مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۱ ، پاییز ۱۳۹۷، ص ۱۵- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال سوم)
شماره ۱۱ / پاییز ۱۳۹۷ / ص ۱۵- ۱

دسترسی امن در اینترنت اشیاء به وسیله احراز هویت چند عاملی کاربر و مبتنی بر بیومتریک سبک

محمدرضا فدوی امیری [۱]، محمدرضا خوانساری [۲]، مهدی رضاتبار [۳]

[۱] استادیار، گروه مهندسی کامپیوتر، دانشگاه شمال.

[۲] مربی، گروه مهندسی کامپیوتر، موسسه آموزش عالی علوم و فناوری آریان.

[۳] کارشناسی ارشد، مهندسی کامپیوتر، شبکه‌های کامپیوتری، موسسه آموزش عالی علوم و فناوری آریان.

نام نویسنده مسئول:
محمدرضا فدوی امیری

چکیده

با اینترنت اشیاء کاربر می‌تواند از طریق برنامه‌های کاربردی دستگاه‌های هوشمند، در هر زمانی و در هر مکانی قابل دسترسی باشد که این کار امنیت و حریم خصوصی را برای اینترنت اشیاء دشوار می‌سازد. برای ایجاد دسترسی امن، احراز هویت چندعاملی می‌تواند امنیت بالاتری را تضمین نماید. ترکیب یک عامل دوم مبتنی بر خصوصیات بیومتریک فردی کاربر به منظور طرح احراز هویت قوی‌تر کاربر و افزایش امنیت هدف اصلی می‌باشد. از طرفی، چون گره‌ها در شبکه‌های اینترنت اشیاء منابع محدودی از لحاظ قدرت پردازش، باطری پشتیبان، حافظه، سرعت و غیره دارند، از این رو یک راه حل امنیتی سبک مورد نیاز می باشد.

در این پژوهش، از اثر انگشت به عنوان عامل بیومتریک استفاده شده است. پس از اسکن اثر انگشت، نقاط کلیدی آن تعیین می‌گردد. البته با توجه به اینکه زمان مقایسه بعد از بالا رفتن حجم پایگاه داده، بالا می‌رود، به جای ذخیره تصویر اسکن شده اثر انگشت، نقاط کلیدی اثر انگشت اسکن شده استخراج می‌گردد و سپس عامل دوم که کلمه عبور می‌باشد، دریافت و جهت امنیت بیشتر با الگوی برداری ایجاد شده از نقاط کلیدی اثر انگشت، ترکیب و رمزنگاری شده و در پایگاه داده ذخیره می‌گردد. در فاز احراز هویت کاربر، با بررسی نقاط کلیدی اثر انگشت ورودی و کلمه عبور، برای کاربر مجاز، اتصال به گره دروازه و دسترسی به تجهیزات منشعب از گره مذکور فراهم می‌گردد.

به دلیل اهمیت مصرف انرژی در محیط اینترنت اشیاء، از میان روش‌های رمزنگاری مختلف، از XOR و ترکیب داده بیومتریک با کلمه عبور رمزنگاری شده استفاده گردید تا رسیدن به هدف مورد نظر میسر گردد. روش پیشنهادی با روش‌های رمزنگاری DES، RSA و ECC مورد مقایسه قرار گرفته و جهت تست امنیت رمزنگاری از روش تست بهمنی اکید استفاده گردید. روش پیشنهادی از نظر تست امنیتی انجام شده و نیز مصرف انرژی نتیجه ایده آلی داشته است.

واژگان کلیدی: اینترنت اشیاء، احراز هویت، امنیت، بیومتریک، رمزنگاری، هش ادراکی.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۱ ، پاییز ۱۳۹۷، ص ۱۵- ۱

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

اینترنت اشیاء[1]، مفهوم نسبتاً جدیدی در دنیای فناوری اطلاعات و ارتباطات است که توسط آن برای هر شیء قابلیت ارسال و دریافت داده از طریق شبکه‌های ارتباطی فراهم می‌شود. با ارتباط اشیاء، توانایی‌هایی همچون ردیابی یکدیگر، هماهنگی باهم و نیز کنترل میسر می‌گردد. با توسعه سریع اینترنت اشیاء، انواع کاربردهای اینترنت اشیاء وجود دارند که در زندگی روزمره به کار گرفته می‌شوند. این کاربردها از تجهیزات معمولی گرفته تا کل لوازم خانگی را شامل شده و کیفیت زندگی انسان را بهبود می‌دهد [۱].

اینترنت اشیاء راحتی و آسایش را برای مردم به ارمغان می‌آورد، ولی اگر اینترنت اشیاء نتواند امنیت حریم خصوصی افراد را تضمین کند، آنگاه اطلاعات خصوصی آنها ممکن است در هر زمانی در معرض خطر قرار گیرد. بنابراین امنیت اینترنت اشیاء نمی‌تواند نادیده گرفته شود. با انتشار گسترده اینترنت اشیاء، این حوزه اطلاعات بسیار ارزشمندی را فراهم خواهد کرد و خطر افشای چنین اطلاعاتی بالا خواهد رفت. اگر اینترنت اشیاء نتواند راه حل خوبی برای مسائل امنیتی داشته باشد، آنگاه توسعه آن تا حد زیادی محدود خواهد شد. بنابراین، فراتر از تمام مسائل اینترنت اشیاء، مشکل امنیتی به طور خاص مهم است. امنیت اطلاعات به اقدامات اتخاذ شده برای جلوگیری از استفاده غیرمجاز، سوء استفاده، دستکاری، یا انکار دانش، حقایق، داده‌ها یا قابلیت‌ها اشاره دارد [۲].

