علوم زیست محیطی و دانش جغرافیا

سیستم احراز هویت هویت امنیت اطلاعات ابری مبتنی بر سیستم رمزنگاری کامپیوتری و امنیت شبکه

الهام وحیدیان[۱]*زهرا رنجبر[۲]،اسما بهشتی پور[۳]،فروغ احمدی شاد[۴]

چکیده

تکنولوژی احراز هویت هویت در زندگی روزمره اهمیت بسیار زیادی دارد. در هر پلتفرم، ما نیاز داریم که وارد حساب کاربری شویم تا وضعیت و تراکنش‌های حساب را تأیید کنیم. البته، احراز هویت هویت نیز بخش ضروری و مهمی از کسب‌وکارهای پلتفرم‌ها است. داده‌های بیشتری از برنامه‌ها به ابر منتقل می‌شوند برای عملیات و ذخیره‌سازی، در حالی که مکانیزم امنیتی اطلاعات ابری نیز به طور مداوم اجرا می‌شود. از سوی دیگر، این مقاله از فناوری بلاک‌چین برای احراز هویت ایمن هویت استفاده می‌کند. در زمینه سیستم احراز هویت ایمن صدا، وضعیت امنیتی موجود در سیستم‌های ویندوز مکانیزم احراز هویت چندعاملی ایمن را اضافه می‌کند. در زمینه مکانیزم عملکرد در فضای ابری، هماهنگی مداوم برای تضمین امنیت سیستم به کار گرفته می‌شود. این مقاله به تفصیل ترکیب سیستم احراز هویت هویت، طراحی، فرآیند پیاده‌سازی و نتایج آزمایشی کاربردی مرتبط با امنیت اطلاعات را معرفی می‌کند. در زمینه اطلاعات احراز هویت هویت، سیستم‌های اطلاعات ابری می‌توانند به طور مداوم عملکرد امنیتی هویت‌ها را بهبود دهند.

کلمات کلیدی: سیستم رمزنگاری، اطلاعات ابری، احراز هویت هویت،بلاک‌چین

[۱] مهندسی برق، واحد کازرون، دانشگاه آزاد اسلامی، کازرون، ایران

elhamvahidian92@gmail.com

[۲] دانشجو، مهندسی نرم افزار، دانشگاه ملی مهارت دختران یاسوج

tavnilan@gmail.com

[۳]دبیر انجمن علمی، مهندسی نرم افزار، دانشگاه ملی مهارت دختران یاسوج

asmabeheshti5217@gmail.com

[۴] دانشجو، مهندسی نرم افزار، دانشگاه ملی مهارت دختران یاسوج

۱.مقدمه

امروزه دلیل رشد انفجاری داده‌ها توسعه مداوم اطلاع‌رسانی اجتماعی و شبکه‌ای است. همچنین داده‌هایی در صنایع مختلف به ویژه در برخی صنایع خرد تولید می‌شود و اطلاعاتی که نیاز به ذخیره دارند نیز افزایش یافته است. هر کاربر ممکن است هنگام تشخیص داده‌های خود تحت نظارت باشد؛ تنها با جستجو در کلیدواژه‌ها می‌توان اطلاعات دقیق کاربران را به دست آورد که تهدیدی برای امنیت اطلاعات کاربران است. با افزایش داده‌ها، هزینه رمزگشایی و دانلود اسناد نیز افزایش می‌یابد، بنابراین نیاز به سیستم رمزنگاری اطلاعات پیشرفته احساس می‌شود. از سوی دیگر، با پیشرفت فناوری، روش‌های حمله هکرها متنوع‌تر شده است. فناوری محافظت سنتی شبکه که توسط سرورهای کلیدی استفاده می‌شود، به عنوان روش محافظت غیرفعال شناخته می‌شود و نمی‌تواند حملات ناشناخته را مدیریت کند. در حوزه کنترل دسترسی برای مجوزها، لازم است امنیت نفوذ شده توسط کاربران دارای امتیاز کاهش یابد. در تأیید اطلاعات هویتی، مسئله نسبتاً جدی است؛ خطا و حذف می‌تواند پیامدهای نامطلوب و زیان‌هایی برای تأیید اطلاعات داشته باشد. امنیت مستمر، مفهوم اصلی در طراحی این سیستم است که با احراز هویت یک‌باره در سایر سیستم‌های احراز هویت متفاوت است.

طراحی این سیستم امکان فراموش کردن موقت قفل کامپیوتر توسط کاربران را در محیط واقعی در نظر می‌گیرد. برای جلوگیری از نفوذ عملیات غیرقانونی در این دوره، احراز هویت هویتی امنیتی و تأیید اطلاعات به صورت پیوسته و در زمان واقعی طراحی شده است که به طور قابل توجهی از نفوذ و اشتباهات ناشی از بی‌احتیاطی افراد جلوگیری می‌کند.

در این مقاله، برای احراز هویت امنیتی اطلاعات صوتی در سیستم‌های رمزنگاری، استاندارد شناسه زیرساخت بلاک‌چین ارائه شده است که از نظر مکانیزم احراز هویت هویتی در ترمینال‌های ابری برای ارائه اطلاعات ابری و مدیریت داده‌های استاندارد به کاربران ناکافی است. این سیستم نسبت به روش‌های ورود دیگر مزایای زیادی دارد و کاربران می‌توانند بدون وابستگی به طرف ثالث، اطلاعات هویتی شخصی خود را به طور مستقل مدیریت کنند. مسئله اصلی قابل حل، حاکمیت داده‌ها و افشای حریم خصوصی در سیستم احراز هویت در فرایند تعامل است.

۲. کارهای مرتبط

مطالعات نشان داده‌اند که در هنگام احراز هویت هویتی، لازم است هویت واقعی فرد اثبات شود، یعنی به احرازکننده ثابت شود که من کیستم، و سپس بر اساس مجوزهای احرازکننده، دسترسی‌های لازم داده شود. با توسعه مداوم اینترنت، احراز هویت هویتی اطلاعات صوتی به مهم‌ترین درگاه امنیتی تبدیل شده است که قبل از ارائه خدمات دیگر نیاز به احراز هویت دارد. روش احراز هویت امنیتی استفاده شده در برخی مطالعات،

روش صرفاً مبتنی بر رمز عبور است، یعنی کاربر ابتدا باید رمز عبور و شناسه را وارد کند و سپس اطلاعات ارسالی توسط سرور بررسی می‌شود. تنها پس از تأیید، دسترسی بر اساس سطح کاربر داده می‌شود. تکنیک‌های رمزنگاری متعددی برای رمزنگاری اطلاعات حساس استفاده شده است تا امنیت احراز هویت تضمین شود. اما چون این روش مبتنی بر نظریه رمزنگاری است، دارای محدودیت‌هایی است. برخی مقالات نیز طرح‌هایی ارائه داده‌اند که می‌تواند در برابر کنترل از راه دور رمزهای عبور مقاومت کند، اما این طرح‌ها نیز محدودیت دارند و نمی‌توانند در برابر حملات دستکاری رمزهای رمزنگاری شده در داخل سرور مقاومت کنند.

