روش‌های احراز هویت و توافق کلید در اینترنت اشیاء

محدثه محمدی[۱]، محمدمهدی گیلانیان صادقی[۱]

[۱]گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه آزاد اسلامی واحد قزوین، قزوین، ایران
mohadesehmohammadi@ymail.com,msadeghi@ieee.com

چکیده

افزایش داده‌های حساس در اینترنت اشیا (IoT)، نیازهای محاسبات، ارتباطات و ذخیره‌سازی را افزایش می‌دهد. در واقع، با استفاده از برچسب‌های RFID و شبکه‌های حسگر بی‌سیم، هر چیزی می‌تواند بخشی از IoT باشد. در نتیجه تولید حجم زیادی از داده، مدیریت تعداد زیادی از دستگاه‌های IoT به دلیل محدودیت منابع و عدم استفاده این دستگاه‌ها از پروتکل‌های امنیتی استاندارد موجود دشوار می‌باشد. امنیت و حریم خصوصی مهم‌ترین جنبه‌های شبکه اینترنت اشیا هستند که شامل احراز هویت، مجوز، حفاظت از داده‌ها، امنیت شبکه و کنترل دسترسی است. در این مقاله در ابتدا به معرفی روش‌های مختلف احراز هویت در IoT پرداخته و سپس نیازمندی‌های امنیتی و حملات مختلف در اینترنت اشیا مطرح می‌گردد. همچنین روش‌های اخیر احراز هویت و توافق کلید در اینترنت اشیا مورد بررسی قرار می‌گیرند و از نظر هزینه ارتباطی، هزینه محاسباتی و امنیت در برابر حملات مختلف با یکدیگر مقایسه می‌شوند.

کلمات کلیدی: اینترنت اشیاء، احراز هویت، حملات، نیازمندی‌های امنیتی.

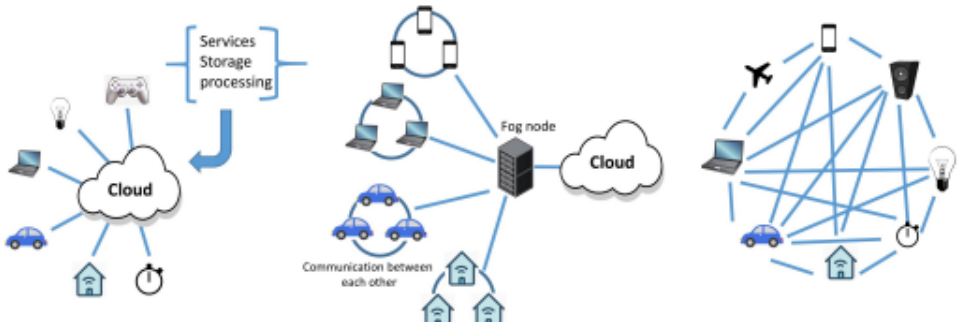
۱ مقدمه

سرعت اتصال دستگاه‌های فیزیکی اطراف ما به اینترنت به سرعت در حال افزایش است. طبق گزارش گارتنر، در سال ۲۰۲۰ حدود ۸٫۴ میلیارد شیء متصل در سراسر جهان وجود دارد. این تعداد در سال ۲۰۲۲، ۴.۲۰ میلیارد شیء برآورد شده است [۱]. شکل (۱) معماری گذشته، حال و آینده IoT را نشان می‌دهد. در آینده انتظار می‌رود که علاوه بر این‌که دستگاه‌ها به اینترنت و سایر دستگاه‌های محلی متصل می‌شوند؛ به طور مستقیم با سایر دستگاه‌ها در اینترنت ارتباط برقرار نمایند. علاوه بر دستگاه‌ها یا اشیائی که به هم وصل می‌شوند، مفهوم اینترنت اشیاء اجتماعی (Social IoT) نیز مطرح می‌باشد. SIoT، کاربران مختلف شبکه‌های اجتماعی را قادر می‌سازد تا به دستگاه‌ها متصل شوند و کاربران می‌توانند دستگاه‌ها را از طریق اینترنت به اشتراک بگذارند [۲].