احراز هویت

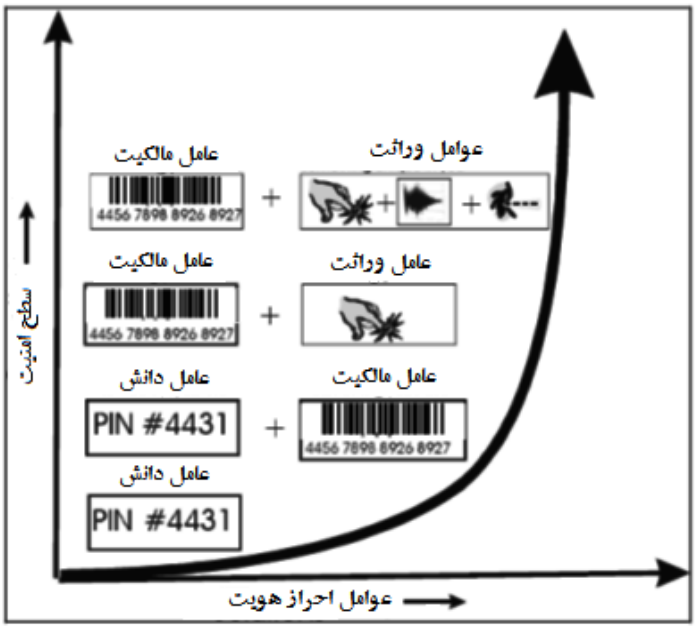
احراز هویت[2]، که نماد هویت کاربر می‌باشد، شامل سه عامل مالکیت، دانش و وراثت می‌باشد. عامل مالکیت یعنی هر چیزی که کاربر دارد مانند کارت های هوشمند، تلفن‌های هوشمند، توکن‌ها[3] و غیره. عامل دانش یعنی هر چیزی که کاربر می داند بعنوان مثال کلمه عبور و عامل وراثت یعنی چیزی که متعلق به کاربر است مثل اثر انگشت، چهره‌نگاری، اسکن عنبیه و غیره [۳].

طرح احراز هویت به صورت سنتی عمدتاً مبتنی بر عامل دانش مانند کلمه عبور می‌باشد. با این حال در چند سال گذشته دیده شده که احراز هویت تک عاملی[4]، رویکرد مبتنی بر کلمه عبور بوده است که نفوذ در آن بسیار آسان بوده و از این رو برای تضمین امنیت کافی نبوده است. بنابراین ترکیب یک عامل دوم مبتنی بر خصوصیات بیومتریک (زیستی) فردی کاربر می‌تواند طرح احراز هویت قوی‌تری را توسعه دهد [۴]. در این پژوهش از اثر انگشت به عنوان عامل بیومتریک استفاده شده است.

استفاده از عوامل تعیین هویت بصورت ترکیبی امنیت بیشتری را تامین می‌نماید. چرا که عوامل مالکیت می‌توانند گم، فراموش یا به راحتی کپی شوند، عوامل دانش می‌تواند فراموش شود و اینکه هر دو عامل دانش و مالکیت می‌توانند دزدیده و یا به اشتراک گذاشته شوند. در نتیجه انکار آن آسان است انکار اینکه شخص عملی را انجام داده، زیراکه فقط عوامل مالکیت یا دانش چک می شود، و این‌ها فقط پیوند ضعیفی با هویت شخص دارند. علم بیومتریک یک راه حل ظریف برای این مسائل توسط تایید هویت درست فرد، تولید می کند. در شکل ۱ سطوح امنیتی احراز هویت با استفاده از عوامل مختلف احراز هویت نشان داده شده است.

[1] Internet of Things
[2] Authentication
[3] Token
[4] Single Factor Authentication (SFA)

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۱ - استفاده از بیومتریک ها برای افزایش سطح امنیت

علم بیومتریک

واژه بیومتری از واژگان یونانی Bios به معنی حیات و Metrikos به معنی میزان آمده است. می‌دانیم که بشر به طور غریزی از برخی خصوصیات بدن همچون چهره، طریقه گام برداشتن یا صدا برای تشخیص یکدیگر استفاده می‌کند. بنابراین، امروزه با تنوع وسیعی از کاربردها، نیاز به برنامه‌های تایید قابل اعتماد برای تایید هویت یک شخص، تشخیص افراد بر مبنای خصوصیات بدن آنها، در کاربردهای تکنولوژی امروزی، بیش از پیش جالب توجه شده است. بطور سنتی، اسم رمز و کارت های شناسایی افراد برای محدود کردن اجازه ورود به سیستم‌های امنیتی استفاده شده‌اند، اما این متدها غیر قابل اعتماد می‌باشند و می‌توان به راحتی در آنها نفوذ کرد، در حالی که خصوصیات زیست سنجی (بیومتریک) نمی‌تواند اقتباس، دزدیده، یا فراموش شود و جعل کردن آن عملاً غیرممکن می باشد.

بیومتریک، علم تعیین یا تایید هویت یک شخص مبتنی بر خصوصیات فیزیولوژیکی یا رفتاری می باشد و یک ویژگی منحصربه فرد و قابل اندازه گیری برای تشخیص هویت می‌باشد. یک سیستم بیومتریک اساساً یک سیستم تشخیص الگو می‌باشد که فردی را بر مبنای بردار ویژگی مشتق شده از خصوصیات فیزیکی و رفتاری که شخص مورد نظر شامل می‌باشد، تشخیص می‌دهد [۵]. بردار ویژگی پس از استخراج شدن، معمولاً در یک پایگاه داده ذخیره می گردد و یا بر روی یک کارت هوشمند داده شده به فرد ذخیره می شود. یک سیستم زیست سنجی مبتنی بر خصوصیات فیزیکی عموماً قابل اتکاتر از سیستم زیست سنجی است که از خصوصیات رفتاری اقتباس شده باشد، اگرچه ممکن است جمع آوری خصوصیات رفتاری در برخی کاربردهای خاص، آسان تر باشد.

اضافه کردن بیومتریک مزایای متعددی دارد چرا که جعل یا توزیع آن مشکل می‌باشد، از دست داده و یا فراموش نمی‌شود و کپی کردن ازآن نیز مشکل است. بیومتریک یک عامل مقیاس پذیر برای احراز هویت قوی کاربر است که بسیاری از سازمان ها می توانند خود و کاربرانشان را امن نگه دارند. همچنین با سرعتی که همه چیز به اینترنت متصل می‌شود احراز هویت چند عاملی یک راه حل مناسب برای اطمینان از امنیت و محرمانگی در شبکه‌های اینترنت اشیاء می‌باشد. در مرجع [۶] به پنج ویژگی زیست سنجی (بیومتریک) اشاره شده است:

- جهانی بودن: زیست‌سنجی یک ویژگی جهانی است که هر فردی از آن برخوردار است.
- متمایز بودن: هر فردی دارای ویژگی زیست‌سنجی مجزا می‌باشد.
- ماندگاری: ویژگی‌های زیست‌سنجی هرگز در طول زمان تغییر نمی‌کند.
- قابل جمع‌آوری: ویژگی‌های زیست‌سنجی می‌تواند اندازه‌گیری شده و به راحتی با دستگاه‌های موجود مانند دستگاه‌های تشخیص اثر انگشت و ... بدست آید.
- منحصر به فرد: ویژگی‌های زیست‌سنجی برای هر شخص منحصر به فرد می‌باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