در طرح‌های احراز هویت کارت هوشمند مختلف، برخی طرح‌ها برای جلوگیری از حملات دستکاری جدول رمز عبور ارائه شده است، اما این طرح‌ها نمی‌توانند احراز هویت چند سرور را پشتیبانی کنند. توسعه سریع احراز هویت بیومتریک، به ویژه فناوری احراز هویت اثر انگشت، نقش مهمی در امنیت شبکه ایفا کرده است. در زمینه احراز هویت بیومتریک، احراز هویت اثر انگشت پیشرفت سریع داشته است.

سیستم رمزنگاری ابری یک سامانه مبتنی بر فناوری میکروسرویس است که بر اساس عملکردهای مختلف به ماژول‌هایی مانند امنیت و ذخیره‌سازی فایل تقسیم می‌شود. فریمورک Spring Cloud Sentinel می‌تواند فیوزهای کنترل فرآیند بین ماژول‌ها را فراهم کند. ماژول‌های مختلف از طریق ثبت و کشف خدمات، پراکسی معکوس انجام می‌دهند و درخواست‌های مختلف مشتری را به سرورهای شبکه داخلی منتقل می‌کنند و یک رابط متحد به مشتریان ارائه می‌دهند تا توسعه مشتریان مختلف تسهیل شود. بر اساس خوشه Nginx، در برخی مطالعات از Spring Cloud Zuul برای احراز هویت اشتغال در مجوزهای رابط مختلف استفاده شده است تا جمع‌آوری لینک‌های کلیدی در لاگ‌ها راحت‌تر شود و داده‌های لاگ جمع‌آوری شده به طور مداوم ذخیره و نمایش داده شوند.

مطالعات روش بازیابی برای تشخیص جنسیت فرعی را پیشنهاد داده‌اند که روند واقعی هر تشخیص را ثبت می‌کند. اگر نمایه‌سازی بر اساس کلیدواژه‌های جستجوی تاریخی باشد، لازم است روش‌های تشخیص ناموفق به کاربر بازگردانده شود. همچنین بسیاری از طرح‌های رمزنگاری مشابه متن اصلی ارائه شده‌اند که در سوابق تاریخی ایستا مختلف، روش‌های جستجوی رمزنگاری اطلاعات مختلف و روش‌های ارتباطی آن‌ها توصیف شده است.

۳. سیستم رمزنگاری اطلاعات ابری

۳,۱ پردازش رمزنگاری داده‌های اطلاعات شبکه

داده‌های اطلاعات شبکه دارای قواعد و نظم نامشخص هستند و داده‌های اطلاعات مختلف ویژگی‌های متفاوتی دارند. اطلاعات شبکه نیازمند به‌روزرسانی مداوم است. بنابراین، اطلاعات شبکه در بازسازی‌های فضایی مختلف، سری زمانی مشابهی دارند. برای حفظ بردار حریم خصوصی اصلی، کاوش دقیق در فضای

چندبعدی و حفظ حریم خصوصی داده‌ها، این عملیات می‌تواند امنیت اطلاعات را تضمین کند و از آسیب دیدن توسط کاوش ویژگی جلوگیری کند. فرض کنیم توالی اطلاعات y_M,...,y_2,y_1 , ..., y_2, y_1 باشد، ساختار بازسازی سری‌های زمانی مختلف اطلاعات به صورت زیر است:

Y=[y1y2⋯yHy1ay2a⋯yHay1nay2na⋯yMna] Y = \begin{bmatrix} y_1 & y_2 & \cdots & y_H \\ y_1^a & y_2^a & \cdots & y_H^a \\ y_1^{na} & y_2^{na} & \cdots & y_M^{na} \end{bmatrix}

پس از تغییر داده‌های اطلاعات شبکه، تأخیر زمانی بازسازی و نقاط داده‌های اطلاعات شبکه، سری‌های زمانی مختلف داده‌های اطلاعات بازسازی شده را در همان فضا نشان می‌دهند. تعداد نقاط P P از داده yj y_j به yi y_i که فاصله آن‌ها کمتر یا مساوی s s است به صورت زیر تعریف می‌شود:

P=∑i,jKs(K(yj,yi)) P = \sum_{i,j} K_s(K(y_j, y_i))

اگر نسبت تمام فاصله‌های تعیین شده انسانی و تمام سری‌های زمانی اطلاعات شبکه به تمام توالی‌های اطلاعات شبکه به عنوان توابع همبستگی مختلف تعریف شود، آنگاه:

DM(s)=1M(M−1)∑i≠jMKs(K(yj,yi)) D_M(s) = \frac{1}{M(M-1)} \sum_{i \neq j}^M K_s(K(y_j, y_i))

اطلاعات ورودی شبکه دارای درجه‌ای از حریم خصوصی هستند. اطلاعات ابری مختلف ویژگی‌های حریم خصوصی شبکه را در مرکز کلان ترکیب می‌کنند و سپس اطلاعات ابری شبکه را به صورت خوشه‌بندی تقسیم و نمونه‌های ویژگی ابری شبکه را دسته‌بندی می‌کنند:

ym=wmmin⁡(ym,wm) y_m = w_m \min(y_m, w_m)

برای نتایج خوشه‌بندی رمزنگاری حریم خصوصی اطلاعات شبکه، داده‌های حریم خصوصی تمام اطلاعات ابری شبکه بر اساس اعداد مختلف محاسبه منظم انجام می‌دهند و سپس بر اساس زمان شبکه رمزگذاری گروهی انجام داده و شبکه‌ها و اطلاعات مختلفی را ایجاد می‌کنند و سپس بر اساس مدل‌های مختلف مرتب می‌کنند. بردار رمزنگاری هایپرکائوتیک اطلاعات ابری شبکه به صورت زیر است:

βj=∑i=1nuiuj \beta_j = \sum_{i=1}^n u_i u_j

۳. سیستم رمزنگاری اطلاعات ابری

۳,۱ پردازش رمزنگاری داده‌های اطلاعات شبکه

داده‌های اطلاعات شبکه دارای قواعد و نظم مشخصی نیستند و داده‌های مختلف ویژگی‌های متفاوتی دارند. اطلاعات شبکه نیاز به به‌روزرسانی مداوم دارد. بنابراین، اطلاعات شبکه دارای سری زمانی مشابه در بازسازی‌های فضایی مختلف است. برای حفظ بردار حریم خصوصی اصلی، کاوش دقیق در فضای چندبعدی و حفظ حریم خصوصی داده‌ها، این عملیات می‌تواند امنیت اطلاعات را تضمین کند و از آسیب ناشی از کاوش ویژگی جلوگیری کند. فرض کنیم توالی اطلاعات y_M۲, y_۱y_ yM,...,۲y,۱y , ..., باشد، ساختار بازسازی سری‌های زمانی مختلف اطلاعات به صورت زیر است:

Y=[y1,y2,...,yHy1a,y2a,...,yHay1na,y2na,...,yMna] Y = \begin{bmatrix} y_1, y_2, ..., y_H \\ y_1^a, y_2^a, ..., y_H^a \\ y_1^{na}, y_2^{na}, ..., y_M^{na} \end{bmatrix}

پس از تغییر داده‌های اطلاعات شبکه، تأخیر زمانی بازسازی و نقاط داده‌های اطلاعات شبکه، سری‌های زمانی مختلف داده‌های اطلاعات بازسازی شده را در همان فضا نشان می‌دهند. تعداد نقاط P P از داده yj y_j تا y_i yi که فاصله آن‌ها کمتر یا مساوی s s است به صورت زیر تعریف می‌شود:

P=∑i,jKs(K(yj,yi)) P = \sum_{i,j} K_s(K(y_j, y_i))

اگر نسبت تمام فاصله‌های تعریف شده انسانی و تمام سری‌های زمانی اطلاعات شبکه به تمام توالی‌های اطلاعات شبکه به عنوان توابع همبستگی مختلف تعریف شود، آنگاه:

DM(s)=1M(M−1)∑i≠jMKs(K(yj,yi)) D_M(s) = \frac{1}{M(M-1)} \sum_{i \neq j}^M K_s(K(y_j, y_i))

اطلاعات ورودی شبکه دارای درجه‌ای از حریم خصوصی هستند. اطلاعات ابری مختلف وارد ویژگی‌های حریم خصوصی شبکه در مرکز کلان شده و با اطلاعات ابری حریم خصوصی شبکه به دست آمده در متن اصلی خوشه‌بندی می‌شود و نمونه‌های ویژگی ابری شبکه چندگانه طبقه‌بندی می‌شوند:

ym=wmmin⁡(ym,wm) y_m = w_m \min(y_m, w_m)

برای نتایج خوشه‌بندی داده‌های حریم خصوصی شبکه رمزگذاری شده، داده‌های حریم خصوصی تمام اطلاعات ابری شبکه به طور منظم بر اساس اعداد مختلف محاسبه می‌شوند و سپس به صورت گروهی بر

اساس زمان شبکه رمزگذاری می‌شوند تا شبکه‌ها و اطلاعات مختلف ایجاد شود و سپس بر اساس الگوهای مختلف مرتب می‌شوند. بردار رمزنگاری ابرآشوب اطلاعات ابری شبکه به صورت زیر است:

βj=∑i=1nuiuj \beta_j = \sum_{i=1}^n u_i u_j

در رمزنگاری اطلاعات ابری روی شبکه، به دلیل عدم تعادل شدید در ذخیره‌سازی داده‌های NSL KDD، پدیده‌های زیادی در فرآیند آموزش رخ داده است که باعث شده مدل نمونه‌های بیشتری در حین آموزش داشته باشد.

۳,۲ تأیید امنیت سیستم رمزنگاری اطلاعات ابری مبتنی بر فناوری بلاک‌چین

برای اطمینان از امنیت ارتباطات، داده‌ها از طریق ۲V ۰۲۰Z۷MYC Y ارسال می‌شوند. روش امضا به صورت زیر قابل بیان است:

sign(X,detail,xi,n,k,a) \text{sign}(X, \text{detail}, x_i, n, k, a)

پس از استفاده از فناوری امضا، امضای امنیتی داده با رمزنگاری دوگانه ترکیب می‌شود تا هدف ضد جعل امضا تحقق یابد.

داده‌های امنیتی ابتدا باید با محتوای متن پیام ترکیب شوند و سپس بر اساس اطلاعات فرستنده منتقل شوند. در این مقاله، شناسه فرستنده به عنوان منبع برچسب استفاده شده تا تأثیر تعارض برچسب‌ها کاهش یابد. بر اساس این، داده‌های پایه مختلف به عنوان کلیدهای رمزگشایی برای هر دو طرف ایجاد می‌شوند. برای افزایش محرمانگی، رمزنگاری و رمزگشایی حول امضای داده‌ها انجام می‌شود.

کلید رمزنگاری تولید شده بر اساس شناسه فرستنده به صورت زیر است:

S1=e(detail,xi,d1) S_1 = e(\text{detail}, x_i, d_1)

که در آن ۱s _۱s کلید رمزنگاری فرستنده است، ۱d _۱d اطلاعات فرستنده، ۱a _۱a و ۱h _۱h پارامترهای ترتیب و تجمع اطلاعات هستند.

کلید رمزگشایی پایه گیرنده به صورت زیر است:

S2=e(detail,xi,d2) S_2 = e(\text{detail}, x_i, d_2)

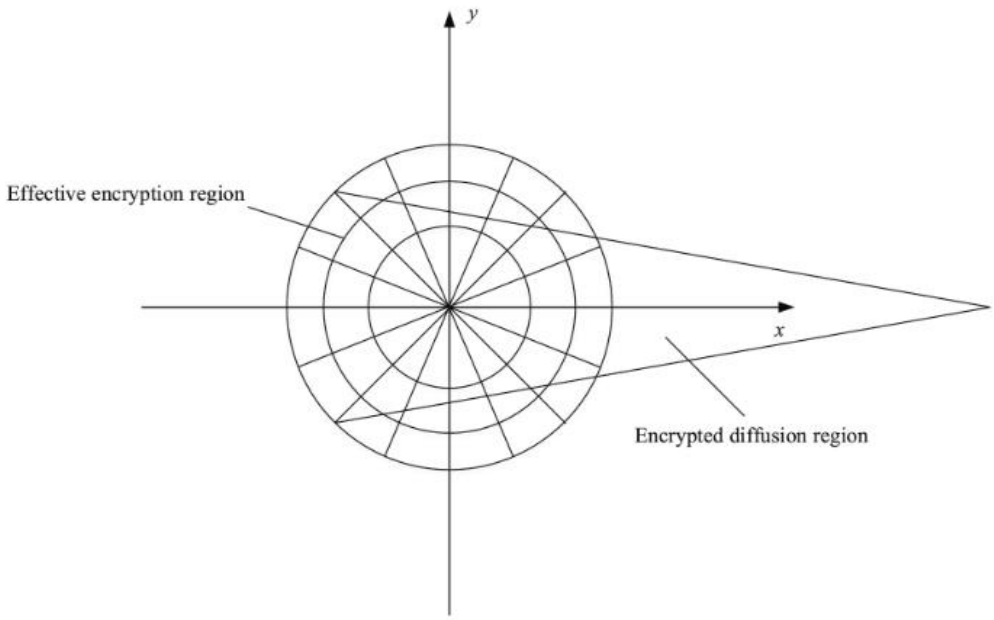
که در آن ۲s_ ۲s کلید رمزنگاری گیرنده است، ۲d_ ۲d اطلاعات گیرنده، ۲a_ ۲a و ۲h_ ۲h پارامترهای ترتیب و تجمع اطلاعات گیرنده هستند.

