است که رجیستری دارایی‌ها و معاملات را از طریق شبکه همتا به همتا (P2P) ذخیره می‌کند. برای حل این مشکل، سامانهی ساخته‌شده است که کنترل دسترسی را بر روی سامانه نظارت تصویری اعمال می‌کند. تیمو و همکاران در مقاله خود در مورد قراردادهای هوشمند، درباره امکاناتی که برای جایگزینی روش سنتی قراردادها و توافق‌نامه‌ها با استفاده از فناوری بلاک‌چین دارند، بحث کرده‌اند. به دلیل ماهیت نامشهود، می‌توان به آن کمک کرد تا تراکنش‌ها را جایگزین آن کند. در این سامانه از معماری مشابهی استفاده‌شده است که در آن توافق‌نامه چند سطحی در مورد هر معامله‌ای که باید روی‌داده‌های فیلم‌برداری ذخیره‌شده در IPFS انجام شود، موجود می‌باشد. بررسی مقالات فوق منعکس‌کننده مرزبندی فن‌آوری‌های مدرن ازنظر امنیت و کارایی است. تکنیک‌های اشتراک داده مانند IPFS و CDN در مقایسه با سامانه‌های پایگاه داده‌های سنتی بسیار سریع‌تر و ایمن‌تر هستند. این پایگاه‌ها را می‌توان به روشی به‌هم‌پیوسته و کارآمد برای دستیابی به یک سامانه کارآمدتر و ایمن‌تر نسبت به سامانه موجود، پیاده‌سازی نمود. [۱۵]

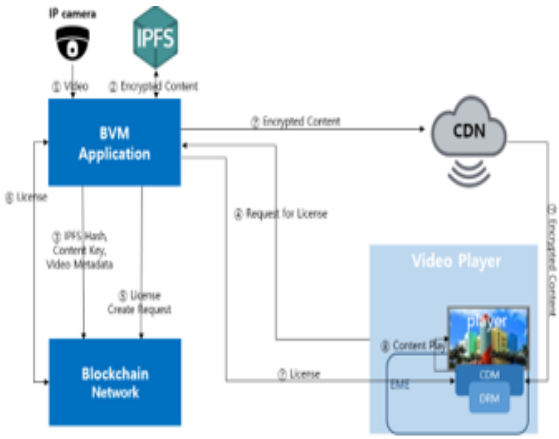
۳-۳- حفظ امنیت و حریم شخصی به کمک بلاک‌چین با مجوز

روش‌های مختلفی مانند رنگ‌بندی نادرست، مناطق صورت، رنگ‌های نامناسب و نورپردازی نادرست می‌تواند به تصویر اصلی دوربین مداربسته در زمان انتقال تصویر صدمه زده یا سبب ماسک زنی آن شود. ولی می‌توان به کمک رمزنگاری امنیت و حریم شخصی را ارتقا داد و از دسترسی‌های غیرمجاز به تصویر جلوگیری کرد، در برخی مواقع نفوذ گران با اعمال تغییرات تصویر خواهان رسیدن به اهداف سو خود هستند. عدم استفاده از رمزنگاری سبب می‌شود که نتوان به تعادل بهینه بین حریم خصوصی، وضوح، شفافیت، امنیت و استحکام سامانه دست‌یافت در شکل ارتباط بین BVM[1] و دوربین و IPFS[2]را نشان می‌دهد و در این روش IPFS وظیفه بازپخش تصاویر را دارد و بر اساس هش ذخیره‌شده در بلاک‌چین کنترل تغییر و دست‌کاری را انجام می‌دهد [۲۱]

[1] Blockchain video management
[2] InterPlanetary File System

۳-۴- جلوگیری از انتشار غیرمجاز تصاویر

جئونگ، در مقاله خود مدیریت یک سامانه نظارت تصویری مبتنی بر بلاک‌چین را برای حل مشکل انتشار غیرمجاز ویدئو در سامانه نظارت تصویری پیشنهاد داده است. در معماری پیشنهادی، فیلم دریافتی از دوربین رمزگذاری شده و در گره IPFS متصل به شبکه بلاک‌چین ذخیره می‌شود. کلید رمزگشایی ویدئو در بلوک ثبت نمی‌شود، اما در DB خصوصی گره بلاک‌چین ذخیره می‌شود که از اختیارات ویژه‌ای برخوردار است و تنها توسط کد بلاک‌چین قابل‌پردازش است. برای تبدیل و رمزگشایی ویدئو، هر شخصی که بخواهد ویدیو را مشاهده کند باید انتقال و تبدیل ویدئو را در شبکه بلاک‌چین تأیید کرده و پس‌ازآن در زنجیره کد، chain code API مجوز ایجاد کند. روش پیشنهادی، مبتنی بر روشی برای ذخیره و تبادل ایمن فیلم در یک سامانه نظارت تصویری است که در مقاله [۶] تمام مراحل و گام‌ها و دیاگرام زمانی ذکرشده است. اجزای این شبکه پیشنهادی به شرح زیر است: دوربین IP، IPFS3 (گره IPFS که فیلم‌های رمزگذاری شده در آن توزیع و ذخیره می‌شوند (برنامه BVM4 (مدیریت فیلم بلاک‌چین)، شبکه بلاک‌چین، CDN5 (شبکه تحویل محتوا)، Video Player [۶]



(شکل-۶): بلوک دیاگرام روش جلوگیری از انتشار غیرمجاز بر اساس مدیریت محتوا

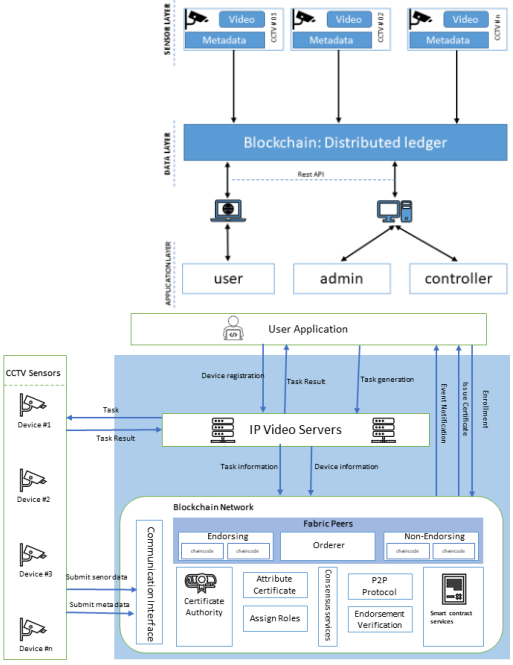
۳-۴- تضمین و قابلیت اطمینان برای تصاویر ویدیویی ذخیره‌شده و کنترل دسترسی کارکنان