چندین نیازمندی کلیدی برای توسعه یک طرح احراز هویت کاربر راه دور موثر برای شبکه‌های اینترنت اشیاء مورد نیاز می‌باشد که در این پژوهش موارد زیر مورد توجه می‌باشد:

- راه حل امنیتی سبک وزن: گره‌ها در شبکه‌های اینترنت اشیاء منابع محدودی از لحاظ قدرت پردازش، باطری پشتیبان، حافظه، سرعت و غیره دارند. از این رو یک راه حل امنیتی سبک وزن مورد نیاز می‌باشد.
- احراز هویت چند عامله: شکستن طرح تک عامله مبتنی بر کلمه عبور آسان می‌باشد، بنابراین، اضافه کردن یک عامل دوم مبتنی بر زیست سنجی فردی امنیت طرح را افزایش‌می دهد.

طبقه بندی روش‌های زیست سنجی

عموماً در سیستم‌های بیومتریک از دو نوع ویژگی مختلف افراد جهت شناسایی استفاده می‌شود که در ذیل به آنها اشاره می‌شود. این طبقه بندی در شکل ۲ نشان داده شده است.

پارامترهای فیزیولوژیکی

اساس شناسایی در این کلاس، اندازه گیری و آنالیز مشخصه‌های ثابت یک شخص می‌باشد. این دسته از ویژگی‌ها به مجموعه ای از خصوصیات همراه انسان اعم از اثرانگشت، عنبیه چشم، چهره، DNA و غیره اشاره دارد، این ویژگی‌ها عمدتاً از بدو تولد انسان و گه‌گاه قبل از تولد انسان شروع به شکل‌گیری نموده و تا آخر عمر در بدن انسان ثابت و غیرقابل تغییر (گاهاً با تغییرات بسیار اندک) می‌مانند.

پارامترهای رفتاری

شناسایی الگوهای رفتاری مشخص یک فرد می‌باشد که این ویژگی‌ها در حقیقت خصوصیات ناشی از رفتارهای انسان هاست نظیر راه رفتن انسان، نحوه فشردن دکمه ها مثلاً موبایل، صفحه کلید و غیره که می‌تواند بیان‌گر مشخصات یک انسان خاص باشد نظیر راه رفتن یک انسان که گاهی با نگاه کردن آن از پشت سر می‌توان تشخیص داد که وی کدام یک از دوستانتان است.

شکل ۲ – طبقه بندی کلی روش‌های زیست سنجی

ISSN: 2745-3673
http://www.Rcsj.ir

اثر انگشت

یکی از قدیمی‌ترین روشهای تشخیص هویت، روش شناسایی از طریق اثر انگشت[5] می‌باشد. در تمام قسمت های کف دست و پای ما، به صورت پیوسته پوست ما با خطوط نازکی چین خورده است که الگویی از خطها و شیارها را به وجود می آورد. این خطوط برجسته روی انگشت خطوط اصطکاکی[6] نامیده می‌شود. از طریق این خطوط، به دلیل افزایش اصطکاک با اجسام، دست می تواند اشیاء را نگه دارد و همچنین حس لامسه در تماس با سطح اشیاء افزایش می یابد. علاوه بر این، به وسیله همین خطوط اصطکاکی هویت افراد تشخیص داده می‌شود زیرا این خطوط برای هر یک از انگشتان دست هر فرد منحصر به فرد و غیر قابل تغییر است به طوری که به کمک اثر انگشت حتی می توان دوقلوهای همسان را از یکدیگر تمیز داد [۷].

الگوهای اصلی اثر انگشت

به طور کلی الگوهای اصلی اثر انگشت به سه دسته کمانی[7]، حلقه‌ای[8] و مارپیچی[9] تقسیم می‌شوند که در شکل ۳ نشان داده شده است [۷].

شکل ۳ - سه نوع الگوی اصلی اثر انگشت

توسط این الگوها می‌توان خصوصیاتی از یک اثر انگشت را دریافت نمود. خطوط اصطکاکی دارای یک سری نقاط مشخصه می باشند که به آنها مینوشیا[10] گفته می‌شود. این نقاط شامل کمانها، مارپیچها، حلقه ها، انتهای خطوط یا قطع آن، انشعاب به دو یا چند شاخه، نقطه‌ها (شیارهای نزدیک به خطوط)، جزایر (دو انشعاب نزدیک به هم)، تقاطع (نقطه تلاقی دو یا چند خط)، منفذها می باشند. در جدول ۱ انواع خصوصیات اصلی و ترکیبی مینوشیا نشان داده شده است [۸].

جدول ۱ - انواع خصوصیات اصلی و ترکیبی مینوشیا

نمونه	مینوشیا	نمونه	مینوشیا
	پل		پایان لبه
	دوشاخه دوبل		دوشاخه
	سه شاخه		نقطه
	دوشاخه مخالف		جزیره (خط کوتاه)

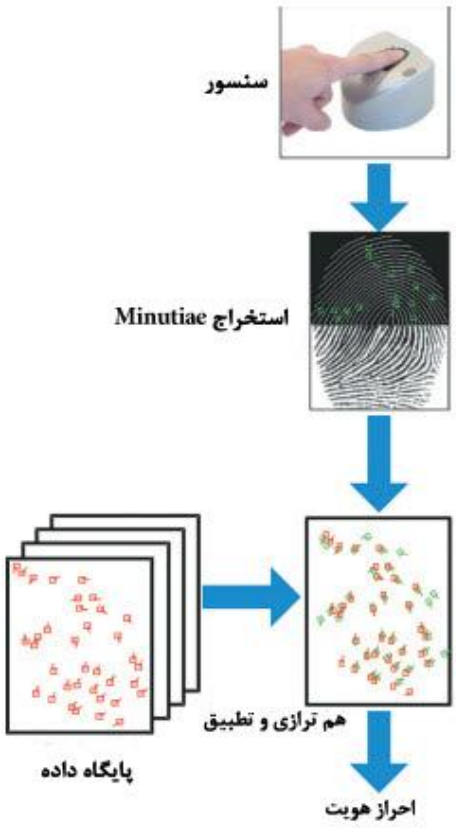
[5] Fingerprint
[6] Friction Ridge
[7] Arch
[8] Loop
[9] Whorl
[10] Minutiae

ISSN: 2745-3673
http://www.Rcsj.ir

متقاطع		دریاچه (محفظه)	
دوشاخه و پایان لبه		قلاب	

تشخیص اثر انگشت

برای استفاده از اثر انگشت از اسکنرهای مخصوصی استفاده می‌شود. بعد از اینکه انگشت روی صفحه اسکنر قرار گرفت، بسته به نرم افزار استفاده شده، اثر انگشت اسکن شده و نقاط کلیدی آن تعیین و با الگوی اولیه تطبیق داده می‌شود. البته برای کمتر کردن زمان مقایسه، ابتدا نقاطی به عنوان نقاط کلیدی برای دسته بندی اسکن های موجود استفاده می‌شود و در زمان انطباق از همین کلیدها استفاده کرده و زمان مقایسه پایین آورده می‌شود. شکل ۴ شمای کلی یک سیستم تشخیص اثر انگشت را نشان می‌دهد [۷].