جدول ۱: دقت نتایج آزمایشی پردازش رمزنگاری

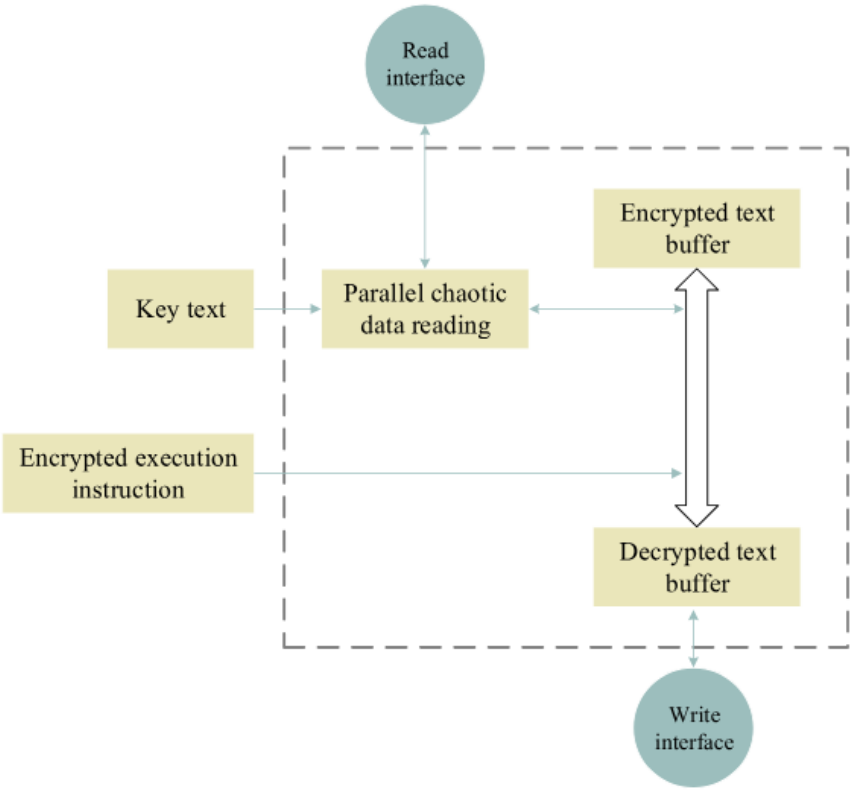
نوع داده	دقت رمزنگاری	نرخ بازیابی رمزنگاری
Normal	84.94%	96.17%
Probe	82.01%	82.39%
U2R	74.51%	22.95%
R2L	91.25%	14.62%

جدول ۲: نتایج کلی تست پردازش رمزنگاری

مدل	زمان آموزش (ثانیه)	زمان تست (ثانیه)	دقت وزنی (٪)
Random Forest	5.451	1.183	70.81
XGBoost	68.091	1.208	70.27



شکل ۱: مناطق مؤثر رمزنگاری اطلاعات ابری



شکل ۲: فرایند خواندن و نوشتن داده‌های اطلاعات ابری

۴. طراحی سامانه احراز هویت امنیت اطلاعات ابری

۴,۱ فناوری‌های مرتبط با احراز هویت هویتی

اطلاعات ابری به عنوان پشتیبانی اساسی برای صنایع کلیدی ملی، می‌تواند به کاربران امکان مجوز شبکه‌ای نسبتاً امن در توسعه‌های بزرگ‌مقیاس را بدهد. فرایند ارائه اطلاعات ابری به کاربران به عنوان احراز هویت هویتی نیازمند ارائه کدهای تأیید از سوی مشتریان است. در دنیای اینترنت، ارائه هر مجموعه داده مشخص نیازمند احراز هویت دیجیتال و مجوزدهی توسط ارائه‌دهندگان خدمات است. برخلاف هر هویت فیزیکی منحصر به فرد که ممکن است مورد حملات جایگزینی قرار گیرد، در یک سیستم خدمات لازم است هویت‌های دیجیتال و فیزیکی کاربران به صورت جداگانه تأیید و مجوزدهی شوند. هر هویت فیزیکی ممکن است در معرض حملات و تکثیر قرار گیرد. در یک سیستم خدمات، لازم است هویت‌های کاربران به صورت یک به یک نگاشت شوند. هنگام ثبت اطلاعات ابری موجود، اغلب رشته‌ای ثابت و رمز عبور ایستا تعیین و به مشتری داده می‌شود. هنگام احراز هویت، هر کاربر رمز عبور احراز هویت اختصاصی خود را دارد. اگر رمز عبور ارائه شده مطابقت داشته باشد، رمز عبور تولید شده توسط کاربر قانونی به عنوان رمز ایستا خود استفاده می‌شود. اگر روش ایمن‌تری ارائه نشود، کاربران ممکن است از روش‌هایی مانند تاریخ تولد تلفن برای شکستن رمزهای ایستا استفاده کنند. اگر عامل امنیتی رمزهای ایستا کافی نباشد، تهدیداتی مانند افشا، رهگیری، حملات کسب و حملات جستجوی فراگیر متوجه آنها خواهد بود.