سامانه‌های نظارت تصویری در شهرهای هوشمند به‌عنوان عناصری هستند که به‌صورت ۲۴*۷ کار می‌کنند و تعداد

[3] Interplanetary File System
[4] Blockchain Video Management
[5] Content Delivery Network

دوربین‌های مداربسته رو به افزایش است. از سویی دیگر با بهبود فناوری پردازش تصویر و سامانه‌های آنالاتیک دسترسی به هر نوع اطلاعاتی سریع‌تر و سهل‌تر شده است؛ اما نکته نگران‌کننده این است که صحت و تمامیت تصاویر ذخیره‌شده چگونه تضمین می‌شود. در سامانه‌های متمرکز به‌واسطه الگوریتم امکان پاک کردن بخشی از تصاویر بسته‌شده است. در این سامانه‌ها ازآنجاکه فریم‌های ویدیویی به‌صورت بازه‌های زمانی مثلاً ۱۰ دقیقه ذخیره می‌شوند، امکان پاک کردن یک فایل ناممکن شده است و یا با ایجاد footprint و یا اثرانگشت توسط دستگاه ذخیره‌ساز تمامیت داده‌ها روی تصاویر ذخیره‌شده رد پایی را بر جا می‌گذارد. نکته قابل‌توجه این است که در چند سال اخیر تحقیقات در این زمینه درباره جعل عمیق، یادگیری عمیق و هوش مصنوعی گسترش‌یافته است. از سویی دیگر با توجه به الگوریتم‌های فشرده‌سازی، فرد متجاوز برای ایجاد جعل روی تصاویر نیاز است که فایل‌های فشرده‌شده را غیر فشرده نموده و با تزریق فیلم موردنظر در بین استریم های ویدیویی، مجدداً آن فایل‌ها را فشرده نماید. [۸]

در شکل (۷) یک معماری چندلایه نشان داده‌شده است. مدل تعامل بلاک‌چین-کاربر (Blockchain-user) سه لایه مهم شامل لایه کاربرد، لایه دیتا و لایه حسگر را معرفی می‌کند. لایه کاربرد شامل برنامه‌های کاربری است که توسط کلاینت‌ها و مدیران شبکه اجرا می‌شود. تبادل داده‌ها در لایه میانی رخ می‌دهد که از بلاک‌چین تشکیل‌شده است. این لجر توزیع‌شده به‌عنوان نقطه احراز هویت و تائید داده‌ها و متادیتاهای دوربین‌های نظارتی عمل می‌کند. قوانین مختلف و قراردادهای هوشمند نیز بر روی این لایه اجرا می‌شوند. این قوانین باید هماهنگ با کاربران، مراجع نظارتی و ارائه‌دهندگان زیرساخت‌ها تدوین شود؛ بنابراین تعهدات مبتنی بر قرارداد هوشمند، مانند معاملات داده‌ها و دارایی‌های فیزیکی، به دلیل اعتماد متقابل به بلاک‌چین قابل تسویه است. لایه حسگر شامل سنسورهای تصویر یا دستگاه‌های نظارتی است که در پژوهش ما، همان دوربین‌های مداربسته هستند. بلاک‌چین به‌منزله‌ی ستون فقرات در این سامانه پیشنهادی است. این برنامه بدون نیاز به‌واسطه به دلیل قابلیت‌های قرارداد هوشمند و P2P کار می‌کند. علاوه بر این، اعتماد در میان ذینفعان همواره الزامی نیست؛ زیرا فناوری پلتفرم لجر توزیع‌شده، ویژگی‌های رمزگذاری و ردیابی کامل هر بلوک را ارائه می‌دهد. [۸]



(شکل-۷): مدل تعاملی بلاک‌چین کاربری [۸]

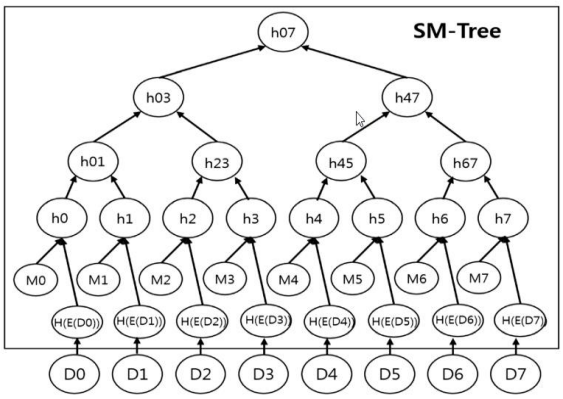
۳-۵- استفاده از درخت مرکل برای حریم شخصی در سامانه‌های نظارت تصویری

امروزه سامانه‌های نوین نظارت هوشمند خدمات مختلفی را ارائه می‌دهند که قبلاً وجود نداشته‌اند؛ نمونه‌ای از این قبیل خدمات نظارت پیشگیرانه، از طریق فناوری تجزیه‌وتحلیل ویدیویی مبتنی بر هوش مصنوعی است. بااین‌حال، چالش‌های مشترک زیادی در حوزه امنیتی و حریم خصوصی ناشی از مهاجمان مجرم و اشخاص ثالث غیرقابل‌اعتماد در سامانه ابری دوربین مداربسته وجود دارد. برای حل این مسأله، از فناوری بلاک‌چین برای اطمینان از یکپارچگی و امنیت سامانه نظارت هوشمند مبتنی بر ابر استفاده‌شده است. روش جدید با عنوان درخت مرکل (Merkle-Tree) برای انتقال کارآمد داده‌های ویدیویی پیشنهادشده است. روش پیشنهادی به دلیل کاهش پهنای باند موردنیاز در انتقال کارآمد می‌باشد؛ همچنین این مزیت را دارد که برای کاهش هزینه‌های ذخیره‌سازی، امکان تکثیر را نیز فراهم می‌کند. روش پیشنهادی ارائه‌شده همچنین می‌تواند داده‌های ویدیویی دوربین مداربسته را با خیال راحت و بدون آشکارسازی حریم خصوصی اشیا، همگام‌سازی کند. [۲۴]