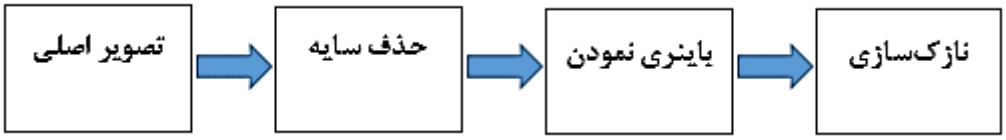


شکل ۴ - شمای کلی یک سیستم تشخیص اثر انگشت

به طور کلی، مراحل تشخیص اثر انگشت شامل دریافت تصویر اثر انگشت[۱۱] که توسط اسکنر انجام می‌پذیرد، پیش پردازش[۱۲] تصویر اثر انگشت، استخراج نقاط مینوشیا[۱۳] و تشخیص مینوشیا[۱۴] می‌باشد. پس از اسکن اثر انگشت، عمل پیش پردازش تصویر اثر انگشت انجام می‌شود که این عمل، خود در سه مرحله اجرا می شود که در شکل ۵ این مراحل نشان داده شده است [۹].

[11] Image Acquisition
[12] Pre-processing
[13] Minutiae Extractor
[14] Minutiae Recognition

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۵ - مراحل پیش پردازش تصویر اثر انگشت

پس از دریافت تصویر اصلی که همان تصویر اسکن شده اثر انگشت می‌باشد، عمل حذف سایه[۱۵] یا نویز و سپس عمل باینری کردن[۱۶] کردن[۱۶] تصویر انجام می‌گردد. در واقع، با استفاده از تصویر خاکستری که در این نوع تصویر، میزان خاکستری بودن هر پیکسل با عددی بین ۰ تا ۲۵۵ نمایش داده می شود، تصویری سیاه سفید که اصطلاحاً تصویر باینری گفته می‌شود، به دست می آید. در این روش با قرار دادن مقدار ۰ برای پیکسل‌های با مقدار خاکستری کمتر از ۱۲۸ و مقدار ۱ برای پیکسل‌های خاکستری برابر یا بیشتر از ۱۲۸، تصویر خاکستری تبدیل به تصویر سیاه سفید می شود. پس از بدست آمدن تصویر باینری، عمل نازک کردن[۱۷] لبه ها انجام می‌شود. شکل ۶ تصویر قبل و بعد از عمل پیش پردازش را نشان می‌دهد.

شکل ۶ - تصویر اثر انگشت قبل و بعد از عمل پیش پردازش
سمت چپ تصویر اصلی و سمت راست تصویر بهبود یافته می‌باشد

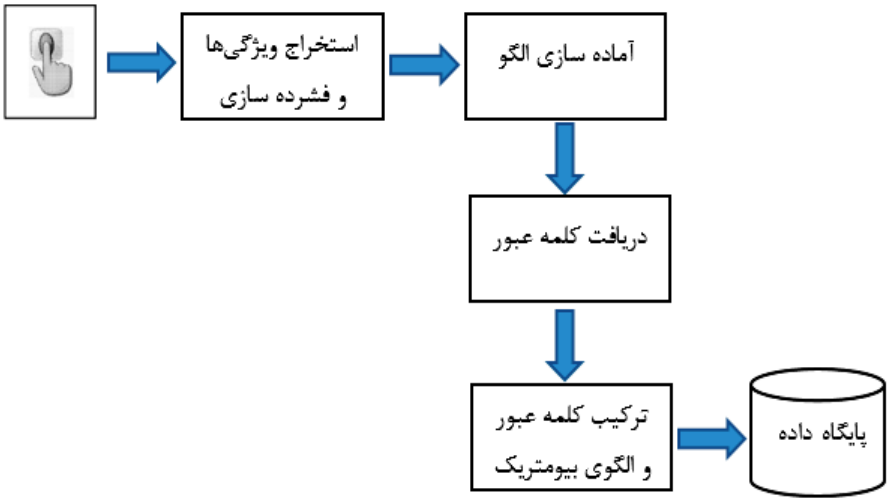
پس از اتمام مرحله پیش پردازش تصویر اثر انگشت، مرحله استخراج و تشخیص مینوشیا انجام می‌شود.

روش پیشنهادی

همان گونه که قبلاً اشاره شد، خطوط و لبه‌ها و پیچ و تاب‌های اثر انگشت هر فردی منحصربه فرد است. پس از اسکن اثر انگشت، نقاط کلیدی آن طبق الگوی تعیین شده اولیه استخراج می‌گردد. البته با توجه به اینکه زمان مقایسه بعد از بالا رفتن حجم پایگاه داده، بالا می‌رود، به جای ذخیره تصویر اسکن شده اثر انگشت، نقاط کلیدی اثر انگشت اسکن شده استخراج و به صورت یک الگوی برداری آماده می‌گردد و سپس عامل دوم که کلمه عبور می‌باشد، دریافت و جهت امنیت بیشتر با الگوی برداری ایجاد شده ترکیب شده و در پایگاه داده ذخیره می گردد. این روال در شکل ۷ نشان داده شده است.