با وجود طیف گسترده‌ای از برنامه‌های IoT، مسئله امنیت و حریم خصوصی مطرح می‌شود. بدون قابل

اعتماد و تعامل بودن محیط‌های IoT، برنامه‌های در حال ظهور IoT، نمی‌توانند به تقاضاهای زیاد پاسخ دهند و ممکن است تمام پتانسیل‌های خود را از دست بدهند.

در کنار مسائل امنیتی که عموماً در اینترنت، شبکه‌های تلفن همراه و شبکه‌های حسگر بی سیم وجود دارد، IoT نیز دارای چالش‌های امنیتی ویژه خود از جمله موارد مربوط به حریم خصوصی، مسائل احراز هویت، مسائل مربوط به مدیریت شبکه، ذخیره سازی اطلاعات و غیره است.



شکل ۱: معماری گذشته، حال و آینده IoT [۲]

جدول (۱) نشان می‌دهد که برقراری امنیت محیط IoT بسیار سخت‌تر از تأمین امنیت دستگاه‌های عادی فناوری اطلاعات (IT) است[۳].

جدول ۱: معماری گذشته، حال و آینده IoT [۲]

امنیت دستگاه‌های عادی فناوری اطلاعات	امنیت دستگاه‌های اینترنت اشیاء
فناوری اطلاعات دارای دستگاه‌هایی است که از نظر منابع غنی هستند.	دستگاه‌های IoT باید اقدامات امنیتی را با دقت ارائه دهند.
فناوری اطلاعات مبتنی بر دستگاه‌های سرشار از منابع است.	سیستم IoT از دستگاه‌هایی تشکیل شده است که از نظر نرم افزار و سخت افزار محدودیت خود را دارند.
برای امنیت گسترده و قابلیت‌های پایین‌تر الگوریتم پیچیده اجرا شده است.	فقط الگوریتم سبک وزن ترجیح داده می‌شود.
فناوری همگن مسئول امنیت بالا است.	IoT با فناوری ناهمگن مقدار زیادی از داده‌های ناهمگن را افزایش می‌دهد و سطح حمله را افزایش می‌دهد.

با توجه به همه این مسائل و آسیب پذیری‌ها، شبکه‌های IoT؛ در معرض انواع مختلف تهدیدات سایبری قرار دارند. اتحادیه‌ی بین‌المللی مخابرات (ITU) بیان می‌کند که حفاظت از داده‌ها و حریم خصوصی کاربران یکی از چالش‌های اساسی در اینترنت اشیاء است. عدم اطمینان به حریم خصوصی منجر به کاهش پذیرش در میان کاربران می شود [۴]. احراز هویت مسلماً مهم‌ترین بخش امنیت در ارتباطات شبکه‌های IoT است. تأیید اعتبار فرستنده تضمین می‌کند که پیام از طرف فرستنده ادعا شده ارسال و تأیید صحت داده‌ها تضمین

می‌کند که داده های آن فرستنده بدون تغییر بوده است و بنابراین یکپارچگی پیام را نیز فراهم می‌کند [۵]. جدول (۲) خلاصه‌ای از چالش‌های خاص امنیت IoT را نشان می‌دهد.

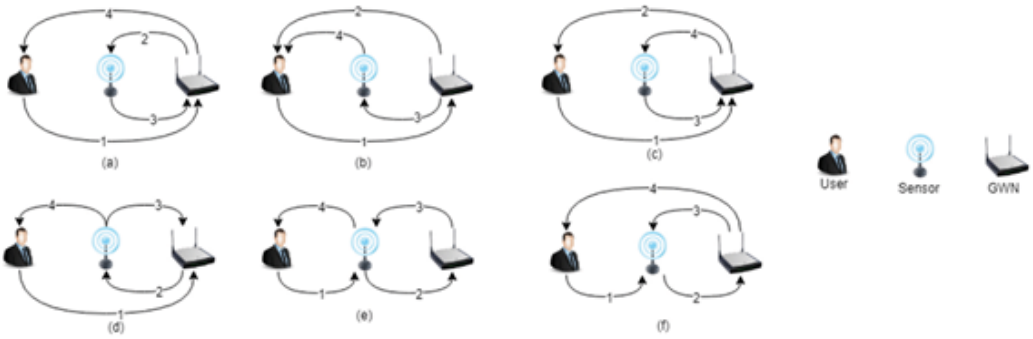
جدول ۲: چالش‌های خاص در امنیت IoT [۳]

