ارائه یک طرح احراز هویت امن با هدف حفظ حریم خصوصی در سیستم خانه هوشمند

فاطمه حمیدی فشکی[۱]، مجید بیات*[۲]، مهدی رمضان علاقه بند[۳]، آناهید محسنی کبیر[۴].

۱- دانشجوی کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران.

۲- استادیار، دانشکده مهندسی کامپیوتر، دانشگاه شاهد.

۳-استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد یادگار امام خمینی.

۴-دانشجوی کارشناسی ارشد، دانشکده مهندسی برق و کامپیوتر، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران.

چکیده

امروزه فنّاوری جدید اینترنت اشیاء توانسته است با اتصال جهان فیزیکی و دنیای دیجیتال با یکدیگر و مرتبط ساختن اشیاء با اشیاء و اشیاء با انسان، تغییرات اساسی در زندگی ما انسان‌ها ایجاد نماید. در این میان می‌توان به یکی از محبوب‌ترین کاربردهای اینترنت اشیاء یعنی فناوری سیستم خانه هوشمند اشاره نمود. به عبارتی با هوشمند نمودن لوازم و وسایل خانه و ساختمان علاوه بر کنترل میزان مصرف و صرفه‌جویی در انرژی‌ها و همچنین راحت‌تر انجام شدن امور، کاربران قادر خواهند بود تا از راه دور مدیریت و کنترل را انجام دهند؛ اما این فناوری نیز در کنار تمام مزیت‌ها دارای چالش‌های فراوانی می‌باشد، از جمله مهم‌ترین نگرانی در این حوزه به خطر افتادن شناسه و الگوی رفتاری کاربران این فناوری می‌باشد. به همین دلیل در این مقاله ابتدا یک طرح احراز هویت با هدف امنیت و حفظ حریم خصوصی برای حوزه‌ی خانه هوشمند که اخیراً ارائه شده است مورد بررسی قرار داده و سپس ضعف‌های امنیتی آن را بیان می‌کنیم، در ادامه یک طرح احراز اصالت بهبود یافته به‌منظور رفع ایرادات امنیتی طرح مذکور ارائه می‌دهیم، که طرح پیشنهادی همه‌ی ویژگی‌های امنیتی لازم برای طرح احراز اصالت سیستم خانه هوشمند را دارا می‌باشد. همچنین طرح پیشنهادی را از لحاظ امنیت و کارایی با طرح‌های مشابه مقایسه می‌کنیم. بر اساس تحلیل امنیتی ارائه شده و مقایسه با طرح‌های مرتبط، طرح پیشنهادی ما یک طرح احراز اصالت امن و مناسب برای خانه هوشمند می‌باشد. روش مورد استفاده ما در این طرح روش رمزنگاری مبتنی بر خم بیضوی[۳](ECC) و نگاشت دوخطی می‌باشد، و بدین ترتیب جلوی حملات و دسترسی‌های غیرقانونی نیز به داده‌های دستگاه‌های هوشمند درون خانه گرفته خواهد شد. در انتها نیز با استفاده از Ban logic به اثبات امنیتی این طرح خواهیم پرداخت.

کلمات کلیدی: اینترنت اشیاء، خانه هوشمند، حریم خصوصی، احرازهویت،خم بیضوی، نگاشت دوخطی.

[۱] **Email: fatemeh.hamidi@srbiau.ac.ir**
* **Corresponding author: mbayat@shahet.ac.ir**
[۳] Elliptic curve

۲.مقدمه

اینترنت اشیاء در حقیقت یک فناوری جدیدی می‌باشد که قادر است، دستگاه‌ها را از طریق شناسه‌شان و یا از روش‌های دیگر از طریق اینترنت با یکدیگر مرتبط سازد. دامنه‌ی کاربردی اینترنت اشیاء بسیار گسترده است و شامل خانه-ساختمان هوشمند، شهر هوشمند، دستگاه‌های پوشیدنی، سلامت الکترونیکی می‌باشد[۱].به‌مرورزمان و در سال‌های آتی ده‌ها و یا حتی صدها میلیارد دستگاه قادر خواهند بود تا به یکدیگر متصل گردند،که این دستگاه‌ها باید قابلیت هوشمند سازی جهت دریافت و بررسی و یا حتی تصمیم‌گیری بدون ایفای نقش انسان را داشته باشند[۲].این فناوری هرروزه باعث ایجاد تغییراتی در ساختار زندگی بشر می‌شود و استانداردهای زندگی را تغییر می‌دهد[۳].

فناوری سیستم خانه هوشمند تعریف شده است از کنترل و مشاهده‌ی وسایل خانه از جمله وسایل نور و روشنایی، دما، تهویه هوا، کنترل و باز و بسته شدن درها و پنجره‌ها[۴]. فنّاوری خانه‌ی هوشمند یکی از محبوب‌ترین خدمات اینترنت اشیاء می‌باشد که به‌طور چشمگیری در سال‌های اخیر با وعده‌های زیادی جهت بهبود کیفیت زندگی انسان‌ها مورد توجه قرار گرفت[۵].در حقیقت هریک از وسایل خانه را جهت بهبود عملکرد توسط قطعاتی، هوشمند نموده و توسط گوشی‌های هوشمند و یا میکروکنترلرها،کنترل می‌نمایند. از طرفی جهت بهبود بهره‌وری و تبادل اطلاعات،دسترسی آسان در مکان‌های مختلف،در صورتی که دستگاه‌ها فضای ذخیره‌سازی کافی و قدرت محاسبات زیادی نداشته باشند،جهت بهبود عملکرد به فضاهای ابری روی آورده می‌شود[۶].

حریم خصوصی را می‌توان میزان حقی که هر فرد یا گروهی جهت نظارت بر اطلاعات شخصی و یا حق پنهان کردن حقایق زندگی‌شان به دیگران می‌دهند، تعریف نمود.

ازآنجایی که اینترنت اشیاء از انواع مختلف و ناهمگون فناوری‌های متفاوت و دستگاه‌های گوناگون ساخته شده است، در این میان الزامات امنیتی و حریم خصوصی بسیار پراهمیت می‌باشد. در حقیقت اعتماد کامل طرفین از محرمانه ماندن اطلاعات، تأیید اعتبار، احراز هویت افراد قانونی، گمنام ماندن شناسه افراد از مهاجمان و کنترل و دسترسی را شامل می‌شود[۷].در حقیقت همین موضوع دسترسی به داده‌ها در هر زمان و هر مکان باعث گردیده است،تا حریم خصوصی افراد توسط عوامل سودجو در خطر قرار گیرد.چراکه ممکن است اطلاعات حساس شخصی و خصوصی کاربران با چالش روبرو شود[۸].از طرفی هیچ فردی مایل به این نیست که از طریق دنبال کردن رفتار و عادات شخصی و روزانه‌اش توسط مهاجمان و یا هکرها ردیابی گردد،درنتیجه محرمانه ماندن اطلاعات که از طریق رمز کردن داده‌ها و گمنامی و عدم ردیابی کاربر که از روش‌های حفظ حریم خصوصی است،مطرح می‌شود[۹].و اما مسئله چگونگی دستیابی به حفاظت از حریم خصوصی امری بسیار مهم است که با توجه به ویژگی‌های منحصربه‌فرد و الزامات اینترنت اشیاء از جمله،منابع محاسباتی محدود،قدرت پردازندگی،پهنای باند، و تعداد بسیار بالای اشیاء مستقر در شبکه و می‌بایست فن‌ها و استراتژی‌های جدید و کاربردی جهت امنیت در اینترنت اشیاء بیان نمود،که در این میان می‌توان به استفاده از طرح‌های سبک‌وزن مانند احراز هویت مبتنی بر شناسه برای حفظ حریم خصوصی اشاره کرد[۱۰]. در ادامه در فصل دوم مروری برکارهای پیشین انجام شده بر روی مبحث احراز هویت امن برای خانه هوشمند خواهیم داشت.ادامه این مقاله بدین صورت سازماندهی شده است : در فصل سوم این مقاله مروری بر روی طرح شوآی و همکاران خواهیم داشت و آنرا از لحاظ امنیت بررسی خواهیم نمود و حملات وارد بر این طرح را بیان می نماییم.فصل چهارم را به بررسی طرح خودمان اختصاص می‌دهیم و آنرا بررسی امنیتی نموده و در نهایت یک جدول مقایسه از لحاظ محاسباتی،مخابراتی و امنیتی با سایر روش‌ها خواهیم داشت.در فصل پنجم نیز به اثبات امنیتی طرح با BAN logic خواهیم پرداخت.

۳.پیشینه‌ی طرح

در سال‌های اخیر طرح‌های احراز هویت متفاوتی در حوزه‌ی خانه‌های هوشمند مطرح گردیده است، که هریک دارای نقاط ضعف و قدرتی بوده‌اند، و بلافاصله بعد از آن‌ها طرح‌هایی جهت رفع نواقص آن‌ها ایجاد گردیده‌اند، اما بااین‌وجود همچنان چالش بر سر یک طرح احراز هویتی که تمامی ملزومات امنیتی را شامل باشد، ادامه دارد.