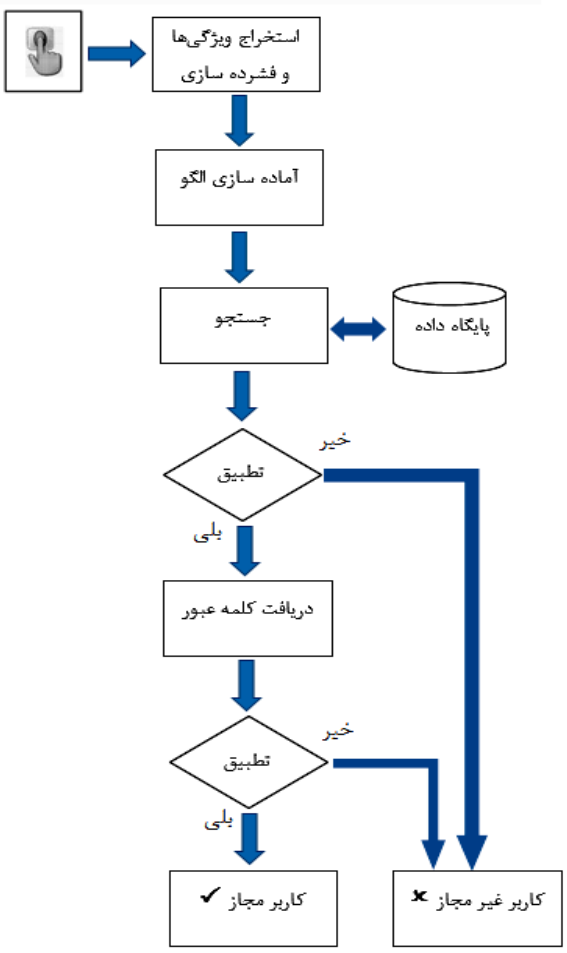
[15] Shading
[16] Binarization
[17] Thinning

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۷ - فاز ثبت اولیه اثر انگشت و کلمه عبور کاربران

در فاز احراز هویت کاربر، از همین کلیدها استفاده شده و اثر انگشت ورودی با نمونه‌های داخل پایگاه داده مقایسه می‌شود و در نهایت با بررسی کلمه عبور، مجاز یا غیر مجاز بودن کاربر مشخص شده و برای کاربر مجاز، اتصال به گره دروازه[۱۸] و دسترسی به شبکه و دستگاه‌های منشعب از گره مذکور فراهم می‌گردد. این مراحل در شکل ۸ نشان داده شده است.



شکل ۸ - فاز تایید هویت کاربر

[18] Gateway

ISSN: 2745-3673
http://www.Rcsj.ir

هنگامی که از بیومتریک برای طرح احراز هویت کاربر استفاده می‌گردد، رمزگذاری[19] استاندارد یا الگوریتم‌های هش[20] نمی‌تواند برای رمزگذاری الگوریتم بیومتریک مورد استفاده قرار گیرد. این بدین دلیل است که داده بیومتریک به عنوان مثال اسکن اثر انگشت و... با زمان و محیط تغییر می‌کند. برای حل این مشکل، استفاده از هش ادراکی[21] پیشنهاد شده است [۱۰]. هش به محاسبه یک مقدار خلاصه از یک داده ورودی اشاره می‌کند. مقدار خلاصه، یک رشته دودویی[22] کوتاه است که به عنوان مقدار هش در نظر گرفته می‌شود. روش هش ادارکی، یک مقدار هش وابسته به محتوای چند رسانه‌ای تولید می‌کند و مقدار آن نمایشگر فشرده‌ای از بیومتریک اصلی می‌باشد.

همان طور که قبلاً اشاره شد، خصوصیات کلیدی اثر انگشت (مینوشیا) از جمله خطوط، لبه‌ها، پیچ و تاب‌ها، دوشاخه‌ای بودن و ... برای هر فرد منحصربه فرد می‌باشد. در این پژوهش، از رشته‌ای از اعداد صفر و یک به طول ۱۶ به عنوان مجموعه داده[23] که بصورت تصادفی ایجاد شده است و حاوی خصوصیات کلیدی اثر انگشت‌های فرضی می‌باشد، استفاده می‌گردد. مقدار صفر بیانگر عدم وجود مشخصه‌ای خاص از اثر انگشت و مقدار یک بیانگر وجود آن خصیصه می‌باشد.

پس از ایجاد الگوی بیومتریک، جهت امنیت بیشتر، کلمه عبور کاربر را با الگوی ایجاد شده ترکیب می‌نماییم بطوری که پس از ذخیره در پایگاه داده، به آسانی قابل تشخیص نباشد. برای این منظور، پس از تبدیل کد اسکی[24] کاراکترهای کلمه عبور به رشته باینری و با اعمال عملگر XOR[25] بیتی بر روی تک تک حروف کلمه عبور با استفاده از یک کلید دلخواه، کلمه عبور رمزنگاری می‌گردد. برای رمزگشایی رشته رمزنگاری شده و به حالت اولیه برگرداندن آن، مجدداً عملگر XOR را با همان کلیدی که در هنگام رمزنگاری مورد استفاده قرار گرفته، بر روی رشته رمزشده اعمال می‌نماییم. به دلیل استفاده از ترکیب عامل بیومتریک و عملگر XOR، روش پیشنهادی را Bio-Xor می‌نامیم.

برای مثال، برای رمزنگاری واژه «Farsi»، کد اسکی باینری شده آن را با کلمه کلید "۱۰۱۱۱۰۰۱" XOR می‌نماییم. این روال در جدول ۲ نشان داده شده است.

جدول ۲ - رمزنگاری کلمه عبور کاربر

کلمه عبور ورودی	i	s	r	a	F
کد اسکی کلمه عبور	105	115	114	97	70
کد اسکی باینری شده حروف کلمه عبور	01101001	01110011	01110010	01100001	01000110
کلید مورد نظر	10111001	10111001	10111001	10111001	10111001
رشته XOR شده حاصل	11010000	11001010	11001011	11011000	11111111

برای رمزگشایی[26]، نتیجه‌ای که از مرحله رمزنگاری بدست آمده، مجدداً با عبارت کلید XOR می‌گردد که در شکل ۹ نشان داده شده است.

11111111 11011000 11001011 11001010 11010000

10111001 10111001 10111001 10111001 10111001

01000110 01100001 01110010 01110011 01101001

شکل ۹- رمزگشایی کلمه عبور کاربر

بار دیگر جهت امنیت بیشتر، قبل از تبدیل کلمه عبور به رشته باینری، موقعیت مکانی حروف کلمه عبور را به صورت جدول ۳ جابجا می نماییم بطوری که پس از ذخیره در پایگاه داده، به آسانی قابل تشخیص نباشد.