چالش‌های مربوط به IoT	مشخصات
حریم خصوصی در تجهیزات IoT	تجهیزات IoT در برابر افشای داده‌های خصوصی کاربران آسیب‌پذیرند.
هزینه و ترافیک	برای کنترل رشد نمایی در دستگاه‌های IoT
بار سنگین در کمبود سرویس و خدمات ابری	سرویس‌های ابری به دلیل حملات، اشکالات در نرم افزار، برق یا سایر مشکلات در دسترس نیستند.
معماری ناقص	تمام قسمت‌های دستگاه‌های IoT دارای نقص هستند که بر شبکه و کل دستگاه تأثیر می‌گذارد.
دستکاری داده‌ها	داده‌ها از دستگاه‌های IoT استخراج می‌شوند و پس از دستکاری، داده‌های آن به روش نامناسب استفاده می‌شود.

روش‌های احراز هویت ارائه شده برای اینترنت اشیاء به شش دسته مطابق شکل (۲) تقسیم می‌شوند [۶]:

در روش اول، کاربر درخواست احراز هویت خود را به دروازه ارسال کرده و سپس دروازه، اطلاعات کاربر را برای نزدیک ترین گره حسگر به کاربر ارسال کرده و دروازه پس از دریافت تایید شدن اطلاعات توسط گره حسگر، پیام تایید احراز هویت را برای کاربر درخواست کننده ارسال می‌نماید. در روش دوم، کاربر درخواست احراز هویت خود را به دروازه ارسال کرده و سپس دروازه، کلید احراز هویت را برای کاربر ارسال می‌کند. در مرحله بعد دروازه اطلاعات کاربر را برای نزدیک ترین گره حسگر به کاربر ارسال کرده و گره حسگر، کاربر را احراز هویت می‌نماید. در روش سوم، کاربر درخواست احراز هویت خود را به دروازه ارسال کرده و سپس دروازه، کلید احراز هویت را برای کاربر و اطلاعات کاربر را برای نزدیکترین گره حسگر به کاربر ارسال می‌کند. در مرحله پایانی گره حسگر، اعتبار کاربر را تایید و اطلاعات اعتبار کاربر به منظور ذخیره شدن در دروازه را برای دروازه ارسال می‌نماید. در روش چهارم، کاربر درخواست احراز هویت خود را به دروازه ارسال کرده و سپس دروازه اطلاعات کاربر را برای نزدیک ترین گره حسگر به کاربر ارسال کرده و گره حسگر با کلیدها به دروازه پاسخ داده و اعتبار کاربر را نیز تایید می‌کند. در روش پنجم، کاربر درخواست احراز هویت خود را برای نزدیک ترین گره حسگر در دسترس ارسال کرده و گره حسگر درخواست کاربر را برای دروازه ارسال می‌کند. دروازه کاربر را احراز هویت نموده و پاسخ را برای گره حسگر می‌فرستد. در مرحله نهایی گره حسگر این پیام را برای کاربر ارسال می‌نماید. در روش ششم، کاربر درخواست احراز هویت خود را برای نزدیک ترین گره حسگر در دسترس ارسال کرده و و گره حسگر درخواست کاربر را برای دروازه ارسال می‌کند. سپس دروازه پیام تایید احراز هویت کاربر را برای کاربر و گره حسگر ارسال می‌نماید.

سازماندهی مقاله به شرح زیر می‌باشد: در بخش دوم دسته بندی انواع روش‌های احراز هویت در اینترنت اشیاء بیان می‌گردد. در بخش سوم و چهارم به ترتیب به بیان نیازمندی‌های امنیتی و تعریف حملات امنیتی می‌پردازیم. در بخش پنجم کارایی و امنیت روش‌های احراز هویت در اینترنت اشیاء مورد بحث قرار می‌گیرد



شکل ۲: روش‌های احراز هویت در اینترنت اشیا [۶]

و در پایان، نتیجه گیری مقاله آورده می‌شود.