در سال ۲۰۰۵ طرح احراز هویتی توسط انلی و چن[۱۱] ارائه شد،که این طرح با استفاده از کارت هوشمند و رمز عبور، اصالت افراد را بررسی می‌نمود.در سال ۲۰۰۶ طرح دیگری توسط یو و جونگ [۱۲] ارائه شد که راهکارهایی جهت بهبود امنیتی مقاله [۱۱] ارائه نمودند .اما دیری نپایید که در سال ۲۰۰۸ توسط جئونگ و همکارانش [۱۳] به مقالات ,[۱۱] [۱۲] حمله‌ی سرقت کارت هوشمند را وارد نمودند،و درنتیجه آن‌ها طرح احراز هویتی پیشنهاد نمودند که مبتنی بر استفاده از رمزهای یک‌بارمصرف بودند.هرچند در این مقاله ادعایی مبنی بر احراز هویت چندگانه و گمنامی اظهار گردیده بود اما،مشخص گردید که احراز هویتی بین درگاه(GWN)[1]و دستگاه هوشمند موجود نیست و همچنین مشخصات کاربر به‌صورت آشکار بر روی کانال عمومی ارسال می‌گردید،که داشتن گمنامی را نقض می‌نمود.از طرفی حمله‌ی داخلی و حمله سرقت کارت هوشمند نیز بر روی آن اتفاق می‌افتاد.در سال ۲۰۱۱ توسط ویدا و همکارانش در[۱٤] طرحی مبتنی بر محاسبات سبک برای احراز هویت با استفاده از تابع چکیده ساز ارائه گردید.آن‌ها ادعا می‌کردند که طرحشان تمامی الزامات امنیتی را دارا می‌باشد و در مقابل حملات مقاوم است، اما چندی نگذشت توسط کیم و همکارش در [۱۵] حملاتی بر آن وارد گردید، از جمله حمله‌ی حدس رمز عبور،نداشتن امنیت پیشرو،و نداشتن گمنامی. ویدا و همکارانش در [۱٦] احراز هویتی مبتنی بر رمزنگاری بر روی خم بیضوی(ECC) پیشنهاد نمودند،اما متأسفانه این طرح نیز در مقابل حمله‌ی جعل کاربر و حدس رمز عبور مقاوم نبود.در سال ۲۰۱۵ کومار [۱۷] نیز یک احراز هویتی سبک برای سیستم خانه هوشمند و ایجاد یک کلید نشست مشترک بین سه نهاد کاربر،درگاه و دستگاه هوشمند ارائه نمود که احراز اصالت بین درگاه و دستگاه هوشمند از طریق یک توکن اتفاق می‌افتاد.اما این طرح نیز از گمنامی و عدم ردیابی حمایت نمی‌کرد. در سال ۲۰۱۷ توسط وازید و همکارانش [۱۸] ایجاد گردید، هرچند که طرح از احراز هویت چندگانه حمایت می‌نمود،اما درنهایت مشخص گردید که طرح ،حمله‌ی داخلی می‌خورد و یک کاربر داخلی ممکن است بتواند به مرحله‌ی ثبت‌نام دسترسی یافته و از آن طریق بتواند حملاتی برای دستیابی به کلید نشست انجام دهد. در این میان طرح‌های دیگری نیز ارائه گردید که هرکدام دارای یکسری مسائل و مشکلات امنیتی و حریم خصوصی بودند. درنهایت در سال ۲۰۱۹ شوآی و همکارانش[۱۹]طرحی ارائه نمودند که با توجه به ادعای نویسندگان که مبتنی بر سبک بودن طرح و پوشش تمام الزامات امنیتی، اما با بررسی‌هایی که بر روی طرح انجام گردید مشخص شد که این طرح نیز دارای مشکلات امنیتی از جمله نداشتن امنیت پیشرو،حمله‌ی سرقت دستگاه هوشمند و دستیابی مهاجم به کلید نشست و همچنین حمله‌ی انکار خدمات است. ازآنجایی‌که ایده‌ی کلی چهارچوب طرح جدید ارائه شده مبتنی بر طرح شوآی و همکارانش[۱۹] است پس ابتداً به معرفی آن خواهیم پرداخت.

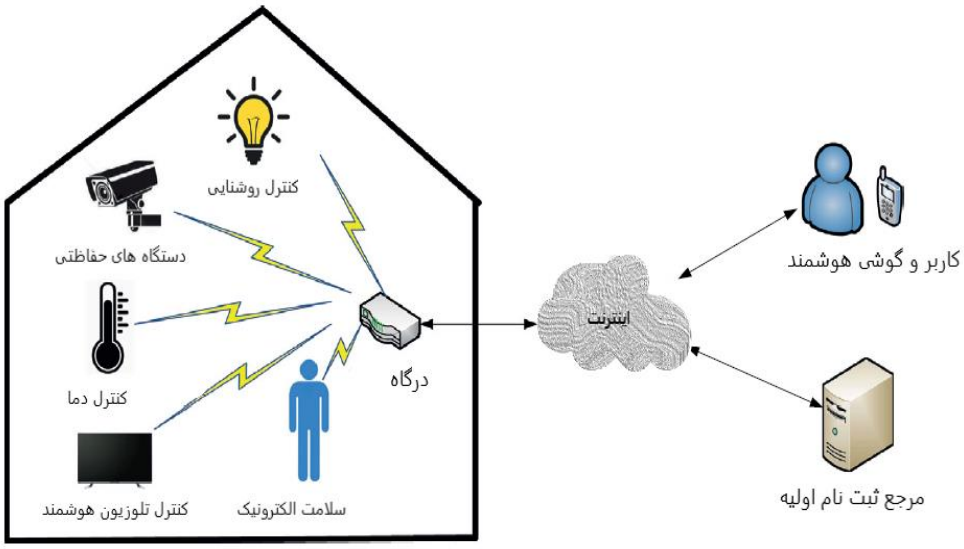
۳.مروری بر طرح احراز هویت [۱۹]

در این بخش قصد داریم تا مروری بر طرح احراز هویت خانه‌های هوشمند شوآی و همکاران [۱۹] انجام دهیم. این طرح جهت برقراری ارتباط امن گمنام در محیط ناامن کانال عمومی بین کاربر و دستگاه‌های هوشمند اتفاق می‌افتد. این طرح شامل سه نهاد می‌باشد.۱- کاربر (U)که همان استفاده‌کننده از فنّاوری می‌باشد که با استفاده از یک گوشی هوشمند ارتباط برقرار می‌نماید.۲- درگاه یا پل ارتباطی (GWN)، که در این طرح نقش واسط ارتباطی مورد اطمینان و درستکار را

[1] Gateway

دارد؛ و ۳- دستگاه هوشمند که می‌تواند هر یک از لوازم خانه باشد.همچنین لازم به ذکر است که این طرح دارای یک نهاد ثبت‌نام کننده[۱] به نام (RA) می‌باشد، که البته این نهاد به‌صورت غیرفعال حضور دارد و تنها در زمان ثبت‌نام فعال است؛ و پس از آن با انتقال کلیدهای خصوصی خود و کلید خصوصی سیستم به درگاه از ارتباط خارج می‌گردد. در این طرح ادعا می‌گردد، با توجه به عدم ذخیره جدول تأیید توسط درگاه، که به‌عنوان واسط ارتباطی، بین کاربر و دستگاه‌های هوشمند واقع شده است و همچنین استفاده از رمزنگاری مبتنی بر خم بیضوی جلوی بسیاری از حملات گرفته خواهد شد.در شکل۱نمایی از ساختار کلی خانه‌های هوشمند را مشاهده می‌نماییم.

طرح شوآی و همکاران دارای پنج فاز می‌باشد: فاز مقدماتی اولیه،ثبت نام(صدور کارت)،ورود و احراز هویت،تغییر کلمه عبور.که در ادامه به بررسی هرکدام خواهیم پرداخت، و در قسمت آخر این فصل به تحلیل امنیتی [۱۹] پرداخته و حملاتی که به آن وارد می‌شود را نشان خواهیم داد.



شکل۱: ساختار کلی مربوط به ارتباطات در سیستم خانه هوشمند[۱۹]

۱-۳- فاز مقدماتی

این قسمت توسط نهاد ثبت نام کننده(RA) و به صورت کاملاً محرمانه اتفاق می افتد.ابتدا RA یک E خم بیضوی روی میدان متنهایی Fp و یک گروه جمعی G که زیر گروه Fp بامرتبه اول q، و مولد g را تولید می‌نماید.در جدول شماره ۱ به معرفی علائم اختصاری مربوط به طرح پرداخته‌ایم.

RA ابتدا کلید خصوصی سیستم یعنی $x\in \mathbb{Z}^*q$ و کلید عمومی سیستم $X=x.P$ را تولید می‌کند. آنگاه عددی به عنوان کلید خصوصی بلند مدت K و یک تابع چکیده ساز $h(0):\{0,1\}^* \in \mathbb{Z}^*q$ تولید نموده و x و k را در حافظه‌ی درگاه ارتباطی ذخیره می‌نماید، و پارامترهای $\{E(F_q), G, P, X, h(0)\}$ را اعلام عمومی می‌نماید.

۲-۳- فاز ثبت‌نام

این بخش شامل دو فاز ثبت نام مربوط به دستگاه‌های هوشمند و کاربر می‌باشد.

[۱] Registration authority

ثبت‌نام کاربر: برای اینکه هرکاربر بتواند به اطلاعات حساس در دستگاه‌های هوشمند دسترسی پیدا کند،در ابتدا احتیاج دارد تا توسط RA احراز هویت گردد شکل ۲.