طرح همگام‌سازی مبتنی بر Merkle-Tree امنیت را در نظر نمی‌گیرد (شکل ۷) و در مبحث رهگیری پیام‌ها، ایمنی لازم را ندارد. بااین‌حال، درروش SM-Tree[1]

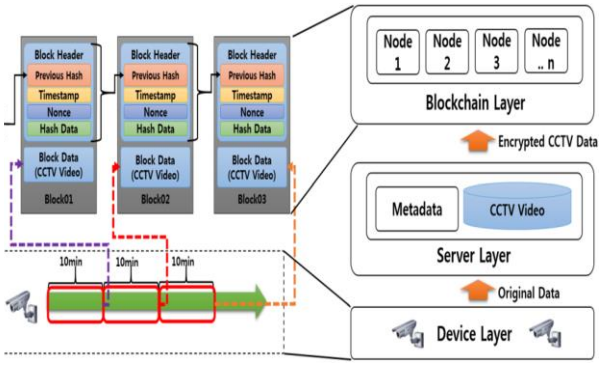
[1] Secure Merkle tree

پیشنهادی، تمام داده‌های منتقل‌شده رمزگذاری و مدیریت می‌شوند و ازآنجاکه کلیدهای مختلف در واحدهای بلوک داده اعمال می‌شوند، مهاجم نمی‌تواند حمله را انجام دهد.



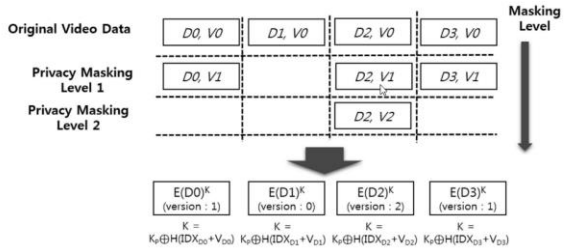
(شکل-۸): بهبود درخت مرکل برای تصاویر و متادیتا و اعمال رمزنگاری [۲۴]

این ویژگی همچنین این مزیت را دارد که در آن حمله به الگوی بلوک داده‌ها دشوار است. روش پیشنهادی بسیار کارآمد است زیرا پهنای باند موردنیاز برای انتقال را کاهش می‌دهد. همچنین این مزیت را دارد که برای کاهش هزینه‌های ذخیره‌سازی امکان تکثیر را نیز فراهم می‌کند. فناوری بلاک‌چین ابزار بسیار مناسبی در محیط‌های دارای دوربین مداربسته چندرسانه‌ای مبتنی بر هوش مصنوعی است. مطابق شکل می‌تواند در بازه‌های زمانی به‌صورت بلوک درآمده و در سه لایه دستگاه، سرور و لایه بلاک‌چین قرار گیرد و ارتباط و تناظر امنی را بین لایه دستگاه و لایه سرور و لایه بلاک‌چین ایجاد نماید [۲۴]



(شکل-۹): مدل ارتباطی برای استفاده از مرکل [۲۴]

کاربرد دیگر درخت مرکل ایجاد ماسک بندی تصویر به‌صورت لایه است و بر اساس کلید رمزنگاری متقاضیان تصویر می‌توان روی بخش خاص تصویر ماسک زنی را انجام داد.

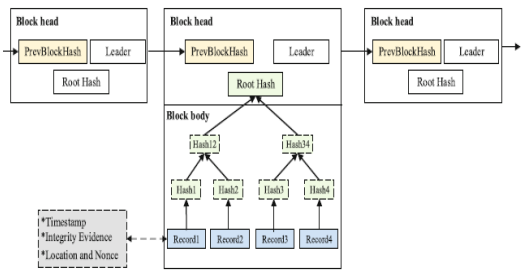


(شکل-۱۰): ماسک زنی چندلایه تصویر [۲۴]

۳-۶- استفاده از زنجیره ویدیویی یا VIDEO CHAIN

زنجیره ویدیویی یکی از روش‌های دیگر برای تمامیت و احراز اصالت تصاویر ضبط‌شده است درروش زنجیره ویدیویی بر اساس گفتار نویسندگان به‌عنوان اولین مقاله‌ای است که بلاک‌چین را به سامانه نظارت تصویری عرضه کرده است. دو قسمت اصلی سامانه بلاک‌چین را نیز طراحی کرده‌اند که عبارت‌اند از: به‌روزرسانی بلاک‌چین و تائید اسناد در بلاک‌چین. (شکل ۱۱) در این روش پروتکل ترکیبی با سرعت‌بالا ارائه‌شده است و امنیت و کارایی آن موردبررسی قرارگرفته است. اهداف طراحی عبارت‌اند از: تعدیل مشارکت، ذخیره‌سازی قابل‌اعتماد، به‌روزرسانی و تائید کارآمد، مقاومت در برابر نفوذ. زنجیره ویدیویی بر اساس معماری بلاک‌چین در چهار لایه طراحی‌شده است که شامل لایه دیتا، لایه شبکه، لایه تعمیم و لایه کاربرد است. زنجیره ویدیویی مزایای بسیاری داشته است: [۲۰]

- زنجیره ویدیویی، یکپارچگی اسناد در بلاک‌چین صحیح و قابل‌اعتماد است.
- زنجیره ویدیویی می‌تواند از مکانیسم‌های دفاعی تحت مدل‌سازی انجام‌شده برای روبرو شدن با تهدیدها بهره بگیرد.
- زنجیره ویدیویی دارای ویژگی‌های امنیتی قابل‌ردیابی و مقاوم در برابر دست‌کاری و خرابکاری است.