---

[19] Encryption
[20] Hash Algorithms
[21] Perceptual Hashing
[22] Binary
[23] Data Set
[24] ASCII: American Standard Code for Information Interchange
[25] Exclusive Or
[26] Decryption

ISSN: 2745-3673
http://www.Rcsj.ir

جدول ۳ - جابجایی موقعیت مکانی حروف کلمه عبور

موقعیت حروف کلمه عبور دریافت شده از کاربر	۶	۵	۴	۳	۲	۱
موقعیت ذخیره حروف کلمه عبور در پایگاه داده	۳	۶	۱	۲	۴	۵

طول کلمه عبور ۶ کاراکتر می‌باشد که پس از تبدیل کد اسکی آن به رشته باینری، طول آن ۴۸ بیت می‌شود. در نهایت الگوی رشته باینری (با طول ۶۴ بیت) که در پایگاه داده ذخیره می‌گردد، بصورت شکل ۱۰ می‌باشد.

رشته باینری کلمه عبور XOR شده (به طول ۴۸ بیت)	رشته باینری الگوی بیومتریک (به طول ۱۶ بیت)

شکل ۱۰ - الگوی ذخیره رشته باینری در پایگاه داده

معیارهای سنجش

برای سنجش امنیت یک سیستم ایمن، چندین معیار وجود دارد که قدرت سیستم ایمن را در مقابل حملات مختلف مشخص می‌کند. در این پژوهش، از معیار تست اثر بهمنی اکید[۲۷] استفاده گردیده است و برای سنجش میزان مصرف انرژی، مدت زمان اجرای پروسه احراز هویت اندازه گیری شده است و سپس روش پیشنهادی با این معیارها سنجیده می‌شود و نتایج حاصل از این معیارها با روش‌های رمز نگاری DES[۲۸]، RSA[۲۹] و ECC[۳۰] مقایسه گردیده است.

تست اثر بهمنی اکید

این ویژگی که اولین بار توسط وبستر[۳۱] و تاوارس[۳۲] ارائه شد، به گونه‌ای است که هر کدام از بیت‌های خروجی به ازای تغییر در یک بیت از ورودی، باید با احتمال $\frac{1}{2}$ تغییر کنند [۱۱]. این بدان معناست که بیتهای خروجی باید به یک شکل بسیار پیچیده به بیتهای ورودی وابسته باشند. در یک رمزنگاری، اگر یک بیت از متن رمز نشده ورودی تغییر داده شود، متن رمزشده خروجی باید به صورت کامل و به یک شکل غیرقابل پیش‌بینی یا شبه تصادفی تغییر کند. یعنی اگر بیت ***i*** ام تغییر داده شود، احتمال اینکه بیت خروجی ***j*** ام تغییر کند باید برابر ٪۵۰ باشد. به صورت کلی تر، تغییر یک مجموعهء ثابت از بیت‌ها باعث تغییر هر بیت خروجی با احتمال ٪۵۰ شود.

این معیار معمولاً با استفاده از ماتریس وابستگی[۳۳] سنجیده می‌شود. در صورتی که هر المان از این ماتریس و مقدار میانگین آن به مقدار ایده آل ۰/۵ نزدیک باشد، الگوریتم دارای ویژگی بهمنی اکید می‌باشد. برای محاسبه این ماتریس، مقدار ورودی ۸ بیتی ***(x)*** را به ورودی الگوریتم داده و خروجی معادل آن ***(y)*** را دریافت می‌کنیم. سپس بیت ***j*** از ورودی را تغییر داده ***(xj)*** و خروجی آن را دریافت می‌کنیم ***(yj)*** به طوری که ***xj*** و ***x*** تنها در بیت ***j*** باهم تفاوت دارند. سپس بردار ***vj*** را به صورت $v_j = y \oplus y_j$ محاسبه می‌کنیم. مقدار بیت ***i*** در بردار ***vj*** به المان ***(i,j)*** از ماتریس وابستگی ***(ai,j)*** که یک ماتریس ۸×۸ می‌باشد اضافه می‌شود [۱۱].

این عملیات را به ازای تمام ۸ بیت از تعداد ۱۰۰ ورودی تصادفی انجام داده و در نهایت هر المان موجود در ماتریس به ۱۰۰ تقسیم می‌شود. مقدار المان ***ai,j*** میزان ارتباط میان بیت ***j*** از ورودی و بیت ***i*** از خروجی را نشان می‌دهد. در صورتی‌که مقدار تمام المان‌های این ماتریس نزدیک به ۰/۵ باشند معیار تست بهمنی اکید برقرار است. یعنی اکیداً تاکید می‌گردد که اگر در همه بیت ها تغییر ایجاد شود، الگوریتم جواب خوبی دارد و به این نتیجه می‌رسیم که باید بهترین حالت را جواب دهد.

ماتریس وابستگی روش‌های تست شده و مقادیر میانگین آنها برای کلید رمز زیر و تعداد ۱۰۰ نمونه ایجاد شده است.

کلید رمز مورد استفاده: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F""

[27] Strict Avalanche Criterion (SAC)
[28] Data Encryption Standard
[29] Rivest–Shamir–Adleman
[30] Elliptic Curve Cryptography
[31] Webster
[32] Tavares
[33] Dependence Matrix

ISSN: 2745-3673
http://www.Rcsj.ir

ماتریس وابستگی و نتیجه اثر بهمنی اکید برای روش DES در جدول ۴، برای روش RSA در جدول ۵، برای روش ECC در جدول ۶ و برای روش پیشنهادی در جدول ۷ نشان داده شده است.

جدول ۴ - ماتریس وابستگی و اثر بهمنی اکید برای روش DES

ورودی‌ها / خروجی‌ها	x1	x2	x3	x4	x5	x6	x7	x8
y1	0.49	0.54	0.46	0.41	0.52	0.52	0.52	0.45
y2	0.45	0.49	0.55	0.48	0.51	0.47	0.55	0.48
y3	0.57	0.48	0.42	0.50	0.57	0.48	0.61	0.46
y4	0.50	0.57	0.51	0.40	0.46	0.33	0.54	0.43
y5	0.52	0.56	0.45	0.55	0.46	0.50	0.49	0.54
y6	0.50	0.59	0.49	0.47	0.52	0.58	0.55	0.50
y7	0.47	0.47	0.52	0.54	0.49	0.46	0.53	0.47
y8	0.52	0.49	0.49	0.48	0.50	0.45	0.47	0.47
میانگین	**0.4945**							