۱- هر کاربر برای خودش یک شناسه و رمزعبور و یک عدد تصادفی a را انتخاب می‌نماید. سپس کاربراز رمز عبور به همراه عدد تصادفی چکیده گرفته و آن را به همراه شناسه به RA در یک کانال امن ارسال می‌کند.

$$HPW_i=h(PW_i||a) \quad (1)$$

۲- RA در ابتدا چک می‌کند که در جدول اطلاعات کاربرآن‌همچین شناسه‌ای موجود نباشد،در صورت وجود RA درخواست یک شناسه دیگر می‌دهد،در غیر اینصورت RA یک کلید مشترک به نام K_{GU} و پارامتر A_1 رامی‌سازد،بعد از آن RA یک عدد تصادفی به نام TEMP ساخته تا با آن تعداد ورودی‌های ناموفق یک کاربر را ثبت نماید و سپس A1 وTEMP را درون یک کارت هوشمند ریخته و آن را به کاربر تحویل می‌دهد.

$$K_{GU}=h(IDi||K) \quad (2)$$

$$A_1= K_{GU}\oplus HPWi \quad (3)$$

۳- کاربر به محض دریافت کارت هوشمند شروع به ساخت دو پارامتر A_2 وA_3 نموده و آن‌ها را نیز داخل کارت هوشمند خود ذخیره می‌نماید.

$$A_2=a\oplus h(ID_i||PW_i) \quad (4)$$

$$A_3=h(ID_i||HPW_i) \quad (5)$$

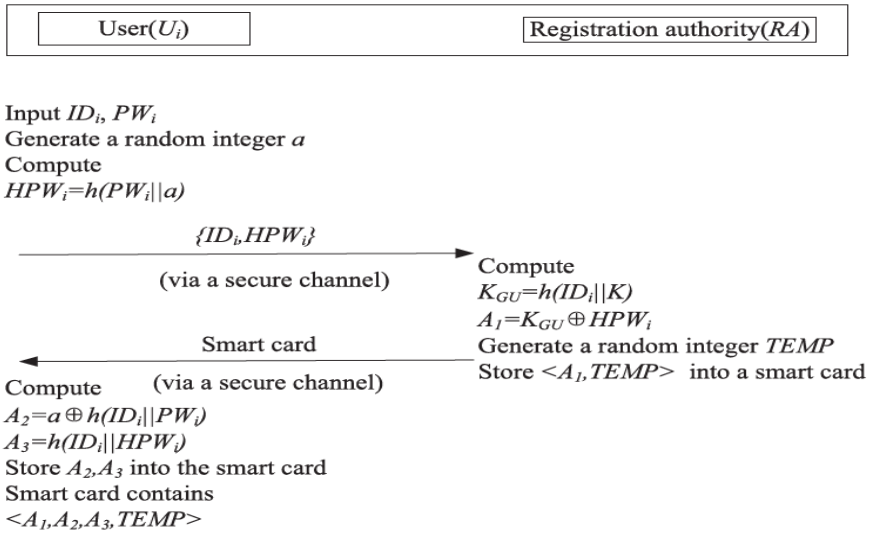
جدول ۱: علائم اختصاری مربوط به طرح [۱۹] و طرح پیشنهادی

نمادها	توصیف
$E(F_q)$	خم بیضوی E بر روی میدان متناهی F_q
G	زیرگروه Fq با مرتبه اول q
P,X	مولد گروه G و دونقطه روی خم بیضوی
ECC	رمزنگاری مبتنی بر خم بیضوی
U_i	کاربر دوردست
GWN	درگاه ارتباطی
SD_k	قطعه هوشمند در خانه
ID_i	شناسه کاربر
PW_i	رمز عبور
DID_i	شناسه مستعار کاربر
GID_j	شناسه درگاه ارتباطی
SID_k	شناسه دستگاه
RA	نهاد ثبت‌نام کننده
K	کلید اصلی خصوصی درگاه ارتباطی
SK	کلید نشست

اعداد تصادفی	R_1,R_2,R_3
تابع هش یک‌طرفه	$h(0)$
الحاق کردن	$X\|\|Y$
جمع به پیمانه ۲	$\oplus$

ثبت نام دستگاه هوشمند : دستگاه هوشمند ابتدا شناسه خود را (SID_k)که قبلاً توسط RA به عنوان یک عدد تصادفی تولید و در حافظه‌ی دستگاه هوشمند ذخیره شده بود را از طریق یک کانال امن برای RA ارسال می‌کند،به محض دریافت، RA ابتدا شناسه را با جدول اطلاعات دستگاه‌ها چک می‌نماید،اگر دستگاهی با آن شناسه موجود بود تقاضای شناسه جدید برای دستگاه هوشمند می‌کند در غیر اینصورت شروع به ساخت کلید K_{GS}می‌نماید و آن را از طریق کانال امن برای دستگاه ارسال می‌نماید.دستگاه پس از دریافت پیام، K_{GS} را در حافظه خود ذخیره می‌کند.

$$K_{GS}=h(SID_k||K) \quad (6)$$



شکل ۲: مرحله‌ی ثبت‌نام کاربر [۱۹]

۳-۳- فاز ورود و احراز هویت

گام اول : کاربر کارت هوشمند خود را روی کارت‌خوان قرار داده و شناسه و رمز عبور خود را وارد می‌نماید. کارت هوشمند عبارات زیر را شروع به محاسبه می‌نماید.

$$a^*= A_2 \oplus h(ID_i \,||\, PW_i) \quad (7)$$
$$HPW^*_i = h\,(PW_i \,||\, a^*) \quad (8)$$
$$A^*_3 = h(ID_i \,||\, HPW^*_i) \quad (9)$$

آنگاه A^*_3 را با A_3 که درون حافظه کارت هوشمند ذخیره شده بود را مقایسه می‌نماید، اگر مقادیر برابر نبودند عدد TEMP را با یک جمع نموده که این عدد تعداد ورودهای ناموفق را نمایش می‌دهد و ارتباط را پایان می‌دهد و در صورتی که هر دو مقدار برابر باشند یعنی کاربر نیز درستکار بوده است و هویتش به درستی برای دستگاه محاسبه کننده محرز می‌گردد و به ادامه محاسبات پرداخته و آن‌گاه دو عدد تصادفی $w \in z_p^*$ و R_1 تولید می‌نماید ؛ وکاربر یک دستگاه را با شناسه (SID_k) انتخاب نموده و بعد از آن دستگاه شروع به محاسبات پارامترهای زیر می‌نماید.

$$K_{GU} = A_1 \oplus HPW_i \quad (10)$$
$$A_4 = w \cdot P \quad (11)$$
$$A_5 = w \cdot X \quad (12)$$
$$DID_i = ID_i \oplus A_5 \quad (13)$$
$$M_1 = (R_1 \,||\, SID_k) \oplus K_{GU} \quad (14)$$
$$V_1 = h\,(ID_i \,||\, R_1 \,||\, K_{GU} \,||\, M_1) \quad (15)$$

و درنهایت کاربر داده‌های M_1, V_1, A_4, DID_i را روی کانال عمومی به سمت درگاه ارسال می‌نماید.

گام دوم : درگاه با داشتن کلید خصوصی x و ضرب اسکالر آن در A_4 ارسالی به A_5 دست می‌یابد و با داشتن این پارامتر مانند زیر می‌تواند شناسه اصلی کاربر را یافته و کلید مشترک بین خود و او را بازیابی نماید و سپس برای اینکه یقین حاصل نماید که این پیام‌ها قطعاً از سمت کاربر ارسال شده‌اند پارامتر V^*_1 را میسازد.

$$A^*_5 = x \cdot A_4 \quad (16)$$
$$DID_i \oplus A^*_5 = ID_i \quad (17)$$
$$K^*_{GU} = h(ID_i || k) \quad (18)$$
$$K_{GU} \oplus M_1 = R^*_1 || SID_k \quad (19)$$
$$V^*_1 = h(ID^*_i || R^*_1 || K^*_{GU} || M_1) \quad (20)$$

و آنگاه با مقایسه‌ی مقادیر V^*_1 با V_1 در صورتی که برابر نباشند به طرح پایان داده و از ارتباط بیرون می‌رود، اما اگر مقادیر یکسان بودند یک عدد تصادفی به نام R_2 و سپس پارامترهای زیر را برای دستگاه هوشمند محاسبه می‌نماید.

$$K_{GS} = h\,(SID_k || k) \quad (21)$$
$$M_2 = (ID_i || GID_j || R_1 || R_2) \oplus K_{GS} \quad (22)$$
$$V_2 = h\,(ID_i || GID_j || K_{GS} || R_1 || R_2 || A_4) \quad (23)$$

و M_2, V_2 را به سمت دستگاه در کانال عمومی ارسال می‌کند.