(شکل-۱۱): ساختار مبانی هش در زنجیره ویدیویی

زنجیره ویدیویی دو فاز در لایه کاربرد دارد: [۲۰]

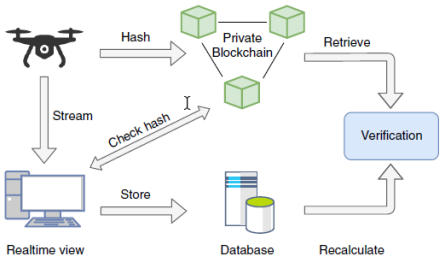
به‌روزرسانی بلاک‌چین: در این بخش، مراحل دقیق به‌روزرسانی بلاک‌چین از منظر عملکرد سامانه، شرح داده‌شده است. ابتدا دوربین داده‌های ویدئویی خام را ضبط کرده و برای پردازش به سرور می‌فرستد. از یک‌سو، سرور داده‌های ویدئویی خام را فشرده می‌کند و آن‌ها را به یک سرور ذخیره‌سازی محلی می‌فرستد؛ و از سوی دیگر، سرور یکپارچگی اسناد را محاسبه و برای عامل بلاک‌چین ارسال می‌نماید. عامل بلاک‌چین اسناد تائید شده را بین گره‌های دیگری که می‌خواهند آن را برای بلاک‌چین بنویسند، منتشر می‌کند. در پایان، اسناد تائید شده در بلاک‌چین نوشته‌شده و بلاک‌چین به‌روزرسانی می‌گردد.

تائید اسناد در بلاک‌چین: هنگامی‌که یک فیلم نظارت به‌طور رسمی منتشر می‌شود، باید صحت یا اعتبار فیلم تائید شود. این روند به مشارکت افراد ذیصلاح نیاز دارد و برای محافظت از حریم خصوصی افراد، افراد مجاز می‌توانند داده‌های اصلی فیلم را مشاهده کرده و بر مبنای عملکرد بلاک‌چین، صحت ویدیو را تشخیص دهند.

۴- ارائه راه‌کار برای اصالت تصاویر دوربین‌های مداربسته بی‌سیم به کمک بلاک‌چین

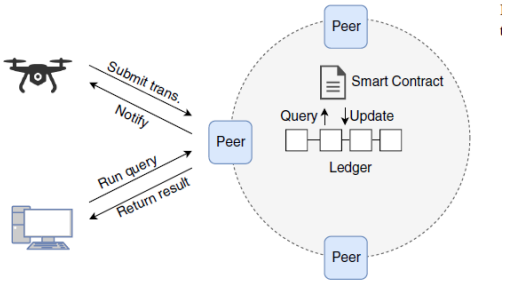
در برخی از سامانه‌های مداربسته نیاز به کاربری در شبکه‌های بی‌سیم است و یکی از این کاربری‌ها مربوط به سامانه‌های پهباد و ارسال داده‌ها توسط آن در شبکه‌های بی‌سیم است. برای مثال، موارد استفاده از هواپیماهای بدون سرنشین را در نظر می‌گیریم که در آن‌ها امکان پخش در بسیاری از برنامه‌های نظارتی وجود دارد و می‌توانند صحنه جرم یا حادثه را ضبط کنند تا به‌عنوان شواهد قانونی در آینده استفاده شود. این چارچوب شامل احراز هویت منبع، حفظ یکپارچگی داده‌های ویدیویی با دریافت هش و ذخیره‌سازی در بلاک‌چین و امکان دریافت ویدئوی اصلی است که از طریق هواپیمای بدون سرنشین به‌صورت پخش هم‌زمان ارائه می‌شود. [۳]

در شکل (۱۲) تصاویر زنده و فریم مربوطه هش می‌شود و اصل تصویر و هش تصویر به گیرنده ارسال می‌شود و گیرنده با محاسبه مجدد هش می‌تواند از دست نخوردن داده مطلع شود و ارسال هش در شبکه بلاک‌چین صورت می‌گیرد تا تضمین‌کننده امنیت باشد.



(شکل-۱۲): بررسی تمامیت داده تصاویر ارسال‌شده به کمک بلاک‌چین [۳]

به‌طور دقیق‌تر، ابتدا چارچوب پیشنهادی محاسبه هش را بر روی‌داده‌های ویدیویی دستگاهی که در آن ضبط‌شده است بدون ارسال به دستگاه لبه یا سرورها انجام می‌دهد. با این کار خطر دست‌کاری هش در حین یا بعد از انتقال کاهش می‌یابد. علاوه بر این، جریان ویدئو را به‌صورت دوره‌ای تقسیم‌بندی کرده تا خطر از دست رفتن کل فیلم را به دلیل هرگونه مشکل احتمالی در هواپیمای بدون سرنشین یا ایجاد اشکال در قسمت دیگری از ویدیو کاهش داده شود. هنگامی‌که پردازش بخش موردنظر انجام شد، هواپیمای بدون سرنشین با زنجیره بلوک ارتباط برقرار می‌کند و متادیتای ویدئو (هش، شناسه و غیره) را که بلافاصله جمع‌آوری کرده و به بلاک‌چین ارسال می‌کند. برای برقراری این ارتباط از TCP برای ایجاد قابلیت اطمینان استفاده‌شده است. از این لحاظ، داده‌های واقعی فیلم نیز باید از TCP استفاده کنند تا اطمینان حاصل شود که هر آنچه در پهباد پردازش می‌شود در سرور از راه دور بدون هیچ‌گونه خطایی دریافت می‌شود. بسیار مهم است تا تضمین شود که هش ارسال‌شده به بلاک‌چین با هش فیلم دریافتی در سرور مطابقت دارد. [۳]



(شکل-۱۳): استفاده پهباد از بلاک‌چین و بهره‌گیری از قرارداد هوشمند [۳]

مدل‌سازی و الزامات سامانه برای این روش عبارت است از:

پردازش با وضوح‌بالا: پردازش ویدئو یک فرایند محاسباتی پرهزینه است که به‌طور ویژه برای دستگاه‌های

اینترنت اشیا و محدود به منابع می‌باشد. بااین‌حال، ضبط یک فیلم باکیفیت بالا برای تفسیر واضح صحنه‌ها از اهمیت ویژه‌ای برخوردار است؛ بنابراین، سامانه باید پردازش فیلم‌های با وضوح‌بالا را در دستگاه‌های اینترنت اشیا فعال نماید.