جدول ۵ - ماتریس وابستگی و اثر بهمنی اکید برای روش RSA

ورودی‌ها / خروجی‌ها	x1	x2	x3	x4	x5	x6	x7	x8
y1	0.36	0.38	0.35	0.40	0.36	0.35	0.32	0.32
y2	0.31	0.33	0.35	0.36	0.36	0.36	0.37	0.39
y3	0.32	0.39	0.34	0.32	0.34	0.33	0.39	0.38
y4	0.34	0.38	0.35	0.38	0.38	0.35	0.30	0.39
y5	0.34	0.37	0.38	0.38	0.40	0.34	0.37	0.38
y6	0.32	0.31	0.37	0.36	0.35	0.33	0.33	0.36
y7	0.32	0.39	0.33	0.35	0.30	0.33	0.33	0.32
y8	0.34	0.32	0.36	0.33	0.36	0.37	0.38	0.36
میانگین	**0.3522**							

جدول ۶ - ماتریس وابستگی و اثر بهمنی اکید برای روش ECC

ورودی‌ها / خروجی‌ها	x1	x2	x3	x4	x5	x6	x7	x8
y1	0.23	0.27	0.21	0.24	0.21	0.24	0.20	0.25
y2	0.25	0.27	0.19	0.19	0.22	0.25	0.22	0.27
y3	0.25	0.23	0.20	0.20	0.29	0.30	0.22	0.18
y4	0.25	0.24	0.25	0.25	0.20	0.29	0.19	0.29
y5	0.26	0.22	0.25	0.28	0.24	0.26	0.29	0.29
y6	0.24	0.21	0.24	0.20	0.22	0.27	0.30	0.28
y7	0.22	0.29	0.20	0.20	0.19	0.19	0.27	0.22
y8	0.29	0.20	0.22	0.29	0.25	0.26	0.26	0.30
میانگین	**0.2417**							

جدول ۷ - ماتریس وابستگی و اثر بهمنی اکید برای روش پیشنهادی

ورودی‌ها / خروجی‌ها	x1	x2	x3	x4	x5	x6	x7	x8
y1	0.43	0.43	0.42	0.45	0.41	0.43	0.40	0.40

ISSN: 2745-3673
http://www.Rcsj.ir

y2	0.38	0.38	0.40	0.41	0.39	0.45	0.43	0.41
y3	0.40	0.45	0.45	0.42	0.41	0.40	0.42	0.41
y4	0.40	0.41	0.40	0.43	0.42	0.41	0.38	0.44
y5	0.38	0.41	0.44	0.43	0.44	0.41	0.44	0.40
y6	0.40	0.41	0.40	0.42	0.41	0.40	0.44	0.45
y7	0.39	0.45	0.43	0.40	0.38	0.41	0.40	0.39
y8	0.38	0.43	0.45	0.44	0.38	0.41	0.43	0.42
میانگین	**0.4148**							

نتیجه جمعی تست اثر بهمنی اکید برای روش‌های مورد بررسی در جدول ۸ نشان داده شده است.

جدول ۸ - نتیجه جمعی تست اثر بهمنی اکید برای روش‌های مورد بررسی

روش رمزنگاری	نتیجه تست بهمنی اکید	تفاوت با مقدار ایده آل
روش DES	0.4945	0.0055
روش RSA	0.3522	0.1478
روش ECC	0.2417	0.2583
روش پیشنهادی	0.4148	0.0859

با توجه به نتایج تست اثر بهمنی اکید در جدول ۸، مشاهده می‌شود روش رمزنگاری DES در رتبه اول و دارای بیشترین اثر بهمنی اکید، روش پیشنهادی در رتبه دوم، روش RSA در رتبه سوم و روش ECC در رتبه چهارم، دارای کمترین اثر بهمنی می‌باشد و روش پیشنهادی با مقدار میانگین ۰/۴۱۴۸ و تفاوت ۰/۰۸۵۹ دارای نتیجه قابل قبولی بوده و نزدیک به مقدار ایده آل ۰/۵ می‌باشد و مقدار میانگین برای روش رمزنگاری ECC در این تست از نتیجه مناسبی برخوردار نبوده و چندان قابل اعتماد نمی‌باشد.

مقایسه مدت زمان اجرا

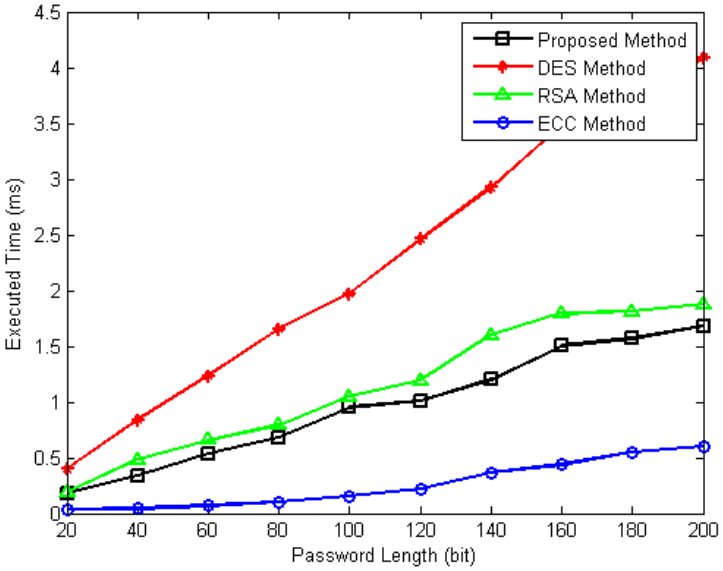
در نمودار ۱ مدت زمان اجرای پروسه احراز هویت روش پیشنهادی با روش‌های رمزگذاری که مورد مقایسه قرار گرفته است، نشان داده شده است. همان‌گونه که مشاهده می‌شود با افزایش طول کلمه عبور، مدت زمان اجرای الگوریتم برای همه روش‌ها افزایش می‌یابد و روش رمزنگاری DES در رتبه اول و بیشترین مدت زمان، روش RSA در رتبه دوم، روش پیشنهادی در رتبه سوم و روش ECC در رتبه چهارم، کمترین مدت زمان اجرا را به خود اختصاص دادند.