گام سوم : در این مرحله دستگاه هوشمند با استفاده از کلید مشترکی که درگاه از مرحله‌ی ثبت نام در حافظه‌اش ذخیره نموده بود،و با داشتن مقدار M_2 که از طریق درگاه در کانال عمومی ارسال شده است،مقادیر اعداد تصادفی و شناسه کاربر و درگاه را بدست آورده و مقدار V^*_2 را محاسبه و مقدارش با V_2 ارسالی مقایسه می‌نماید تا از درستکاری درگاه اطمینان حاصل نماید. در صورت مساوی بودن به ساخت اعداد تصادفی R_3 پرداخته وکلید نشست SK_S بین هر سه نهاد را با استفاده از شناسه هر سه نهاد و اعداد تصادفی که هرکدام ساخته بودند،می‌سازد. درنهایت M_3 و V_3 را برای درگاه ساخته و برای او بر روی کانال عمومی ارسال می‌نماید.

$$M_2 \oplus K_{GS} = (ID_i || GID_j || R_1 || R_2) \quad (24)$$
$$V^*_2 = h(ID^*_i || GID^*_j || K_{GS} || R^*_1 || R^*_2) \quad (25)$$
$$SK_S = (ID_i || GID_j || SID_k || R_1 || R_2 || R_3) \quad (26)$$
$$M_3 = K_{GS} \oplus R_3 \quad (27)$$
$$V_3 = h(R_3 || K_{GS} || SK_S) \quad (28)$$

سپس مقادیر V_3,M_3 را به سمت درگاه ارسال می‌کند.

گام چهارم : ازآنجایی‌که در این طرح درگاه هم می‌بایست کلید نشست را محاسبه نماید، پس اطلاعات مجدداً از سمت دستگاه هوشمند به سمت درگاه آمده و درگاه برای به دست آوردن کلید نشست ابتدا شروع به محاسبه‌ی R_3 نموده و کلید نشست SK_g را محاسبه می‌نماید و برای اینکه اطمینان حاصل کند پیام‌ها را یک دستگاه قانونی که در مرحله‌ی قبلی با او ارتباط برقرار کرده بود، می‌باشد مقدار V^*_3 را محاسبه می‌نماید.

$$R^*_3=M_3 \oplus K_{GS} \quad (29)$$
$$SK_g=(ID_i||GID_j||SID_k||R_1||R_2||R_3) \quad (30)$$
$$V^*_3=h(A^*_8||R^*_3||K_{GS}||SK_S||T_s) \quad (31)$$

در صورت مساوی بودن این دو مقدار V^*_3وV_3، مقادیر M_4 و V_4 را می‌سازد و آن‌ها را برای کاربر ارسال می‌کند.

$$M_4=(GID_j||R_1||R_3)\oplus K_{GU} \quad (32)$$
$$V_4=h(R_2||R_3||K_{Gu}||SK_g) \quad (33)$$

حال برای اینکه کاربر نیز از درستکاری درگاه و دستگاه مطمئن شود V^*_4 را حساب کرده و با V_4 که درگاه ارسال کرده مقایسه می‌کند و در صورت درست بودن مقادیر احراز هویت تکمیل و از کلید نشست ساخته شده برای مراحل بعدی ارتباط استفاده می‌کنند و از درستی یکدیگر مطمئن و حریم خصوصی کاربر نیز حفظ می‌گردد.

$$M_4\oplus K_{GU}=(GID_j||R_4||R_3) \quad (34)$$
$$SK_u=(ID_i||GID_j||SID_k||R_1||R_2||R_3) \quad (35)$$
$$V^*_4=h(R_2||R_3||K_{Gu}||SK_g) \quad (36)$$

در شکل شماره ۳ نیز نحوه‌ی تعامل نهادها در طرح شوآی و همکاران آورده شده است.

۴-۳- فاز تغییر رمز عبور

در این مرحله کاربر هرزمانی که بخواهد می‌تواند بدون هیچ تعاملی با درگاه، تنها با انجام دادن گام‌های زیر رمز عبور قبلی خود را تغییر داده و یک رمز عبور جدیدی بسازد.

۱) کاربر شناسه و رمزعبور خود را روی دستگاه موبایل وارد می‌کند

۲) دستگاه مویابل شروع به محاسبه و بدست آوردن عدد تصادفی که کاربر درابتدا ساخته بود می‌کند.

$$a^*= A_2\oplus h(ID_i || PW_i) \quad (37)$$
$$HPW^*_i = h(PW_i || a^*) \quad (38)$$

و در صورتی که مقدار A^*_3 با مقدار A_3 که در کارت هوشمند ذخیره شده بود یکی باشد به کاربر اطمینان کرده و در صورتی که در این مرحله کاربر درخواست یک تغییر رمزعبور نماید،دستگاه می‌پذیرد چرا که وی را به عنوان یک نهاد قانونی پذیرفته است.

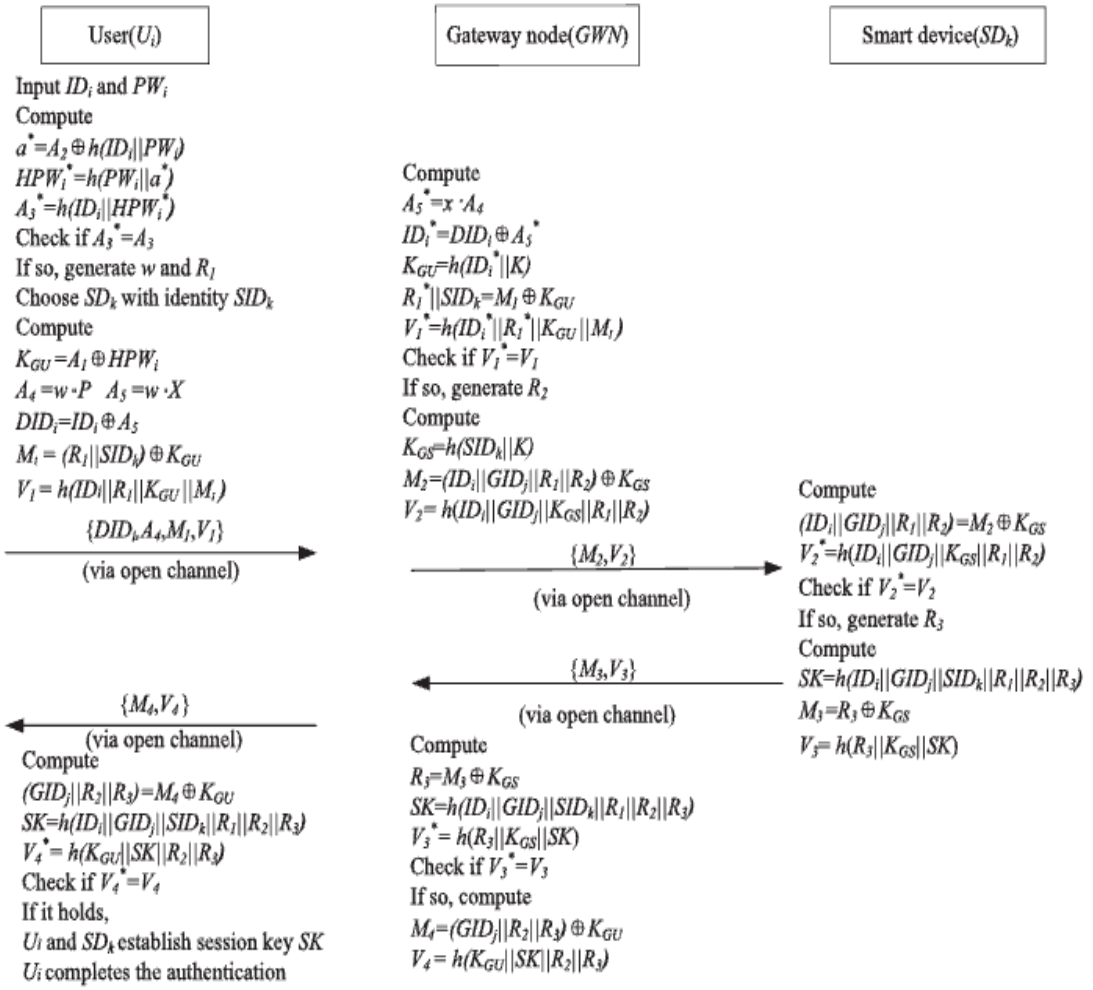
۱) حال دستگاه موبایل شروع به محاسبات جدید می‌نماید و مقادیر جدید را جایگزین مقادیر قبلی که در کارت ذخیره بودند می‌کند.

$$HPW^{new}_i = h\,(PW^{new}_i \,||\, a^*) \quad (39)$$

$$A^{new}_1 = KGU \oplus HPW^*_i = HPWi \oplus A_1 \oplus HPW^{new}_i \quad (40)$$

$$A^{new}_2 = a^* \oplus h(ID_i||PW^{new}_i) \quad (41)$$

$$A^{new}_3 = h(ID_i\ HPW^{new}_i) \quad (42)$$



شکل ۳: مرحله‌ی ورود و احراز هویت [۱۹]

۳-۵- تحلیل امنیتی طرح احراز هویت[۱۹]:

در این قسمت ما نشان خواهیم داد که طرح شوآی و همکاران [۱۹] در مقابل حملاتی چون انکار خدمات سرویس(DOS)،سرقت دستگاه هوشمند و عدم تامین امنیت پیشرو با سرقت درگاه ارتباطی،ضیف و مستعد خوردن حمله می‌باشد.

- **حمله‌ی انکار خدمات سرویس (DOS) :**

با توجه به عدم استفاده از مهر زمانی در طرح شوآی مشاهده می‌نماییم که به این طرح حمله‌ی انکار خدمات وارد میشود.

بدین ترتیب که مهاجم می‌تواند با ارسال پی در پی M_1, V_1, A_4, DID_i به درگاه، او را مشغول نموده و تا حدی که می‌تواند درگاه را از کار بی اندازد،چرا که در درگاه هیچ معیاری جهت سنجش پارامتری مانند زمان که آیا این پیام قبلاً ارسال شده است یا خیر را چک نمیکند.