پخش فیلم به‌صورت هم‌زمان: از ویدئو ارسالی می‌توان برای کنترل هم‌زمان دستگاه توسط اپراتور استفاده کرد. این امر انتقال ویدئو با تأخیر کم را ضروری می‌کند.

جریان انطباقی: ازآنجاکه پهباد در حال پیمایش است، ممکن است پهنای باند اتصال بین دستگاه IoT و اتاق کنترل در حین کار تغییر کند. کیفیت فیلم باید بر اساس پهنای باند موجود تنظیم شود.

تقسیم‌بندی کارآمد: برای ذخیره قسمت‌های ضبط‌شده‌ی ویدئو، باید هش به‌صورت دوره‌ای محاسبه شود، بنابراین به تقسیم‌بندی فیلم به چند قطعه کوچک با استفاده کارآمد از منابع محاسباتی محدود احتیاج دارد.

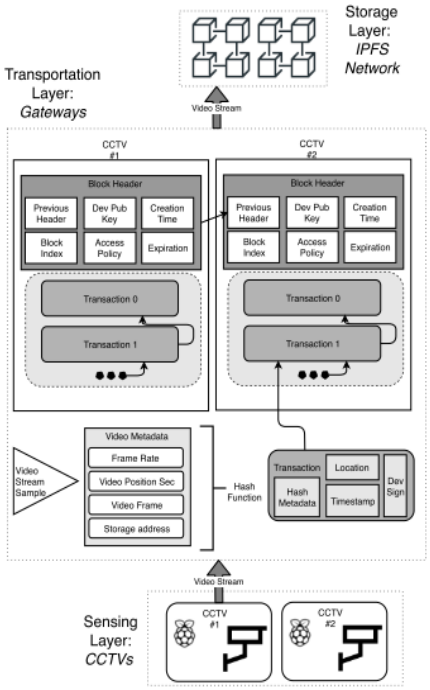
برای ارزیابی عملکرد روش پیشنهادی بلاک‌چین و سامانه‌های مداربسته در شبکه‌های بی‌سیم از معیارهای استفاده از پردازنده، تأخیر در انتقال، جیتر، تأخیر در تراکنش‌های بلاک‌چین استفاده‌شده است.

۵- روش پیشنهادی بلاک‌چین و speedy chain [۲۲]

روش دیگر speedychain یا زنجیره سریع است که درزمینهٔ نظارت تصویری، به یک چارچوب سبک برای بلاک‌چین نیاز دارد که برای محیط محدود اینترنت اشیا محدود باشد و حداقل تأخیر را در مدیریت معاملات (قرارداد هوشمند) وارد کند. از راه‌حل‌های موجود مبتنی بر اینترنت اشیا، از چارچوبی به نام SpeedyChain استفاده‌شده است که بر اساس قابلیت منحصربه‌فرد آن امکان افزودن تراکنش‌های متعدد در بلوک‌های موجود را دارد، نه در مقابل بلاک‌چین های سنتی که فقط در زمان ایجاد بلوک می‌توانند تراکنش‌ها را اضافه کنند. در SpeedyChain هر دستگاه بلوک مخصوص به خود را دارد و کلیه تراکنش‌های مربوط به آن دستگاه در آن بلوک ذخیره می‌شود، بنابراین زمان پردازش تراکنش به میزان قابل‌توجهی کاهش می‌یابد اما شرکت‌های سازنده دوربین معمولاً برای استفاده از این روش پافشاری می‌کنند چراکه قدرت پردازشگر خود را به‌جای کیفیت تصویر باید به این امر اختصاص دهند. این اجرای بلاک‌چین مجاز سبک در سطح درگاه اجرا می‌شود و تراکنش‌های دریافتی از منابع مختلف را مدیریت می‌کند. [۲۲]

در این چارچوب پیشنهادی از معماری سه لایه‌ای تشکیل‌شده است. فرض بر این است که دوربین‌های نظارتی قابل‌اعتماد هستند و در لایه سنجش مستقر می‌شوند. درگاه‌ها همچنین مورد اعتماد و قابل‌استفاده در لایه انتقال هستند و وظیفه جریان ویدئو، حفظ بلاک‌چین و ارائه اثبات یکپارچگی فیلم رادارند. سرانجام، یک‌لایه ذخیره‌سازی شخص ثالث غیرقابل‌اعتماد وجود دارد که می‌تواند از هر سامانه ذخیره‌سازی مناسب استفاده کند. برای این کار، از شبکه (IPFS) برای ذخیره فیلم‌های نظارتی استفاده‌شده است.

در این چارچوب پیشنهادی از معماری سه لایه‌ای تشکیل‌شده است. فرض بر این است که دوربین‌های نظارتی قابل‌اعتماد هستند و در لایه سنجش مستقر می‌شوند. درگاه‌ها همچنین مورد اعتماد و قابل‌استفاده در لایه انتقال هستند و وظیفه جریان ویدئو، حفظ بلاک‌چین و ارائه اثبات یکپارچگی فیلم رادارند. سرانجام، یک‌لایه ذخیره‌سازی شخص ثالث غیرقابل‌اعتماد وجود دارد که می‌تواند از هر سامانه ذخیره‌سازی مناسب استفاده کند. برای این کار، از شبکه (IPFS) برای ذخیره فیلم‌های نظارتی استفاده شده است.