گواهی‌های دیجیتال به عنوان کارت هویت دیجیتال شبکه کاربران، حامل اطلاعات کلیدی مانند کلیدهای عمومی کاربر هستند. احراز هویت دیجیتال کاربران می‌تواند به عنوان گواهی‌های شخص ثالث مورد استفاده قرار گیرد و به موجودیتی مورد اعتماد در مدیریت، احراز هویت و لغو گواهی‌ها تبدیل شود. CIA گواهی‌های دیجیتال را در قالب استاندارد بر اساس کلید عمومی و اطلاعات کاربر تولید می‌کند و به صورت دیجیتال بر روی صلاحیت گواهی امضا می‌کند. اصل کار آن در شکل ۳ نشان داده شده است:

معادلات کد تصحیح خطا

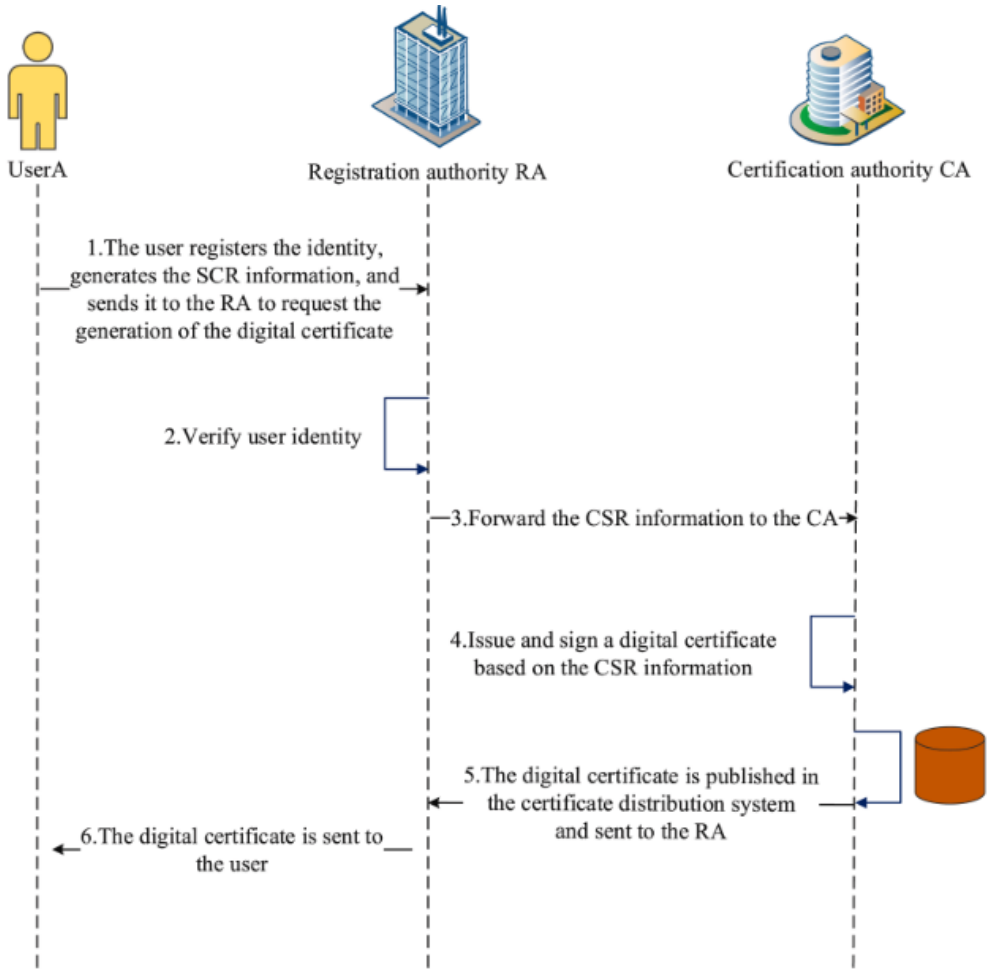
برای اطلاعات داده‌های مختلف، ابتدا باید کد خطا اصلاح و سپس بر اساس الگوریتم کد کنترلی محاسبه شود. مراحل بر اساس چندجمله‌ای داده‌های نمادین و کاراکترهای داده‌ها بر اساس کد کلمه است:

$$d(x)=dn−1xn−1+dn−2xn−2+⋯+d1x+d0$$ d(x) = d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_1 x + d_0

چندجمله‌ای تولید کد تصحیح خطا به صورت زیر است:

$$g(x)=x3+x2+⋯+g1x+g0$$ g(x) = x^3 + x^2 + \cdots + g_1 x + g_0

رابطه اعتماد همچنین می‌تواند از طریق زنجیره اعتماد منتقل شود. اگر لازم باشد اعتبار یک گواهی دیجیتال تأیید شود، باید رابطه ایجاد انتقال گواهی بر اساس مسیر اعتماد CA بررسی شود تا مدل اعتماد مسیر تعیین گردد.



شکل ۳. اصول کار سیستم احراز هویت امنیت اطلاعات ابری.

الگوریتم فیلتر کاکوی

الگوریتم فیلتر کاکوی از هش کاکوی نشأت گرفته است. هش‌های کاکوی مختلف به عنوان دو هش خالی تعریف می‌شوند هنگام فیلتر کردن یک رویداد. هر موقعیت در یک لیست دارای چند جایگاه مختلف است و هر تابع هش می‌تواند برخوردهای هش را مدیریت کند. به دلیل اینکه جداول هش مختلف فقط اثر انگشت عناصر را ذخیره می‌کنند، فرآیند محاسبات ساده شده است (شکل ۴).

هنگام احراز هویت هویت کاربر، گره احراز هویت باید گواهی‌های معتبر را از طریق فیلتر دوگانه کاکوی جستجو کند. اگر تعداد گواهی‌های معتبر بیشتر از تعداد گواهی‌های لغو شده باشد، باید فیلتر با عناصر کمتر

جستجو شود. وقتی گواهی به فیلتر گواهی لغو تعلق نداشته باشد، نتیجه منفی واقعی به درستی تعیین می‌شود. اگر گواهی معتبر باشد، نتیجه بازگردانده می‌شود. اگر فیلتر کاکوی مثبت کاذب صادر کند، نیاز به بررسی بیشتر گواهی وجود دارد.

۴,۲ پیاده‌سازی و آزمون سامانه احراز هویت امنیت اطلاعات ابری

این سامانه می‌تواند هویت کاربران پلتفرم ابری را در حین عملیات تأیید کند. اگر اطلاعات احراز هویت از یک بعد مشابه آغاز شود، اطلاعات ورود سنتی برای تأیید تقویت می‌شود. اگر بیشتر سیستم‌های ورود احراز هویت متفاوت باشند، این سامانه می‌تواند احراز هویت سنتی را به احراز هویت امنیتی مستمر ارتقا دهد. نظارت کامل فرآیند می‌تواند بر اساس دیدگاه‌های زمان اجرای مختلف انجام شود تا اطمینان حاصل شود که سامانه با مجوزهای صحیح کاربران به طور منطقی عمل می‌کند.

این سامانه با ساختار CS طراحی شده و عوامل مختلف احراز هویت هویتی را از طریق سیستم احراز هویت ترمینال ویندوز ترکیب می‌کند. برای ارائه خدمات احراز هویت سریع، ایمن و مستمر به کاربران قانونی سرورهای ابری، لازم است روش نجات چرخه‌ای بدون وقفه مسدود شود.