۲ مرور روش‌های احراز هویت

در ادامه مقاله، مروری بر روش‌های احراز هویت ارائه شده در اینترنت اشیاء طی سال‌های اخیر انجام می‌گیرد. به منظور فراهم شدن احراز هویت دوطرفه در IoT در سال‌های اخیر روش‌های مختلفی ارائه شده است. روش‌های احراز هویت ارائه شده در IoT شامل چهار گروه به شرح زیر می‌باشند [۶]: (۱) مبتنی بر رمز عبور، (۲) مبتنی بر رمز عبور و توکن (توکن سخت افزاری، کارت هوشمند، دانگل)، (۳) مبتنی بر رمز عبور، توکن و بیومتریک (اثرانگشت، صورت، عنبیه، دست و صدا) که در اصطلاح روش‌های سه فاکتوره نامیده می شود و (۴) روش‌های مبتنی بر رمزنگاری [۶].

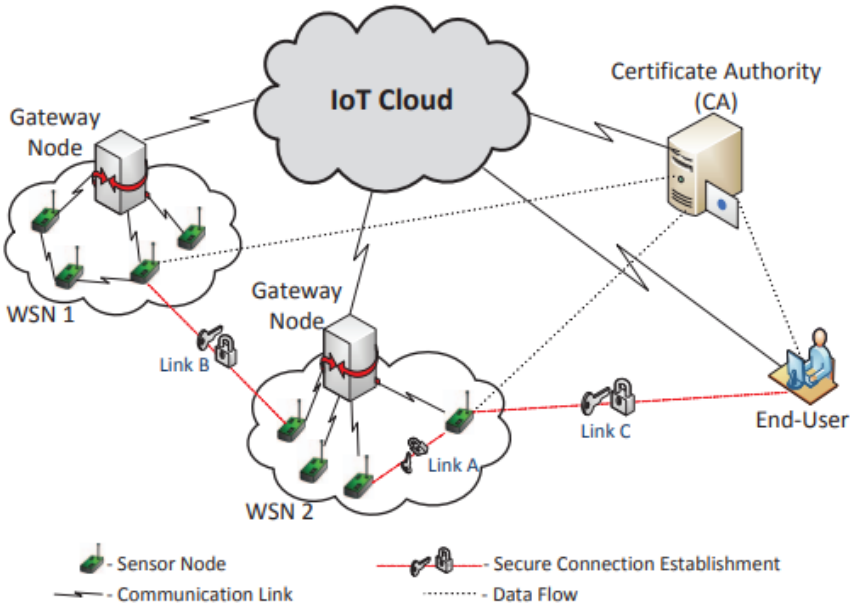
نویسندگان در [۷] طرح احراز هویت کاربر از راه دور مبتنی بر احراز هویت پویا با استفاده از کارت هوشمند را برای تأیید اعتبار کاربران ارائه دادند. نویسندگان به منظور جلوگیری از سرقت شناسه کاربر از شناسه مستعار در روش پیشنهادی خود استفاده کردند. به منظور فراهم شدن امنیت در [۷] نویسندگان از توابع درهم ساز و XOR استفاده نموده اند. Wang و همکاران [۸] یک روش احراز هویت کاربر از راه دور مبتنی بر شناسه پویا، رمز عبور و کارت هوشمند با استفاده از توابع درهم ساز و XOR ارائه دادند. Sood و همکاران در [۹] یک روش بهبود یافته مبتنی بر کارت هوشمند با به کارگیری توابع درهم ساز و XOR ارائه و اثبات کردند که روش ارائه شده در[۸] در برابر حملات دزدیده شدن کارت هوشمند، حمله جعل هویت و حدس رمز عبور به صورت غیر برخط آسیب پذیر است. نویسندگان در [۱۰] اثبات کردند روش ارائه شده در [۹] در معرض حملات کاربر مخرب، مرد میانی و دزدیده شدن اطلاعات پایگاه داده است و یک روش جدید احراز هویت را ارائه نمودند که در آن به جای همگام سازی زمان از اعداد تصادفی استفاده شده و سرور نیازی به حفظ جدول تایید ندارد. مراحل روش آن‌ها شامل ثبت نام، ورود به سیستم، تایید و توافقنامه کلید جلسه و تغییر رمز عبور می‌باشد. نویسندگان در [۱۱] طرحی را ارائه دادند که در آن گره حسگر و کاربر می‌توانند بدون نیاز به دروازه، هویت خود را به طور متقابل تایید و برای شبکه‌های حسگر دارای محدودیت منابع، مناسب است. معماری شبکه مورد نظر در شکل (۳) نشان داده شده است، دستگاه‌های لبه شبکه (به عنوان