(شکل-۱۴): معماری لایه‌ای speedy chain

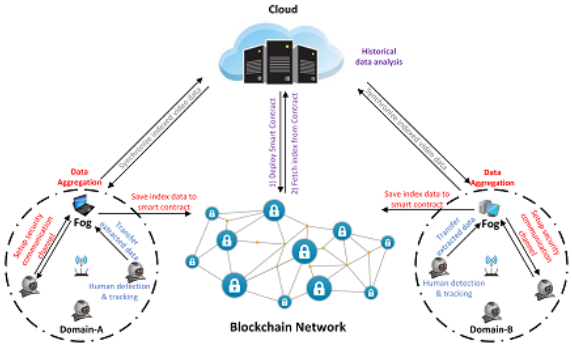
فرآیند راه‌اندازی خودکار دستگاه: فرآیند راه‌اندازی خودکار هنگامی اتفاق می‌افتد که یک درگاه شناسایی کند

که هیچ بلوکی در بلاک‌چین حاوی کلید عمومی دوربین وجود ندارد. هر دوربینی توسط کلید عمومی موجود در سرایند بلوک به‌طور منحصربه‌فرد شناخته می‌شود. این بلوک ایجادشده و از اجرای پروتکل اجماع PBFT پیروی می‌کند تا آن را در بلاک‌چین قرار دهد. تنها پس از دستیابی به اجماع، بلوک در بلاک‌چین واردشده و به دوربین مجاز اجازه می‌دهد جریان ویدئو را شروع کند.

پروتکل یکپارچگی ویدئو: در لایه سنجش، هر دوربین نظارتی جریان ویدئویی را تولید می‌کند که به درگاه منتقل می‌شود. درگاه‌ها وظیفه پردازش جریان ویدئو و ارسال آن به سامانه ذخیره‌سازی رادارند. ما در چند مرحله عملکرد درگاه‌ها را توضیح می‌دهیم:

۶- احراز هویت به‌صورت هم‌زمان

در مقاله دیگر، احراز هویت افراد در مقابل دوربین به کمک قراردادهای هوشمند صورت پذیرفت. امروزه، میزان بسیار زیادی از داده‌های نظارتی به‌طور مداوم توسط حسگرهای ویدئویی توزیع نشده تولید می‌شوند .بسیار چالش‌برانگیز است که بلافاصله شیء موردنظر را شناسایی کرده یا در اقدامات مشکوک از هزاران فریم ویدیویی تفکیک گردد. در این مقاله با الهام از قراردادهای هوشمند و فناوری بلاک‌چین، یک تائید اعتبار هم‌زمان برای سامانه‌های نظارت ویدئویی بر رویدادها پیشنهادشده است تا مکانیسم امنیتی جریان‌های ویدیویی غیرمتمرکز را در محیط شبکه‌های غیرقابل‌اعتماد، ارائه دهد. روش پیشنهادی یک سناریو شامل حوزه نظارت تصویری مبتنی بر اینترنت اشیا، بدون رابطه اعتماد از پیش تعیین‌شده است. با انجام وظایف ردیابی و تشخیص اشیا توسط دوربین‌های هوشمند، اطلاعات پردازش سطح پایین با پردازش جریان نظارت تصویری در لبه شبکه در محل استخراج می‌شود و پس‌ازآن برای جمع‌آوری داده‌ها و تجزیه‌وتحلیل بیشتر به دستگاه‌های مبهم یا fog منتقل می‌گردد. در هر دامنه، دستگاه fog نه‌تنها سیاست‌های امنیتی از پیش تعیین‌شده را برای مدیریت دستگاه‌ها و سرویس‌های مرتبط با دامنه اعمال می‌کند، بلکه همچنین به‌عنوان یک واسطه برای تعامل با بلاک‌چین عمومی و ابر عمل می‌کند تا احراز هویت شاخص را برای درخواست نظارت ویدئویی مبتنی بر رویداد را فعال نماید. اجزای اصلی این چارچوب شامل پرسش ویدئوی نظارت بر رویداد، نمایه‌سازی به‌صورت هم‌زمان و انتقال امن داده‌ها و تأیید اعتبار فعال‌شده توسط بلاک‌چین است. [۲۷]



(شکل-۱۵): تصویری از معماری سامانه. [۲۷]

در این سامانه، پردازش ویدئویی به‌صورت فوری، درک بهتری از رویداد به‌صورت هم‌زمان ارائه می‌دهد. فرایند آن به‌گونه‌ای است که در آن دوربین مداربسته فیلم را ضبط کرده و به دستگاه‌های لبه / مه دلخواه به‌صورت هم‌زمان منتقل می‌نماید. دستگاه لبه از طریق شبکه محلی (LAN) به دوربین متصل می‌شود و هر فریم را به‌عنوان اولین نقطه از مکانیسم تشخیص غیرطبیعی خودکار در نظر می‌گیرد. پس از دریافت فریم، دستگاه لبه، وظیفه استخراج ویژگی‌های سطح پایین را برای تشخیص رفتار غیرطبیعی بر عهده دارد. برای داشتن یک سامانه عملکردی به‌منظور تشخیص یا پیش‌بینی رفتارهای ناهنجار، سامانه نظارت باید اشیا را به‌طور دقیق شناسایی کند. در غیر این صورت سامانه ممکن است در تشخیص مواقع ضروری ناکام بوده و یا میزان هشدار کاذب بالایی را متحمل شود. همچنین، در استفاده از نظارت هوشمند، دستگاهی که وظیفه تشخیص حرکات انسانی را دارد، با محدودیت‌هایی در قدرت محاسباتی و منابع ذخیره‌سازی موجود برای این کار مواجه خواهد بود. ویژگی‌های اشیای شناسایی‌شده است. این ویژگی‌ها ممکن است شامل سرعت، جهت و برخی دیگر از معیارهای توصیفی مانند برخی از حرکات خاص یک شیء باشد. حرکات با تشخیص سر، شانه، بالای بازو و بازوی تحتانی جسم و زاویه‌هایی تعریف می‌شوند که ممکن است در طی حرکت ایجاد شوند. شبکه عصبی یا CNN می‌تواند قسمت‌های مختلف جسم را طبقه‌بندی کند و مکان فعلی اجسام یا افرادی که شناسایی می‌شوند در کنار سایر ویژگی‌های آن‌ها به‌عنوان اشیای جداگانه در نظر گرفته می‌شود. انتقال داده‌ها از گره لبه به گره مه در یک کانال ارتباطی امن رمزگذاری شده با الگوریتم‌های AES و RSA صورت می‌گیرد. مزیت استفاده از