- **امنیت پیشرو:**

همان طور که در طرح شوآی عنوان گردید،نهاد ثبت نام کننده(RA) کلیدهای خصوصی x و K را در حافظه‌ی درگاه ذخیره می‌نماید.در نتیجه برای امنیت پیشرو با فرض دستیابی مهاجم به کلید خصوصی نهاد ، وی می‌تواند پارامترهای زیر را به ترتیب محاسبه نموده :

گام اول: محاسبه‌ی پارامترA^*_5 و سپس می‌تواند با استفاده از شناسه مستعار ارسال شده(DID_i) و مقدار A^*_5 به شناسه اصلی کاربر دست یابد از طرفی در این مرحله گمنامی کاربر و حریم خصوصی وی در معرض خطر قرار می‌گیرد.

گام دوم :در این مرحله مهاجم با داشتن شناسه اصلی کاربر و همچنین کلید K می‌تواند به کلید اشتراکیK_{GU} بین درگاه و کاربر دست یابد حال با داشتن مقدار M_1 که از طرف کاربر در کانال عمومی ارسال شده بود می‌تواند عدد تصادفی که کاربر تولید نموده بود و هچنین دستگاه هوشمندی را که انتخاب نموده بود دست یابد.

$$M_1 \oplus K_{GU} = R^*_1 || SID_k \quad (43)$$

گام سوم :مهاجم یک عدد تصادفی به نام R_2 نیز انتخاب نموده و تمامی مراحلی که در مرحله‌ی احراز هویت درگاه بیان گردید را انجام می‌دهد،و برای دستگاه هوشمند در کانال عمومی ارسال می‌نماید.از طرفی با مقادیری که دستگاه هوشمند تولید میکند و در مراحل بعد برای درگاه ارسال می‌کند وی می‌تواند به عدد تصادفی انتخابی دستگاه دست یافته و کلید نشست بین سه نهاد را ایجاد نماید و امنیت سیستم را به مخاطره اندازد.

$$R^*_3 = M_3 \oplus K_{GS} \quad (44)$$

$$SK_{GWN} = (ID_i || GID_j || SID_k || R_1 || R_2 || R_3) \quad (45)$$

- **حمله‌ی سرقت دستگاه هوشمند :**

در صورتی که فرض نماییم دستگاه هوشمند بدست افراد خرابکار بیفتد،از آنجایی که در مرحله‌ی ثبت نام کلید اشتراکی بین درگاه و دستگاه توسط RA در حافظه‌ی دستگاه هوشمند ذخیره گردید،در نتیجه مهاجم می‌تواند به K_{GS} دست یابد و با محاسبه‌ی

$$M_2 \oplus K_{GS} = (ID_i || GID_j || R_1 || R_2) \quad (46)$$

به یکباره به شناسه کاربر و اعداد تصادفیR_1 و R_2 تولید شده توسط کاربر و درگاه دست می‌یابد از طرفی خود نیز یک عدد تصادفی R_3 تولید می‌نماید و به کلید نشست دست می‌یابد.

$$SK_s = (ID_i || GID_j || SID_k || R_1 || R_2 || R_3) \quad (47)$$

.

۴. طرح ارائه شده پیشنهادی

طرح احراز هویت پیشنهادی ما نیز مشابه طرح [۱۹] دارای پنج فاز می‌باشد:فاز مقدماتی- فازثبت نام(اخذ کارت هوشمند)- فاز ورود- فاز احرازهویت- فاز تغییر رمزعبور. در اینجا بدلیل محدودیت‌های نوشتاری از تکرار فازهای مشابه با طرح [۱۹] که به تفضیل در فصل قبل توضیح داده شد اجتناب می‌نماییم.

۴-۱- فاز مقدماتی

مشابه طرح [۱۹] می‌باشد.

۴-۲- فاز ثبت نام

این فاز شامل دو ثبت نام است:ثبت نام کاربر(مشابه طرح [۱۹] می‌باشد.) و ثبت نام دستگاه هوشمند.

ثبت نام دستگاه هوشمند : هر دستگاه دارای یک شناسه SID_k و یک کلید خصوصی x_j می‌باشد. دستگاه هوشمند ابتدا شناسه SID_k خود را از طریق یک کانال امن برای RA ارسال می‌کند، به‌محض دریافت RA ابتدا شناسه را با جدول اطلاعات دستگاه‌ها چک می‌نماید، اگر دستگاهی با آن شناسه موجود بود تقاضای شناسه جدید برای دستگاه هوشمند می‌کند در غیر این صورت شروع به ساخت کلید K_{GS} می‌نماید و آن را از طریق کانال امن برای دستگاه ارسال می‌نماید. دستگاه پس از دریافت پیام K_{GS} شروع به محاسبه‌ی B_1 می‌نماید و درنهایت به‌جای ذخیره K_{GS} که باعث به وجود آمدن تهدیدات فراوانی می‌گردد،B_1 را در حافظه خود ذخیره می‌کند.

$$K_{GS}=h(SID_K||K) \quad (48)$$
$$B_1= K_{GS} \oplus h(SID_K|| x_j) \quad (49)$$

۴-۳- فاز ورود

این قسمت نیز مشابه فاز ورود طرح[۱۹] می‌باشد که در قسمت ۳-۳- به تفضیل توضیح داده شد.تنها پارامتری که اضافه شده است استفاده از یک مهر زمانی T_u می‌باشد،که هم در محاسبات V_1 آورده شده و هم به صورت آشکار برروی کانال عمومی به اشتراک گذاشته خواهد شد.

$$V_1 = h\ (ID_i \,||\, R_1 \,||\, K_{GU} \,||\, M_1 /\!/ T_u) \quad (50)$$

و درنهایت کاربر داده‌های $T_u, M_1, V_1, A_4, DID_i$ را به سمت درگاه ارسال می‌نماید.

۴-۴- فاز احراز هویت

گام اول : درگاه ابتدا به محاسبه‌ی پارامترهای زیر می‌پردازد.

$$A^*_5 = x \cdot A_4 \quad (51)$$
$$ID_i=DID_i \oplus A^*_5 \quad (52)$$
$$K_{GU}=h(ID_i||k) \quad (53)$$
$$R^*_1||SID_k=M_1 \oplus K_{GU} \quad (54)$$

و آنگاه با محاسبه‌ی V^*_1 مقدار آن را با مقدار V_1 مقایسه می‌نماید. در صورتی که برابر نباشند به طرح پایان داده و از ارتباط بیرون می‌رود، اما اگر مقادیر یکسان بودند به تولید مقادیر تصادفی$y,R_2 \in \mathbb{Z}^*_n$و مهرزمانی T_g پرداخته و سپس پارامترهای زیر را محاسبه می‌نماید.

$$V^*1=h(ID^*i||R^*1||K^*GU||M1) \quad (55)$$
$$A6=y.P \quad (56)$$
$$KGS=h\ (SIDk||k) \quad (57)$$
$$M2= (IDi||GIDj||R1||R2) \oplus KGS \quad (58)$$
$$V2=h\ (IDi||GIDj||KGS||R1||R2||A4||A6||Tg) \quad (59)$$

و V_2, M_2, T_g, A_6, A_4 را به سمت دستگاه ارسال می‌کند.

گام دوم : در این مرحله برخلاف مقاله[۱۹] که دستگاه هوشمند کلید را در حافظه‌ی خود ذخیره می‌کرد،در اینجا باید آن را محاسبه نماید و چون در فرمول محاسباتی آن از کلید خصوصی دستگاه استفاده‌شده است تنها خود او قادر به محاسبه‌ی مقدار خواهد بود.پس دستگاه در ابتدا شروع به محاسبه‌ی K_{GS} می‌نماید.و ادامه محاسبات را به روال زیر انجام می‌دهد.

$$K_{GS}=B_1 \oplus h(SID_k||x_j) \quad (60)$$
$$M_2 \oplus K_{GS}=(ID_i||GID_j||R_1||R_2) \quad (61)$$
$$V^*_2=h(ID^*_i||GID^*_j||K_{GS}||R^*_1||R^*_2||A_4||A_6||T_g) \quad (62)$$

و مقادیر V^*_2 را با مقدار V_2 مقایسه می‌نماید، در صورت مساوی بودن به ساخت اعداد تصادفی$z,R_3 \in \mathbb{Z}^*_n$و مهرزمانی T_s پرداخته و سپس محاسبات مقادیر زیر را انجام می‌دهد.

$$A_v=z.P \quad (63)$$
$$A_8=z.X \quad (64)$$
$$K_S=e(A_4,A_6)^z \quad (65)$$

درنهایت شروع به ساخت کلید نشست و M_3 و V_3 می‌نماید.

$$SK_S=(K_S||A_4||A_6||A_v R_1||R_2||R_3) \quad (66)$$
$$M_3=K_{GS} \oplus R_3 \quad (67)$$
$$V_3=h(A_8||R_3||K_{GS}||SK_S||T_s) \quad (68)$$

سپس مقادیر V_3,M_3,T_S,A_7 را به سمت درگاه ارسال می‌کند.