هسته اصلی این سامانه احراز هویت دو عاملی هنگام ورود است که ورود سریع را تسهیل می‌کند. این نیازمند روشی خاموش و قابل مشاهده برای تأیید ایمن هویت در سیستم شناسه وارد شده توسط کاربر است. همچنین هنگام پردازش اطلاعات هویتی ایمن محلی، لازم است ماژول احراز هویت و ماژول امنیتی در سمت سرور ابری ترکیب شوند.

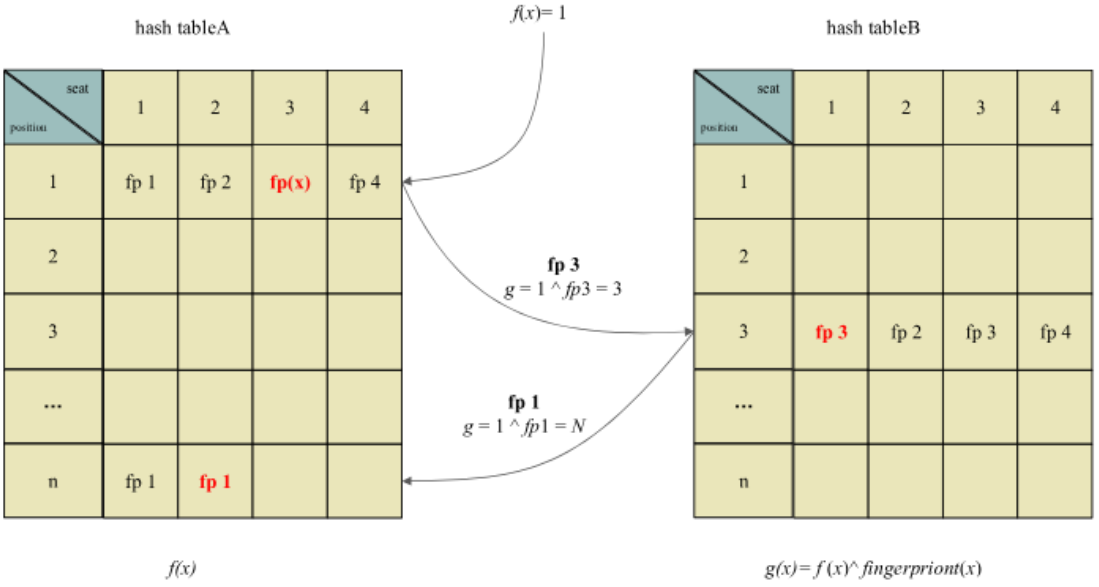
حامل تعاملی داده‌های هویتی می‌تواند به عنوان JWS برای انتقال داده‌های مختلف استفاده شود. فرمت داده ذکر شده در مقاله می‌تواند محتوا را بر اساس روش امضای داده‌ها محافظت کند. برای تأمین نیازهای امنیت داده‌ها، امضاهای JWS می‌توانند به صورت تعاملی در ماژول‌های عملکردی مختلف بر اساس امضای دیجیتال بارگذاری قالب‌بندی شوند. قالب طراحی بارگذاری داده JWS با عملکردهای مختلف تعریف می‌شود. ثبت بارگذاری JWS و قالب تعامل داده‌ها در جدول ۳ نشان داده شده است.

سیستم ویندوز هسته اصلی این سامانه از نظر احراز هویت امنیت ترمینال است. عملکردهای آن عمدتاً شامل جمع‌آوری اطلاعات نام کاربری و پردازش و بارگذاری هویت تصویری است. اگر اطلاعات لوگوی کاربر فعلی نتواند عملیات ورود را گذرانده، ماژول احراز هویت هویتی در سمت سرور ابری باید به سرعت جمع‌آوری اطلاعات کاربر را پردازش کند تا تأیید امنیت اطلاعات پایگاه داده تسهیل شود. ماژول هسته سرور ابری مسئول جمع‌آوری اطلاعات، پردازش داده‌ها و سایر مسئولیت‌های مهم در سمت کاربر است. ماژول احراز هویت امنیتی نیاز به همکاری با دایرکتوری‌ها برای اجرای ویژگی‌های امنیتی، اطلاعات یا تغییرات دارد. اجرای وظایف مختلف احراز هویت در سامانه احراز هویت و شناسایی امنیتی عمدتاً از دو بخش اصلی تشکیل شده است: ماژول پردازش ترمینال و ماژول پردازش سرور ابری.

در فرایند طراحی سامانه، امنیت مستمر هسته اصلی است. برخلاف احراز هویت یک‌باره سایر سیستم‌ها، این سامانه مسائل موجود در محیط واقعی کاربرد را در نظر می‌گیرد. دلیل قفل کردن کامپیوتر توسط کاربران جلوگیری از نفوذ عملیات غیرقانونی در این دوره است. در شناسایی اطلاعات هویتی امن، لازم است احراز هویت هویتی شفاف و ایمنی برای اطلاعات کاربر انجام شود تا از عملیات نادرست ناشی از بی‌احتیاطی جلوگیری شود. این عملیات ممکن است برای کاربران نامحسوس و شفاف باشد، اما سامانه احراز هویت هویتی محلی می‌تواند از طریق پردازش خاموش پس‌زمینه عملیات مختلفی انجام دهد، در حالی که کاربران قانونی انگار هیچ‌گاه چنین اتفاقی را مشاهده نکرده‌اند. در پردازش سامانه امنیتی احراز هویت محلی، لازم است بر اساس روش ورود سنتی وارد شوند. فقط پس از تأیید اطلاعات امنیتی، احراز هویت اطلاعات هویتی در سایر فرآیندهای ورود تکمیل می‌شود.