هر دو الگوریتم رمزگذاری شده این است که یک‌زمان کوتاه برای ایجاد کلید در نظر گرفته و در برابر حملات شبکه‌ای مقاومت بیشتری دارد؛ اما بلاک‌چین در این بخش نیز کارا شده است، در این قسمت، ویژگی‌های استخراج‌شده توسط دستگاه‌های لبه‌ای و داده‌های متنی در لایه fog که اطلاعات را برای کارهای سطح بالا با ابر به اشتراک می‌گذارد، باهم ادغام می‌شوند. استراتژی احراز هویت نمایه‌سازی فعال بلاک‌چین برای فعال‌سازی یک سرویس اشتراک داده غیرمتمرکز، مقیاس‌پذیر و ایمن ارائه‌شده است که اجزای اصلی ثبت کردن، استقرار قرارداد هوشمند، ایجاد رکورد نمایه‌ی تجزیه‌شده، احراز هویت نمایه‌ای است. [۲۷]

۷- اقدامات آینده

پژوهش‌های آینده باید بیشتر بر روی اقدامات امنیتی در محیط‌های نظارت تصویری هوشمند چندرسانه‌ای متمرکز بوده و آن‌ها را به‌عنوان فن‌آوری‌های محافظت از حریم خصوصی برای امنیت اجتماعی معرفی نمایند. در تحقیقات آینده، اصلاحات بیشتری را در مورد الگوریتم پوشاندن حریم خصوصی و شناسایی هویت در نظر باید گرفته شود و ارزیابی روش پیشنهادی و مقایسه آن‌ها صورت پذیرد. همان‌طور که ذکر شد مدیریت کارکنان و ایجاد الگوی سریع‌تر و امن‌تر نیز یکی از مواردی است که در مقالات کمتر به آن اشاره‌شده است.

تحقیقات آینده باید بیشتر بر روی تلاش‌ها برای شناسایی مناسب‌ترین کاربردهای اینترنت اشیا در سطح عملی برای پیاده‌سازی مکانیسم‌های امنیتی مبتنی بر بلاک‌چین و چگونگی اجرای لجرهای توزیع‌شده (پایگاه‌های داده) پشتیبانی‌کننده از گره‌ها و المان‌های مداربسته متمرکز باشد. همچنین، تعیین اینکه کدام‌یک از پیاده‌سازی‌های فوق برای ایجاد بلاک‌چین در نقاط مختلف شبکه مناسب است، می‌تواند یکی دیگر از حوزه‌های تحقیقاتی در نظر گرفته شود.

۸- نتیجه‌گیری

مفهوم بلاک‌چین در ابتدا با ارز دیجیتال همراه بود، اما بسیاری دیگر از کاربردهای بالقوه این فناوری در حال ظهور است که ازجمله‌ی آن‌ها می‌توان به برنامه‌های ادغام و یکپارچه‌سازی برای داده‌های اینترنت اشیا اشاره کرد. بلاک‌چین ها ابزارهای قدرتمندی هستند که فراتر از کاربردهای اساسی امنیتی می‌باشند، زیرا به‌طورکلی، مکانیسمی برای اعتماد مشترک جهانی به شمار می‌روند. بااین‌حال، به دلیل محدودیت‌های معمول موجود در گره‌های اینترنت اشیا، همواره ممکن استفاده از یک شبکه کاملاً امن بلاک‌چین در تمام کاربردهای اینترنت اشیا عملی نباشد. یکی از کاربردهای مهم در اینترنت اشیا سامانه‌های نظارت تصویری است و مفاهیمی همچون تمامیت داده ذخیره‌شده، تمامیت داده ارسال‌شده، کشف تغییرات در پیکربندی و یا صحنه مقابل دوربین و مدیریت کارکنان می‌تواند در سامانه بلاک‌چین بسیار کاراتر باشد. در سامانه‌های گذشته که به‌صورت متمرکز یا نیمه‌متمرکز امن سازی در یک مرکز صورت می‌گرفت اما به‌واسطه بلاک‌چین و ساختار هش امکان دست‌کاری در تصاویر ذخیره‌شده، پیکربندی، مجوزهای دسترسی و بسیاری موارد دیگر به حداقل می‌رسد.

تشکر و قدردانی

در پایان لازم است از زحمات و حمایت‌های جناب آقای دکتر محمود صموتی و خانم مهناز خوشگوار کمال تشکر و قدردانی را داشته که با حمایت‌های ایشان این تحقیق به سرانجام رسید.

۹- مراجع

[۱] س. صموتی, م. فتحی, ت. تفنگچی, "مطالعه میدانی سامانه‌های نظارت تصویری در صنعت ریلی و ارایه راهکار های هوشمندسازی برای افزایش امنیت از دیدگاه پدافند غیر عامل," دومین کنفرانس ملی پدافند غیرعامل و پیشرفت پایدار, ۱۳۹۶.

[۲] س. صموتی, م. فتحی, ع. خلیلی, "مروری بر اقدامات پیشگیرانه و نگهداری در عملکرد سامانه‌های نظارت تصویری," کنفرانس بین المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلانشهرها، راه‌کارها و چالش‌ها با محوریت پدافند غیر عامل و مدیریت بحران, ۱۳۹۷.

[3] S. Mercan, M. Cebe, R. S. Aygun, K. Akkaya, E. Toussaint, and D. Danko, "Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices," Security and Privacy, vol. 4, no. 2, p. e143, 2021.

[4] U. Javaid, A. Siang, M. Aman, and B. Sikdar, "Mitigating loT Device based DDoS Attacks using

Blockchain," pp. 71-76, 2018, doi: 10.1145/3211933.3211946.