گام چهارم : ازآنجایی‌که در این طرح درگاه هم می‌بایست کلید نشست را محاسبه نماید، پس اطلاعات مجدداً از سمت دستگاه به سمت دستگاه آمده و دستگاه برای به دست آوردن کلید نشست ابتدا شروع به محاسبه‌ی R_3 نموده و کلید مخصوص خود یعنی K_g می‌نماید.

$$R^*_3= M_3 \oplus K_{GS} \quad (69)$$
$$K_g=e(A_4,A_7)^y \quad (70)$$
$$SK_g=(K_g||A_4||A_6||A_7||R_1||R_2||R_3) \quad (71)$$
$$A^*_8=A_7.x \quad (72)$$
$$V^*_3=h(A^*_8||R^*_3||K_{GS}||SK_S||T_s) \quad (73)$$

در این مرحله باز برای اینکه صحت و درستی دستگاه را بررسی کند، مقدار V^*_3 را با V_3 مقایسه می‌کند، وقتی از اصالت دستگاه مطمئن می‌شود مقادیر M_4 و V_4 را می‌سازد و آن‌ها را برای کاربر ارسال می‌کند.

$$M_t=(GID_j||R_1||R_3) \oplus K_{GU} \quad (74)$$
$$V_t=h(A_6||A_7||R_2||R_3||K_{Gu}||SK_g||T_{g2}) \quad (75)$$

حال برای اینکه کاربر نیز از درستکاری درگاه و دستگاه مطمئن شود V^*_4 را حساب کرده و با آن عددی که درگاه ارسال کرده مقایسه می‌کند و در صورت درست بودن از آن کلید نشست برای مراحل بعدی ارتباط استفاده می‌کنند و از درستی یکدیگر مطمئن و حریم خصوصی کاربر نیز حفظ می‌گردد.

$$M_t \oplus K_{GU}=(GID_j||R_1||R_3) \quad (76)$$
$$K_u=e(A_6,A_7)^w \quad (77)$$
$$SK_u=(K_u||A_4||A_6||A_7||R_1||R_2||R_3) \quad (78)$$
$$V^*_4=h(A_6||A_7||R_2||R_3||K_{Gu}||SK_g||T_{g2}) \quad (79)$$

۵. تحلیل امنیتی طرح پیشنهادی

۵-۱- احراز هویت دوگانه:

در طرح ارائه شده در حقیقت کاربر و دستگاه هوشمند یکدیگر را از طریق درگاه احراز هویت می‌کنند و پارامتر مهمی که در طرح به نام V مشخص گردیده بود در حقیقت معیاری برای سنجش درستی یا نادرستی نهادها بود، و در صورتی که مقادیر V ها با یکدیگر مطابقت نداشت در همان زمان طرح قطع می‌گردید.

۵-۲- گمنامی و عدم ردیابی:

همان‌گونه که در طرح نیز مشخص است در هیچ مرحله‌ای شناسه کاربر یعنی IDi و یا حتی دستگاه هوشمند SID_k به‌صورت آشکار در طرح ارسال نگشته است برای کاربر از یک شناسه مستعار استفاده می‌گردد که DID_i نام دارد بنابراین گمنامی‌شان و عدم ردیابی آن‌ها به‌خوبی رعایت گردیده است.

۵-۳- مقاوم در برابر حمله‌ی دزدیده شدن دستگاه:

با بهبودی که در طرح ایجاد نمودیم یعنی اصلاح مرحله ی ثبت نام دستگاه هوشمند به طوری که دستگاه بعد از مراجعه به RA و دریافت کلید مشترک بین خود و درگاه آن را ذخیره نمی کند بلکه پارامتر دیگری ساخته که در ساختار آن از کلید خصوصی خودش استفاده شده است در نتیجه انتظار می رود با توجه به عدم دسترسی مهاجم به کلید خصوصی دستگاه، برای انجام این حمله و دستیابی به کلید نشست موفق نخواهد بود.

$$B_1 = K_{GS} \oplus h(SID_K || x_j) \quad (80)$$

۵-۴- امنیت پیشرو:

با توجه به طرح بهبود یافته و تغییر در ساختار کلید نشست آن قابل مشاهده است که مهاجم حتی با داشتن کلیدهای خصوصی درگاه و سیستم قادر نخواهد بود به کلید نشست دست یابد، چرا که در هر مرحله هر نهاد یک عدد تصادفی انتخاب می‌نماید و با استفاده از تزویج دوخطی و خم بیضوی کلید نشست را محاسبه می‌نمایند، که با استفاده از این روش دیگر مهاجم قادر به محاسبه کلید نخواهد بود و امنیت کلید در نشست‌های قبلی نیز حفظ می‌گردد.

۵-۵- مقاوم در برابر حمله‌ی انکار خدمات (DOS):

همان طور که مشاهده می کنیم در طرح بهبود یافته در انتهای هر نشست در مرحله ی احراز هویت ما از برچسب های زمانی استفاده می کنیم که این برچسب های زمانی را برای جلوگیری از دستکاری توسط مهاجمین در داخل پیام های تایید هویت V نیز قرار می دهیم تا در صورت هرگونه تغییر سمت مقابل با محاسبه V متوجه و از احراز هویت وی اجتناب نماید.

۵-۶- توافق کلید نشست:

همان‌طور که در جزئیات طرح نیز گفته شد تنها سه نهاد کاربر و درگاه و دستگاه هوشمند قادر به ساخت کلید نشست هستند، چرا که در ساخت کلید نشست از نگاشت دوخطی و رمزنگاری مبتنی بر خم بیضوی و اعداد تصادفی بهره برده ایم که تنها خود صاحبان آن کلید دارنده آن هستند. پس شخص دیگری قادر نخواهد بود کلیدها را محاسبه نماید مگر اینکه مجوزهای دسترسی برایشان ایجاد گردد..

۶.مقایسه عملکرد سیستم طرح پیشنهادی با سایر طرح‌های ارائه شده :

در این قسمت به بررسی و مقایسه چهار طرح لی[۲۰]، هان و همکاران[۲۱]،کومار و همکاران [۱۷] و شوآی و همکاران [۱۹] با طرح احراز اصالت پیشنهادی در این مقاله می‌پردازیم.

مقایسه امنیتی : جدول شماره ۲ بررسی الزامات امنیتی طرح پیشنهادی با سایر طرح‌ها می‌باشد

.

جدول شماره۲: مقایسه ویژگی‌های امنیتی

ویژگی‌های امنیتی	طرح لی(۲۰۱۳)	طرح هان و همکاران(۲۰۱۳)	طرح کومار و همکاران(۲۰۱۵)	طرح وازید و همکاران(۲۰۱۷)	طرح شوآی و همکاران(۲۰۱۹)	طرح ما
احراز هویت دوطرفه	خیر	خیر	خیر	بله	بله	بله
توافق کلید نشست	بله	بله	بله	بله	بله	بله
گمنامی	بله	بله	خیر	بله	بله	بله
عدم ردیابی	بله	بله	خیر	بله	بله	بله
حمله‌ی غیرهمزمانی	بله	بله	بله	خیر	بله	بله
حمله‌ی مردی در میانه	بله	بله	بله	بله	بله	بله
امنیت پیشرو	بله	بله	بله	خیر	خیر	بله
حمله‌ی از دست دادن گوشی همراه	بله	بله	بله	بله	خیر	بله
حمله‌ی داخلی	بله	بله	بله	بله	خیر	بله
حمله‌ی جعل	بله	بله	بله	بله	بله	بله
حمله‌ی تکرار	بله	بله	بله	بله	بله	بله

مقایسه محاسباتی :

جهت تحلیل عملکرد و کارآیی یک طرح بررسی سربارهای محاسباتی‌اش از اهمیت ویژه‌ای برخوردار است چرا که ارتباط مستقیم با سرعت دارد و هرچه زمان کمتر عملکرد بیشتر خواهد بود.به همین دلیل در جدول ۲ با استفاده از پارامترهای $T_{ED}, T_{exp}, T_{fe}, T_{mac}, T_{hmac}, T_h$ که به ترتیب نمایش دهنده‌ی زمان تابع رمزنگاری و رمزگشایی در رمزنگاری متقارن، زمان تابع ECC ،زمان توابع فازی،تابع هش و تابع مک می‌باشند.طرح پیشنهادی ما نسبت به طرح[۱۹] تنها سه نگاشت خطی اضافه دارد، که در جدول شماره ۳ این مقایسه انجام شده است.