پشتیبانی از نسخه‌های مختلف سیستم ویندوز

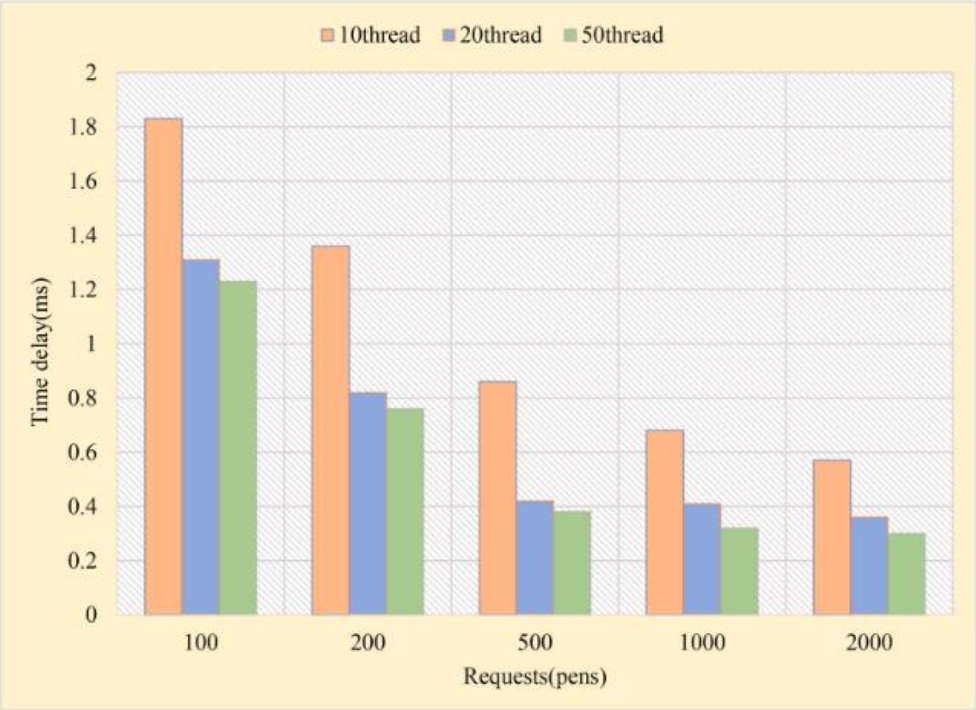
این ماژول احراز هویت باید تفاوت‌های نسخه سیستم عامل جامعه کاربران ابر غالب فعلی را در نظر بگیرد. اکثر نسخه‌های سیستم عاملی که کاربران استفاده می‌کنند، شامل ویندوز ۷، ویندوز ۸، ویندوز ۱۰ و نسخه‌های دیگر است. برای ایجاد تفاوت‌هایی هنگام ورود در نسخه‌های مختلف سیستم عامل، سرور باید هویت امنیتی کاربر را هنگام بررسی طراحی احراز هویت کند و به‌صورت روان بین سیستم‌ها سوییچ کند تا ریسک‌های ناشی از تغییرات مکانیزم احراز هویت مدیریت شود. هم سرور اصلی و هم سایر سرورها هنگام برنامه‌نویسی مبتنی بر نسخه سیستم عامل مکانیزم احراز هویت را گذرانده‌اند. منابع سیستم محلی برای پردازش تصویر و احراز هویت امنیتی فراهم شده است. بخشی از سامانه احراز هویت امنیتی پردازش شده در سمت سرور ابر می‌تواند روی کامپیوتر ترمینال قرار گیرد.



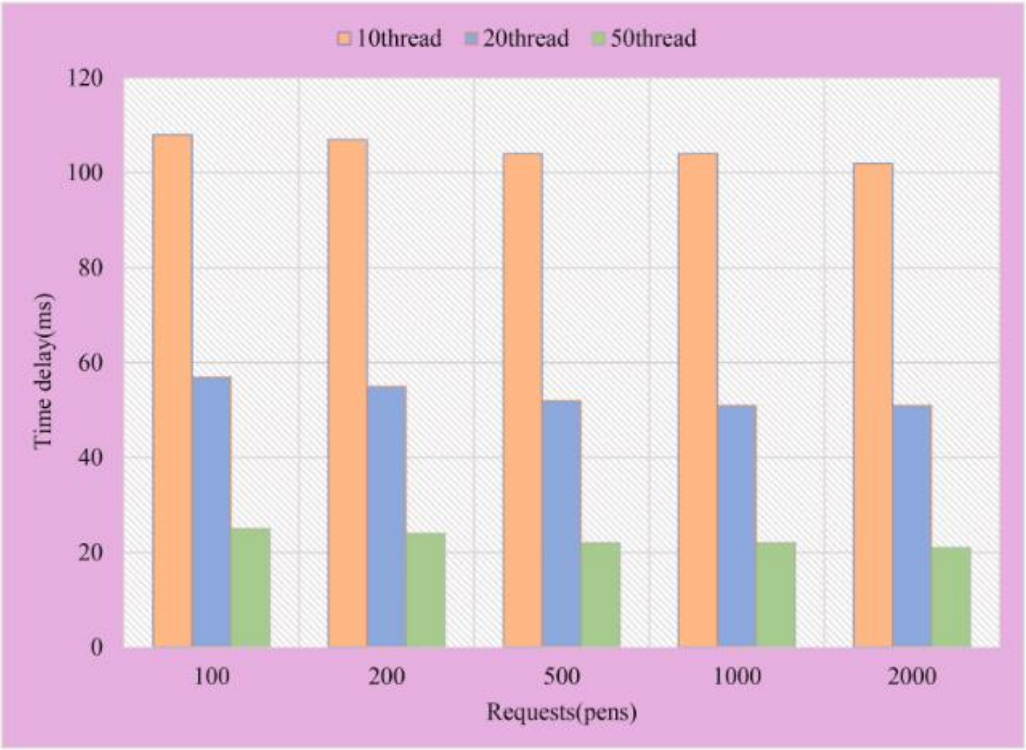
شکل ۴: تبدیل فیلتر کاکوی اطلاعات ابری

جدول ۳: قالب بارگذاری JWS ثبت احراز هویت امنیت اطلاعات ابری

Type	UID	Signature	KeyInfo	PKu	گزینه داده
شرح داده	حساب احراز هویت ثبت شده کاربر	شناسه احراز هویت ابر اطلاعات ثبت شده توسط کاربر	امضای احراز هویت ثبت کاربر	ابر اطلاعات	احراز هویت هویتی کاربر



شکل ۵: تأخیر ایجاد DID احراز هویت هویتی



شکل ۶. تأخیر تأیید هویت DID.

۵. نتیجه‌گیری

این مقاله به بررسی چالش‌های مختلفی مانند رمزنگاری شبکه و پژوهش مبتنی بر سامانه‌های رمزنگاری و احراز هویت اطلاعات ابری و سامانه‌های احراز هویت امنیتی پرداخته است. سامانه احراز هویت امنیتی اطلاعات ابری بر پایه رمزنگاری شبکه پیاده‌سازی شده است تا انجام عملکردهای اصلی سامانه احراز هویت امنیتی را تسهیل کند. در این مقاله، برنامه‌های کاربردی از طریق قراردادهای هوشمند بین بلاک‌چین‌ها منتقل می‌شوند. پردازش داده‌ها و منطق اطلاعات نیازمند انتقال باز و شفاف است. از جمله عملکردهای سامانه، باید عملیات پرس‌وجو، به‌روزرسانی و مجوزدهی در قراردادهای هوشمند پیاده‌سازی شود و سیستم رمزنگاری که بتواند به‌خوبی با اطلاعات هماهنگ شود به شرح زیر است:

۱. تحلیل و پژوهش عمیق مستمر بر روی سامانه‌های رمزنگاری اطلاعات ابری که در چین رتبه‌بندی شده‌اند، وضعیت فعلی اطلاعات ابری را تحلیل و ویژگی‌های سامانه‌های رمزنگاری مختلف را مقایسه کند. بر اساس ویژگی‌های سامانه‌های رمزنگاری، مسائل دشوار در فرایند طراحی اطلاعات جمع‌بندی شود.