مدت زمان صرف شده روش پیشنهادی، کمتر از روش‌های DES و RSA می‌باشد که همین امر باعث مصرف کمتر انرژی و افزایش عمر گره‌های شبکه حسگر بی‌سیم برای استفاده در محیط‌های اینترنت اشیاء می‌گردد و مدت زمان صرف شده در روش ECC از روش پیشنهادی کمتر است که دلیل این امر، کاهش محسوس طول کلید در الگوریتم‌های مبتنی بر رمزنگاری ECC نسبت به سیستم‌های مشابه منجمله RSA می‌باشد و به همین دلیل، سرعت عملیات محاسباتی آن بالا می‌باشد ولی همان گونه که از نتیجه تست بهمنی اکید پیداست، از امنیت مطلوبی برخودار نمی‌باشد. مشخصات پردازنده و حافظه سیستم مورد استفاده در جدول ۹ نشان داده شده است.

جدول ۹ - مشخصات پردازنده و حافظه سیستم مورد استفاده

Processor	Intel® Core™ i3-4130 @ 3.40GHz Cores#: 2, Threads#: 4 L3 Cache Size: 3 MB
Memory (RAM)	8.00 GB DDR3 (PC3-12800)

ISSN: 2745-3673
http://www.Rcsj.ir



نمودار ۱ – مقایسه مدت زمان اجرای روش پیشنهادی با روشهای رمز گذاری

ISSN: 2745-3673
http://www.Rcsj.ir

جمع‌بندی و پیشنهاد

هدف از این پژوهش بالا بردن امنیت حریم خصوصی اینترنت اشیاء بوسیله احراز هویت چندعاملی کاربر با لحاظ نمودن سبک بودن حجم پردازش، حافظه مصرفی و مصرف انرژی بوده و به دلیل اهمیت مصرف انرژی در محیط اینترنت اشیاء، از میان روشهای رمزنگاری مختلف، از XOR و ترکیب داده بیومتریک با کلمه عبور رمزنگاری شده استفاده گردید تا رسیدن به هدف مورد نظر میسر گردد.

جهت مقایسه با روش پیشنهادی، روشهای رمزنگاری DES، RSA و ECC پیاده سازی گردید و جهت سنجش امنیت از معیار تست اثر بهمنی اکید استفاده گردید و نتایج تست نشان داد که روش‌های رمز نگاری DES، RSA و روش پیشنهادی دارای اثر بهمنی خوبی بوده و روش رمزنگاری ECC دارای کمترین اثر بهمنی می‌باشد که چندان قابل اعتماد نمی‌باشد.

مقایسه مدت زمان اجرای پروسه احراز هویت نشان داد که روش رمزنگاری DES در رتبه اول و بیشترین مدت زمان، روش RSA در رتبه دوم، روش پیشنهادی در رتبه سوم و روش ECC در رتبه چهارم کمترین مدت زمان اجرا را به خود اختصاص دادند.

دلیل پایین بودن مدت زمان صرف شده در روش ECC این است که در این روش، طول کلید بطور محسوسی نسبت به سیستم‌های مشابه منجمله RSA کاهش داده شده و به همین دلیل، سرعت عملیات محاسباتی آن بالا می‌باشد و این ویژگی، این الگوریتم را برای دستگاههای با اندازه کوچک و با توانایی‌های محاسباتی، حافظه و پهنای باند محدود، بسیار مناسب نموده است، ولی همان گونه که از نتیجه تست بهمنی اکید پیداست، از امنیت مطلوبی برخودار نمی‌باشد.

روش پیشنهادی از نظر رمزنگاری با تست های امنیتی انجام شده نتیجه ایده آلی داشته و نسبت به روش‌های مورد مقایسه با در نظر گرفتن فاکتور امنیت، مدت زمان اجرای پایینی دارد که همین امر باعث مصرف کمتر انرژی و افزایش عمر گره‌های شبکه حسگر بی‌سیم برای استفاده در محیط های اینترنت اشیاء می‌گردد.

جهت ادامه پژوهش موارد ذیل پیشنهاد می‌گردد:

- استفاده از توابع درهم ساز (هش) ساده برای امنیت کلمه عبور.
- ترکیب روش رمزنگاری ECC به دلیل سرعت اجرای آن با XOR.
- استفاده از دو عامل بیومتریک بعنوان مثال دریافت اثر دو انگشت دست.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Tsai, C., Lai, C., Vasilakos, V. (2014), "Future internet of things: Open issues and challenges", ACM/Springer Wireless Networks, doi: 10.1007/s11276-014-0731-0.

[2] Madakam, S., Date, H. (2016), "Security Mechanisms for Connectivity of Smart Devices in the Internet of Things", Springer Computer Communications and Networks (CCN), pp. 23-41, doi: 10.1007/978-3-319-33124-9_2.

[3] Choi, Y., Nam, J., Lee, D., Kim, J., Jung, J., Won, D. (2014), "Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics", Sci World J, doi: 10.1155/2014/281305.

[4] Chang, CC., Lin, IC. (2004), "Remarks on fingerprint-based remote user authentication scheme using smart cards", ACM SIGOPS Oper Syst Rev, 38:4, pp. 91–96, doi: 10.1145/1031154.1031165.

[5] Jain, A.K., Ross, A., Prabhakar, S. (2004), "An introduction to biometric recognition", Transactions on Circuits and Systems for Video Technology, IEEE, vol. 14, no. 1, pp. 4–20.

[6] Kuo WC, Wei HJ, Chen YH, Cheng JC. (2015), "An enhanced secure anonymous authentication scheme based on smart cards and biometrics for multi-server environments", Information security (AsiaJCIS), 10th Asia joint conference, IEEE, pp. 1–5, doi: 10.1109/AsiaJCIS.2015.11.

[7] Jain, A.K., Feng, J., Nandakumar, K. (2010), "Fingerprint Matching", IEEE Computer Society, 43(2), pp. 36-44, doi: 10.1109/MC.2010.38

[8] "Fingerprint Ridge Characteristics Images", http://navalwiki.info/fingerprint-ridge-characteristics.asp, Accessed June 9, 2018

[9] Arantes, M., Ide, A. N., Saito, J. H. (2002), "A system for fingerprint minutiae classification and recognition", 9th International Conference on Neural Information Processing, ICONIP '02', doi: 10.1109/iconip.2002.1201939.

[10] Niu, X.M., Jiao, YH. (2008), "An overview of perceptual hashing", Acta Electron Sinica, 36:7, pp. 1405–11.

[11] Webster, A. F., Tavares, S. E. (1986), "On the design of S-boxes", In: Williams, H. C. (ed.), Advances in Cryptology (CRYPTO ’85 Proceedings), Springer Berlin Heidelberg, Vol. 218, pp. 523-534.