جدول شماره ۳: مقایسه هزینه‌های محاسباتی

طرح احراز هویت	کل هزینه
طرح لی(۲۰۱۳)	$4\,T_{exp} + 2\,T_{ED} + 2\,T_{mac} + 2\,T_h$
طرح هان و همکاران(۲۰۱۳)	$6\,T_{ED} + 12\,T_{mac} + 10\,T_h$
طرح کومار و همکاران(۲۰۱۵)	$2\,T_{ED} + T_{mac} + T_{hmac} + 2\,T_h$
طرح وازید و همکاران(۲۰۱۷)	$T_{ED} + T_{fe} + 22\,T_h$
طرح شوآی و همکاران(۲۰۱۹)	$3\,T_{exp} + 16\,T_h$
طرح ما	$۳T_{exp} + ۱۶\,T_h + ۳T_e$

مقایسه مخابراتی :

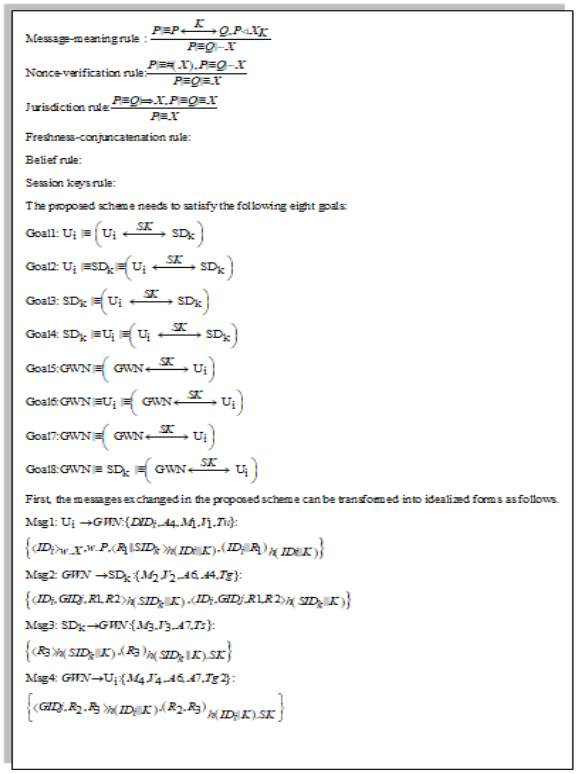
جدول شماره ۴ سربار مخابراتی طرح پیشنهادی ما را با سایر طرح‌های ذکر شده در بالا مقایسه می‌نماید.برای مقایسه‌ی بهتر فرض کنیم که تعداد بیت‌های شناسه-شبه شناسه-رمزعبور-شناسه حسگر هرکدام ۱۲۸ بیت و مهرزمانی ۳۲ بیت و کلید خصوصی و اعداد تصادفی ۱۶۰ بیت و ضرب ECC ۳۲۸ بیت و هرکدام از خروجی‌های توابع چکیده ساز ۲۵۶بیت باشد طبق جدول خواهیم داشت:

جدول شماره ۴: مقایسه سربار مخابراتی

طرح احراز هویت	کل پیام	مجموع بیت‌ها
طرح لی(۲۰۱۳)	۴ پیام	**۱۲۱۶**
طرح هان و همکاران(۲۰۱۳)	۶ پیام	**۲۲۷۲**
طرح کومار و همکاران(۲۰۱۵)	۳ پیام	**۱۳۷۶**
طرح وازید و همکاران(۲۰۱۷)	۴ پیام	**۲۰۸۲**
طرح شوآی و همکاران(۲۰۱۹)	۴ پیام	**۱۷۲۸**
طرح ما	۴پیام	**۳۹۶۸**

۷. اثبات امنیتی از طریق BAN logic:

BAN logic یک روش منطقی برای اثبات امنیتی پروتکل‌های رمزنگاری می‌باشد در حقیقت مجموعه ای از قوانین برای تعریف و تحلیل پروتکل های تبادل اطلاعات است که به کاربران خود کمک می کند تا تعیین کنند که آیا اطلاعات تبادل شده در برابر استراق سمع، قابل اعتماد هستند یا خیر . منطق BAN با این فرض آغاز می شود که همه تبادل اطلاعات در کانال های عمومی و آسیب پذیر در برابر دستکاری و نظارت عمومی صورت می گیرد. در نهایت پس از بررسی طرح با منطق BAN برای مقاله‌ی طرح پیشنهادی، امنیت و مصونیت در برابر دستکاری مشهود گشت که در زیر به آنها اشاره می‌شود.



Message-meaning rule : $\frac{P\equiv P\xleftrightarrow{K} Q, P\triangleleft X_K}{P\equiv Q\mid\sim X}$

Nonce-verification rule: $\frac{P\equiv\#(X), P\equiv Q\mid\sim X}{P\equiv Q\equiv X}$

Jurisdiction rule: $\frac{P\equiv Q\Rightarrow X, P\equiv Q\equiv X}{P\equiv X}$

Freshness-conjuncatenation rule:

Belief rule:

Session keys rule:

The proposed scheme needs to satisfy the following eight goals:

Goal1: $U_i \equiv \left(U_i \xleftrightarrow{SK} SD_k\right)$

Goal2: $U_i \equiv SD_k \equiv \left(U_i \xleftrightarrow{SK} SD_k\right)$

Goal3: $SD_k \equiv \left(U_i \xleftrightarrow{SK} SD_k\right)$

Goal4: $SD_k \equiv U_i \equiv \left(U_i \xleftrightarrow{SK} SD_k\right)$

Goal5: $GWN \equiv \left(GWN \xleftrightarrow{SK} U_i\right)$

Goal6: $GWN \equiv U_i \equiv \left(GWN \xleftrightarrow{SK} U_i\right)$

Goal7: $GWN \equiv \left(GWN \xleftrightarrow{SK} U_i\right)$

Goal8: $GWN \equiv SD_k \equiv \left(GWN \xleftrightarrow{SK} U_i\right)$

First, the messages exchanged in the proposed scheme can be transformed into idealized forms as follows.

Msg1: $U_i \rightarrow GWN: \{DID_i, A4, M_1, T_1\}$:

$\left\{\langle ID_i\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

Msg2: $GWN \rightarrow SD_k: \{M_2, T_2, A5, A4, T_E\}$:

$\left\{ID_i, GID_j, R1, R2\rangle_{h(SID_k \| K)}, \langle ID_i, GID_j, R1, R2\rangle_{h(SID_k \| K)}\right\}$

Msg3: $SD_k \rightarrow GWN: \{M_3, T_3, A7, T_3\}$:

$\left\{\langle R_3\rangle_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\right\}$

Msg4: $GWN \rightarrow U_i: \{M_4, T_4, A6, A7, T_E 2\}$:

$\left\{\langle GID_j, R_2, R_3\rangle_{h(ID_i \| K)}, (R_2, R_3)_{h(ID_i \| K)}, SK\right\}$

Second, some initial assumptions about the proposed scheme are listed below:

A1: $GWN \mid\equiv \#(R_1)$

A2: $SD_k \mid\equiv \#(R_2)$

A3: $GWN \mid\equiv \#(R_3)$

A4: $U_i \mid\equiv U_i \xleftrightarrow{x, w, P} GWN$

A5: $GWN \mid\equiv GWN \xleftrightarrow{W, X, P} (U_i)$

A6: $GWN \mid\equiv GWN \xleftrightarrow{h(SID_k \| K)} SD_k$

A7: $SD_k \mid\equiv SD_k \xleftrightarrow{h(SID_k \| K)} GWN$

A8: $U_i \mid\equiv SD_k \mid\Rightarrow \{R_3, SID_k, SK\}$

A9: $U_i \mid\equiv GWN \mid\Rightarrow \{R_2, GID_j, SK, W, P\}$

A10: $GWN \mid\equiv U_i \mid\Rightarrow \{R_1, ID_i, SK, x, w, P\}$

A11: $GWN \mid\equiv SD_k \mid\Rightarrow \{R_3, SID_k, SK\}$

A12: $SD_k \mid\equiv U_i \mid\Rightarrow \{R_1, U_i, SK\}$

A13: $SD_k \mid\equiv GWN \mid\Rightarrow \{R_2, GID_j, SK\}$

Third, based on the BAN logic rules and assumptions, the main proofs are performed as follows:

According to the Msg1, we get:

S1: $GWN \triangleleft \left\{\langle ID_i\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

Based on Assumption A5, S1 and message-meaning rule, we have:

S2: $GWN \mid\equiv U_i \mid\sim$

$\left\{\langle ID_i\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

From A1 and freshness-conjuncatenation rule, we get:

S3: $GWN \mid\equiv \#\left\{\langle ID_i\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

From S3, S2 and nonce-verification rule, we get:

S4: $GWN \mid\equiv U_i \mid\equiv$

$\left\{\langle ID_i\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

According to the Msg2, we get:

S5: $SD_k \triangleleft \left\{\langle ID_i, GID_j, R_1, R_2\rangle_{h(SID_k \| K)}, \langle ID_i, GID_j, R_1, R_2\rangle_{h(SID_k \| K)}\right\}$

From A7, S5 and message-meaning rule, we have:

S6: $SD_k \mid\equiv GWN \mid\sim \left\{\langle ID_i, GID_j, R_1, R_2\rangle_{h(SID_k \| K)}, \langle ID_i, GID_j, R_1, R_2\rangle_{h(SID_k \| K)}\right\}$

From A2 and freshness-conjuncatenation rule, we get:

From S12, A11 and jurisdiction rule, we get:

S22: $GWN \mid\equiv \left(GWN \xleftrightarrow{SK} SD_k\right) (\text{Goal7})$

From S8, A13 and jurisdiction rule, we get:

S23: $SD_k \mid\equiv \left\{< IDi, GIDj, R_1, R_2 >_{h(SID_k \| K)}, (IDi, GIDj, R_1, R_2)_{h(SID_k \| K)}\right\}$

From S7, S8, S23 and session keys rule, we get:

S24: $SD_k \mid\equiv GWN \mid\equiv \left(GWN \xleftrightarrow{SK} SD_k\right)$

From S24, A13 and jurisdiction rule, we get:

S25: $SD_k \mid\equiv \left(GWN \xleftrightarrow{SK} SD_k\right)$

From S16, A9 and jurisdiction rule, we get:

S26: $U_i \mid\equiv \left\{< GIDj, R_1, R_2 >_{h(ID_i \| K)}, (R_2, R_3)_{h(ID_i \| K), SK}\right\}$