[5] M. Kerr, H. Fengling, and R. van Schyndel, "A Blockchain Implementation for the Cataloguing of CCTV Video Evidence," pp. 1-6, 2018, doi: 10.1109/AVSS.2018.8639440.

[6] Y. Jeong, D. Hwang, and K.H. Kim, "Blockchain-based management of video surveillance systems," in 2019 International Conference on Information Networking (ICOIN), 2019: IEEE, pp. 465-468.

[7] M. Kerr, F. Han, and R. van Schyndel, "A blockchain implementation for the cataloguing of CCTV video evidence," in 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2018: IEEE, pp. 1-6.

[8] P. W. Khan, Y.C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities," Electronics, vol. 9 ,no. 3, p. 484, 2020.

[9] V. Damjanovski, CCTV: from light to pixels, Third edition. ed. Amsterdam ; Boston, MA: Butterworth-Heinemann, an imprint of Elsevier, 2014, p. 614 pages.

[10] F. Nilsson and Axis Communications. Intelligent network video: understanding modern video surveillance systems. Boca Raton: CRC Press, 2018, pp. xxxi, 389 p.

[11] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The Security of IP-Based Video Surveillance Systems," Sensors, vol. 20, no. 17, p. 4806, 2020. [Online]. Available: https://www.mdpi.com/1424-8220/20/17/4806.

[۱۲] س. صموتی, ح. حسن پور, ع. خلیلی, "مروری بر مخاطرات سایبری در سامانه‌های نظارت تصویری تحت شبکه و ارائه راهکار جهت توسعه امن سازی آن," چهارمین کنفرانس ملی کامپیوتر، فناوری اطلاعات و کاربردهای هوش مصنوعی, ۱۳۹۹.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[۱۴] ج. عباسی, بلاک‌چین آشنایی با مفاهیم بنیادی. موسسه کتاب مهربان نشر, ۱۳۹۷.

[15] K. Deepak, A. N. Badiger, J. Akshay, K. A. Awomi, G. Deepak, and H. Kumar, "Blockchain-based Management of Video Surveillance Systems: A Survey," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), 2020: IEEE, pp. 1256-1258.

[16] P. Gallo, S. Pongnumkul, and U. Q. Nguyen, "BlockSee: Blockchain for IoT video surveillance in smart cities," in 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), 2018: IEEE, pp. 1-6.

[17] J. Wu and N. K. Tran, "Application of blockchain technology in sustainable energy systems: An overview," Sustainability, vol. 10, no. 9, p. 3067, 2018.

[۱۸] م. د. پیمان اخوان بلاک‌چین از بیت کوین تا دنیای صنعت. آتی نگر, ۱۳۹۸.

[19] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," Internet of Things, vol. 1, pp. 1-13, 2018.

[20] M. Liu, J. Shang, P. Liu, Y. Shi, and M. Wang, "VideoChain: trusted video surveillance based on blockchain for campus," in International conference on cloud computing and security, 2018: Springer, pp. 48-58.

[21] A. Fitwi and Y. Chen, "Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain," pp. 1-8, 2021, doi: 10.1109/ICCCN52240.۲۰۲۱.۹۵۲۲۱۹۹.

[22] R. A. Michelin, N. Ahmed, S. Kanhere, A. Seneviratne, and S. Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp.۲۰۲۰ ,۱-۳ .

[۲۳] س. صموتی و م. فتحی, "ارزیابی تهدیدها، آسیب‌پذیری و ریسک در زیر ساخت سامانه‌های نظارت تصویری تحت شبکه سامانه‌های حمل و نقل هوشمند," دومین همایش سامانه‌های حمل و نقل هوشمند جاده ای, ۱۳۹۵.

[24] D. Lee and N. Park, "Blockchain based priv acy preserving multimedia intelligent video surveillance using secure Merkle tree," Multimedia Tools and Applications, 2020, doi: 10.1007/s11042-020-08776-y.

[25] D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, 2017.

[۲۶] م. ح. م. خوانساری, بلاک‌چین در توری و عمل ناقوس, ۱۳۹۸.

[27] S. Y. Nikouei, R. Xu, D. Nagothu, Y. Chen, A. Aved, and E. Blasch, "Real-time index authentication for event-oriented surveillance video query using blockchain," in 2018 IEEE International Smart Cities Conference (ISC2), 2018: IEEE, pp. 1-8.

سید علی صموتی دانشجوی دکترای مهندسی فناوری اطلاعات در دانشگاه آزاد اسلامی سبزوار است. ایشان تحصیلات کارشناسی ارشد خود را در سال ۱۳۹۰در رشته مخابرات امن در دانشگاه علم و صنعت و دوره کارشناسی خود را در رشته مهندسی برق مخابرات دانشگاه آزاد اسلامی شهرری در سال ۱۳۸۶ گذرانده است. وی بیش از ۱۵ سال است که بر روی پروژه های نظارت تصویری و حفاظت الکترونیک در پروژه های ملی به عنوان مشاور یا مدیر پروژه مشغول به فعالیت است و در دانشگاه فنی و حرفه ای بیش از ۱۰ سال در زمینه امنیت اطلاعات و امنیت سایبر تدریس دارد. محورهای پژوهشی ایشان حفاظت الکترونیک، بلاک‌چین ، هوش تجاری و ترکیب آنها است .

یاسر علمی کارشناسی مهندسی کامپیوتر را از دانشگاه آزاد اسلامی واحد مشهد در سال ۱۳۸۰ و کارشناسی ارشد معماری کامپیوتر را از دانشگاه علم و صنعت ایران، تهران، در سال ۱۳۸۲ دریافت کرد. وی مدرک دکتری خود را در رشته معماری کامپیوتر از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران در سال ۱۳۹۷ دریافت کرد و در حال حاضر عضو هیئت علمی گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد سبزوار می باشد. علایق تحقیقاتی او شامل پردازش تصویر، شبکه های کامپیوتری و سامانه‌های توزیع شده است.