۲. بر اساس معماری پژوهش، سامانه باید فناوری رمزنگاری کلیدهای مرتبط با محتوا را خلاصه کند. بر این اساس، فناوری هسته‌ای به عنوان تضمین جزئی از قابلیت اطمینان احراز هویت امنیتی، بهینه‌سازی‌ها و معرفی فناوری بلاک‌چین را انجام داده است.
۳. فناوری رمزنگاری اطلاعات ابری و معماری سامانه به تفصیل طراحی شده است. همچنین برای معماری سامانه رمزنگاری، عملکردهای مختلف باید به صورت متفاوت طراحی شوند.
۴. در زمینه فناوری احراز هویت امنیتی، لازم است عملکرد انتقال و همزمانی سامانه آزمایش و بهبود یابد تا قابلیت استفاده و کامل بودن سامانه اثبات شود.

منابع

[۱] K. Katz, O. Shutov, R. Lapoint, et al., The sequence read archive: a decade m explosive growth, Nucleic Acids Res. ۵۰ (D۱) (۲۰۲۲) D۳۸۷–D۳۹۰.
[۲] Naman H., Hussien N., Al-dabag M., et al. Encryption system for hiding information based on internet of things. ۲۰۲۱. ore of
[۳] V. Lytvyn, I. Peleshchak, R. Peleshchak, et al., Information encryption based on the synthesis of a neural network and AES algorithm, in: Proceedings of the ۲۰۱۹ ۳rd International Conference on Advanced Information and Communications Technologies (AICT), IEEE, ۲۰۱۹, pp. ٤٤٧–٤٥٠.
[٤] J. Ding, Y. Wang, Fu X. Wihi, WiFi based human identity identification using deep learning, IEEE Access ۸ (۲۰۲۰) ۱۲۹۲٤٦–۱۲۹۲٦۲.
[٥] S. Kaman, K. Swetha, S. Akram, et al., Remote user authentication using a voice authentication system, Inf. Secur. J. Glob. Perspect. ۲۲ (۳) (۲۰۱۳) ۱۱۷–۱۲٥.
[٦] A. Ponticello, M. Fassl, K. Krombholz, Exploring authentication for security-sensitive tasks on smart home voice assistants, in: Proceedings of the SOUPS@ USENIX Security Symposium, ۲۰۲۱, pp. ٤٧٥–٤٩۲.
[۷] Z. Cui, X.U.E. Fei, S. Zhang, et al., A hybrid blockchain-based identity authentication scheme for multi-WSN, IEEE Trans. Serv. Comput. ۱۳ (۲) (۲۰۲۰) ۲٤۱–۲٥۱.
[۸] P.N. Mahalle, B. Anggorojati, N.R. Prasad, et al., Identity authentication and capability based access control (IACAC) for the internet of things, J. Cyber Secur. Mobil. ۱ (٤) (۲۰۱۳) ۳۰۹–۳٤۸.
[۹] C.H. Hsu, S. Wang, D. Zhang, et al., Efficient identity authentication and encryption technique for high throughput RFID system, Secur. Commun. Netw. ۹ (۱٥) (۲۰۱٦)۲٥۸۱ –۲٥۹۱.
[۱۰] C. Yu, H. Li, X. Wang, SVD-based image compression, encryption, and identity authentication algorithm on cloud, IET Image Process. ۱۳ (۱۲) (۲۰۱۹) ۲۲۲٤–۲۲۳۲.
[۱۱] Z.A. Zukarnain, A. Muneer, M.K. Ab Aziz, Authentication securing methods for mobile identity: issues, solutions and challenges, Symmetry ۱٤ (٤) (۲۰۲۲) ۸۲۱ (Basel).
[۱۲] Q. Tian, Y. Lin, X. Guo, et al., An identity authentication method of a MIoT device based on radio frequency (RF) fingerprint technology, Sensors ۲۰ (٤) (۲۰۲۰) ۱۲۱۳. Fig. ٦. Identity authentication DID verification delay. T. Li and S. Liu Results in Engineering ۲۷ (۲۰۲٥) ۱۰٦۲٥٤
۱۳] M. Tebaa, S. El Hajji, A. El Ghazi, Homomorphic encryption method applied to

cloud computing. ۲۰۱۲ National Days of Network Security and Systems, IEEE, ۲۰۱۲, pp. ۸٦–۸۹.
[۱٤] M. Horv´ath, Attribute-based encryption optimized for cloud computing, in: Proceedings of the SOFSEM ۲۰۱٥: Theory and Practice of Computer Science: ٤۱st International Conference on Current Trends in Theory and Practice of Computer Science, Pec pod Sn˘e˘zkou, Czech Republic, January ۲۹-۲٤, ۲۰۱٥. Proceedings ٤۱, Springer Berlin Heidelberg, ۲۰۱٥, pp. ٥٦٦–٥۷۷.
[۱٥] M.A. Hossain, A. Al Hasan M, Improving cloud data security through hybrid verification technique based on biometrics and encryption system, Int. J. Comput. Appl. ٤٤(٥) (۲۰۲۲) ٤٥٥–٤٦٤

Identity Authentication System for Cloud Information Security Based on Computer Cryptography and Network Security

Elham Vahidian *Zahra Ranjbar, Asma Beheshtipour, Forough Ahmadi Shad

Abstract

Identity authentication technology is of great importance in daily life. In every platform, we need to log in to the user account to verify the status and transactions of the account. Of course, identity authentication is also an essential and important part of platform businesses. More and more data from applications is transferred to the cloud for operation and storage, while the cloud information security mechanism is also continuously implemented. On the other hand, this paper uses blockchain technology for secure identity authentication. In the context of the secure voice authentication system, the existing security status of Windows systems adds a secure multi-factor authentication mechanism. In the context of the cloud operation mechanism, continuous coordination is used to ensure the security of the system. This paper introduces in detail the identity authentication system composition, design, implementation process and practical experimental results related to information security. In the field of identity authentication information, cloud information systems can continuously improve the security performance of identities.

Keywords: Cryptographic system, cloud information, identity authentication, blockchain