From S15, S16, S26 and session keys rule, we get:

S27: $U_i \mid\equiv GWN \mid\equiv \left(U_i \xleftrightarrow{SK} GWN\right)$

From S27, A9 and jurisdiction rule, we get:

S28: $U_i \mid\equiv \left(U_i \xleftrightarrow{SK} GWN\right)$

From S18 and S24, we get:

S27: $U_i \mid\equiv SD_k \mid\equiv \left(U_i \xleftrightarrow{SK} SD_k\right) (\text{Goal2})$

From S21 and S27, we get:

S27: $SD_k \mid\equiv U_i \mid\equiv \left(U_i \xleftrightarrow{SK} SD_k\right) (\text{Goal2}) 4$

From S29, A9 and jurisdiction rule, we get:

S31: $U_i \mid\equiv \left(U_i \xleftrightarrow{SK} SD_k\right) (\text{Goal1})$

From S30, A12 and jurisdiction rule, we get:

S32: $SD_k \mid\equiv \left(U_i \xleftrightarrow{SK} SD_k\right) (\text{Goal3})$

S7: $SD_k \mid\equiv GWN \mid\sim \left\{\langle IDi, GIDj, R_1, R_2\rangle_{h(SID_k \| K)}, \langle IDi, GIDj, R_1, R_2\rangle_{h(SID_k \| K)}\right\}$

From S6, S7 and nonce-verification rule, we get:

S8: $SD_k \mid\equiv GWN \mid\equiv \left\{\langle IDi, GIDj, R_1, R_2\rangle_{h(SID_k \| K)}, \langle IDi, GIDj, R_1, R_2\rangle_{h(SID_k \| K)}\right\}$

According to the Msg3, we get:

S9: $GWN \triangleleft \{< R_3 >_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\}$

From A6, S9 and message-meaning rule, we have:

S10: $GWN \mid\equiv SD_k \mid\sim \{< R_3 >_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\}$

From A3 and freshness-conjuncatenation rule, we get:

S11: $GWN \mid\equiv \#(SD_k) \mid\sim \{< R_3 >_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\}$

From S10, S11 and nonce-verification rule, we get:

S12: $GWN \mid\equiv SD_k \mid\equiv \{< R_3 >_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\}$

According to the Msg4, we get:

S13: $U_i \triangleleft \left\{\langle GIDj, R_1, R_2\rangle_{(ID_i \| K)}, \langle R_2, R_3\rangle_{(ID_i \| K)}, SK\right\}$

From A4, S13 and message-meaning rule, we have:

S14: $U_i \mid\equiv GWN \mid\sim \left\{\langle GIDj, R_1, R_2\rangle_{(ID_i \| K)}, \langle R_2, R_3\rangle_{(ID_i \| K)}, SK\right\}$

From A1, A2, A3 and freshness-conjuncatenation rule, we get:

S15: $U_i \mid\equiv \#\left\{\langle GIDj, R_1, R_2\rangle_{(ID_i \| K)}, \langle R_2, R_3\rangle_{(ID_i \| K)}, SK\right\}$

From S14, S15 and nonce-verification rule, we get:

S16: $U_i \mid\equiv GWN \mid\equiv \left\{\langle GIDj, R_1, R_2\rangle_{h(ID_i \| K)}, \langle R_2, R_3\rangle_{h(ID_i \| K)}, SK\right\}$

From S4, A5, A10 and jurisdiction rule, we get:

S17: $GWN \mid\equiv \left\{\langle IDi\rangle_{W.X}, W.P, \langle R_1 \| SID_k\rangle_{h(ID_i \| K)}, SK, (ID_i \| R_1)_{h(ID_i \| K)}\right\}$

From S3, S4, S17 and session keys rule, we get:

S18: $GWN \mid\equiv U_i \mid\equiv \left(GWN \xleftrightarrow{SK} U_i\right) (\text{Goal6})$

From S18, A10 and jurisdiction rule, we get:

S19: $GWN \mid\equiv U_i \mid\equiv \left(GWN \xleftrightarrow{SK} U_i\right) (\text{Goal5})$

From S12, A11 and jurisdiction rule, we get:

S20: $GWN \mid\equiv SD_k \mid\equiv \{< R_3 >_{h(SID_k \| K)}, (R_3)_{h(SID_k \| K)}, SK\}$

From S11, S12, S20 and session keys rule, we get:

S21: $GWN \mid\equiv SD_k \mid\equiv \left(GWN \xleftrightarrow{SK} SD_k\right) (\text{Goal8})$

شکل های ۴- کدهای BAN logic –به ترتیب از بالا از سمت چپ

۸.نتیجه‌گیری

همانند سایر زیر حوزه‌های اینترنت اشیاء، برای خانه‌های هوشمند نیز مسئله‌ی حریم خصوصی و احراز هویت یک چالش مهمی به شمار می‌آید. چراکه ممکن است با انتشار اطلاعات خصوصی و یا ردیابی رفتارها و الگوهای مصرفی‌شان در حریم خانه، زندگی‌شان به مخاطره بیفتد. همان‌طور که در متن نیز اشاره شده طرح‌های گوناگونی برای این موضوع ایجاد شده است که یکی از جدیدترین آن‌ها طرح شوآی و همکارانش[۱۹] بود. با توجه به اینکه طرح شان یک طرح سبک جهت احراز هویت محسوب می‌گردید، می‌توانست برای محیط اینترنت اشیاء بسیار مناسب باشد اما با بررسی‌های به عمل آمده نشان داده شد که در مقابل تهدیدات امنیتی کارساز نبود ، و بدین ترتیب طرح پیشنهادی جهت حفظ حریم خصوصی و امنیت کاربران ارائه گردید؛ که در ساختار آن‌هم از خم بیضوی و هم از نگاشت دوخطی استفاده می‌گردد؛در انتها با استفاده از تحلیل Ban logic نیز نشان دادیم که طرح امن بوده و مشکلات طرح قبلی را نیز ندارد.

۹. مراجع

[1] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors (Switzerland)*, vol. 19, no. 5, Mar. 2019.

[2] S. Li, L. Da Xu, and S. Zhao, “The internet of things: a survey,” *Inf. Syst. Front.*, vol. 17, no. 2, pp. 243–259, Apr. 2015.

[3] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” *Int. J. Inf. Technol.*, vol. 10, no. 2, pp. 189–200, Jun. 2018.

[4] J. M. Hernández-Muñoz *et al.*, “LNCS 6656 - Smart Cities at the Forefront of the Future Internet,” 2011.

[5] J. Bugeja, A. Jacobsson, and P. Davidsson, “On Privacy and Security Challenges in Smart Connected Homes,” 2016.

[6] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, “A security authorization scheme for smart home Internet of Things devices,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 740–749, Sep. 2018.

[7] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of things: The road ahead,” *Computer Networks*, vol. 76. Elsevier B.V., pp. 146–164, 15-Jan-2015.

[8] M. Seliem, K. Elgazzar, and K. Khalil, “Towards Privacy Preserving IoT Environments: A Survey,” *Wireless Communications and Mobile Computing*, vol. 2018. Hindawi Limited, 2018.

[9] K. He, J. Weng, Y. Mao, and H. Yuan, “Anonymous identity-based broadcast encryption technology for smart city information system,” 2017.

[10] J. Zhou, Z. Cao, X. Dong, and A. V Vasilakos, "Security and Privacy for Cloud-Based IoT : Challenges , Countermeasures , and Future Directions," no. January, pp. 26–33, 2017.

[11] N. Y. Lee and J. C. Chen, "Improvement of one-time password authentication scheme using smart cards," *IEICE Trans. Commun.*, vol. E88-B, no. 9, pp. 3765–3767, 2005.

[12] I. You and E. S. Jung, "A light weight authentication protocol for digital home networks," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2006, vol. 3983 LNCS, pp. 416–423.

[13] J. Jeong, Y. C. Min, and H. Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2008.

[14] B. Vaidya, J. H. Park, S. S. Yeo, and J. J. P. C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment," *Comput. Commun.*, vol. 34, no. 3, pp. 326–336, Mar. 2011.

[15] H. J. Kim and H. S. Kim, "AUTHHOTP - HOTP based authentication scheme over home network environment," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2011, vol. 6784 LNCS, no. PART 3, pp. 622–637.

[16] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Device authentication mechanism for smart energy home area networks," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2011, pp.

787–788.

[17] V. Odelu, A. K. Das, and A. Goswami, "A secure and efficient ECC-based user anonymity preserving single sign-on scheme for distributed computer networks," *Security and Communication Networks*, vol. 8, no. 9. pp. 1732–1751, 2015.

[18] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment," *IEEE Transactions on Dependable and Secure Computing*, Institute of Electrical and Electronics Engineers Inc., 17-Oct-2017.

[19] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security," *Comput. Secur.*, vol. 86, pp. 132–146, Sep. 2019.

[20] R. Wang, M. Zhang, D. Feng, Y. Fu, and Z. Chen, "De-anonymization attack; hidden markov model; privacy disclosure; spatio-temporal influences," vol. 9977, pp. 478–484, 2016.

[21] A. Karati, R. Amin, S. K. H. Islam, and K. K. R. Choo, "Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment," *IEEE Trans. Cloud Comput.*, vol. 7161, no. c, pp. 1–14, 2018.

[22] F. Wu *et al.*, "A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3527–3542, Nov. 2016.