مثال، گره‌های حسگر) و کاربران نهایی، اعتبارنامه‌ها و گواهی‌های امنیتی را از مرجع صدور گواهی (CA) درخواست می‌کنند. در روش احراز هویت ارائه شده توسط آن‌ها؛ ابتدا کاربر به منظور دریافت گواهی در مرجع صدور گواهی ثبت نام کرده و سپس در مرحله احراز هویت، ارتباطات بین کاربر و گره حسگر انجام می‌شود (دو مرحله). در روش پیشنهادی ارائه شده از ضرب و جمع نقطه‌ای روی منحنی استفاده شده و کلید نهایی مورد توافق طرفین براساس ضرب نقطه‌ای روی منحنی بیضوی ساخته می‌شود. نویسندگان در [۱۲] نشان دادند روش [۱۱] در برابر حملات مرد میانی، منع سرویس، حمله شخص داخلی و تکرار آسیب پذیر می‌باشد و گمنامی کاربر را حفظ نمی‌کند و از این رو یک روش جدید سه فاکتوره مطابق روش اول شکل (۳) ارائه نمودند. امنیت روش پیشنهادی آن‌ها با استفاده از XOR، توابع درهم ساز و روش متقارن AES-128 فراهم شده است.

نویسندگان در [۱۳] یک پروتکل احراز هویت متقابل مبتنی بر منحنی بیضوی دارای سه مرحله ثبت نام، ورود و احراز هویت؛ برای ارتباط ایمن دستگاه‌های تعبیه شده و سرورهای ابری با استفاده از کوکی‌های پروتکل انتقال متن (HTTP) پیشنهاد دادند و برای اثبات امنیت روش ارائه شده از ابزار رسمی اویسپا استفاده نمودند. در [۱۴] نویسندگان نشان دادند روش ارائه شده در [۱۳] در برابر حملات حدس رمز عبور غیر بر خط، دزده شدن اطلاعات تایید کننده و شخص داخلی آسیب پذیر است و نیازمندی‌های امنیتی گمنامی کاربر، توافق کلید نشست و احراز هویت دو طرفه را فراهم نمی‌کند؛ از این رو یک روش دو فاکتوره سه مرحله‌ای مبتنی بر منحنی بیضوی جدید با حفظ محرمانگی شناسه کاربر را ارائه دادند. نویسندگان در[۱۵] ایرادات امنیتی حمله دزدیده شدن تایید کننده‌ها، لو رفتن پارامترهای تصادفی، حمله تکرار و منع سرویس را به روش مقاله [۱۵] وارد کردند و به منظور رفع ایرادات مطرح شده و فراهم کردن امنیت از XOR و توابع درهم ساز استفاده نمودند و در آن از مهر زمانی به منظور جلوگیری از حمله تکرار استفاده کردند. در روش ارائه شده توسط آن‌ها هیچ شناسه‌ای به صورت آشکار در مرحله احراز هویت در کانال عمومی ارسال نمی‌شود در نتیجه گمنامی را نیز فراهم آورده‌اند.

نویسندگان در [۱۶] نشان دادند روش [۱۵] در برابر حدس رمز عبور آسیب پذیر می‌باشد. در [۱۷] نویسندگان یک روش احراز هویت دارای گمنامی برای محیط خانه‌های هوشمند براساس رمزنگاری منحنی بیضوی ارائه نمودند که طرح آن‌ها نیازی به ذخیره جدول تایید برای احراز هویت ندارد. مراحل تبادل پیام در پروتکل ارائه شده توسط آن‌ها مطابق مورد اول شکل (۳) می‌باشد. نویسندگان در [۱۸] نشان دادند روش ارائه شده در [۱۷] از نظر هزینه‌های محاسباتی و ارتباطی مناسب نمی‌باشد و روش احراز هویتی براساس توابع درهم ساز با حفظ گمنامی برای خانه‌های هوشمند ارائه دادند. به منظور رفع مشکل هزینه محاسباتی و ارتباطی روش‌های گذشته، نویسندگان در [۱۹] یک روش سه فاکتوره سبک وزن احراز هویت کاربر برای محیط IoT بر مبنای رمزنگاری منحنی بیضوی ارائه کردند و امنیت روش ارائه شده را با نرم افزار اویسپا اثبات نمودند. در مقاله ارائه شده، مهم‌ترین چالش‌های مورد نیاز برای برقراری ارتباط امن بین محیط اینترنت اشیاء و کاربر، به شرح زیر عنوان شده است:

- الزامات هویت: هویت سیستم اینترنت اشیاء و کاربر باید تایید شود. (احراز هویت)

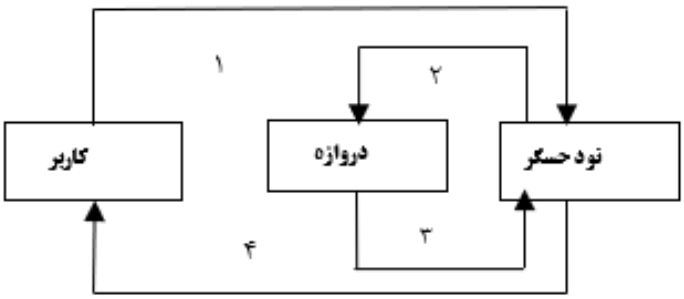


شکل ۳: معماری شبکه در مقاله [۱۱]

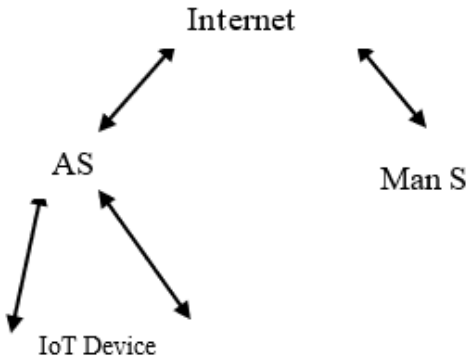
- الزامات حریم خصوصی: اهمیت حفظ محرمانه بودن داده‌های مبادله شده بین سیستم اینترنت اشیاء و کاربر.
- الزامات اعتماد: اهمیت مدیریت اعتماد، هدف اصلی محیط اینترنت اشیاء، بین فرستنده و گیرنده.

در پروتکل پیشنهادی آن‌ها، شبکه اینترنت اشیاء به چهار پیام متوالی برای برقراری ارتباط بین هر یک از شرکت کنندگان (کاربر راه دور، گره حسگر، دروازه) شبکه نیاز دارد. کاربر راه دور می‌تواند با گره حسگر برای احراز هویت متقابل تماس بگیرد و سپس در مرحله دوم گره با دروازه برای احراز هویت ارتباط برقرار می‌کند. پس از احراز هویت موفق، گره حسگر مستقیماً داده‌ها را به کاربر منتقل می‌کند (روش پنجم در شکل (۲)). روش ارائه شده در [۱۹]شامل پنج مرحله‌ی برپایی، ثبت‌نام (ثبت نام کاربر در دروازه و ثبت نام گره IoT در دروازه)، احراز هویت و توافق کلید، تغییر رمز عبور و آپدیت کلید متقارن می‌باشد. شکل (۴) نشان دهنده مراحل تبادل پیام در روش آن‌ها می‌باشد.

در مقاله [۲۰] نویسندگان یک روش احراز هویت با تبادل شش پیام در سه مرحله متوالی ارائه نمودند. این طرح از تابع درهم ساز HMAC برای ارائه احراز هویت متقابل و تابع رمزنگاری متقارن AES برای ارائه یکپارچگی و محرمانه بودن داده‌های مبادله شده استفاده می‌کند. طرح پیشنهادی از پروتکل UDP استفاده می‌کند که در مقایسه با پروتکل TCP، سربار کمتری را از نظر مصرف انرژی و باتری نشان می‌دهد. در این مقاله به ارائه محدودیت‌های روش‌های احراز هویت در IoT پرداخته و بیان می‌دارد اکثر طرح‌های پیشنهادی دارای مقادیر زیادی هزینه‌های ارتباطی و محاسباتی بوده و این نشان از شکست این طرح‌ها در ارائه احراز



شکل ۴: مراحل تبادل پیام در روش احراز هویت مقاله [۱۹]



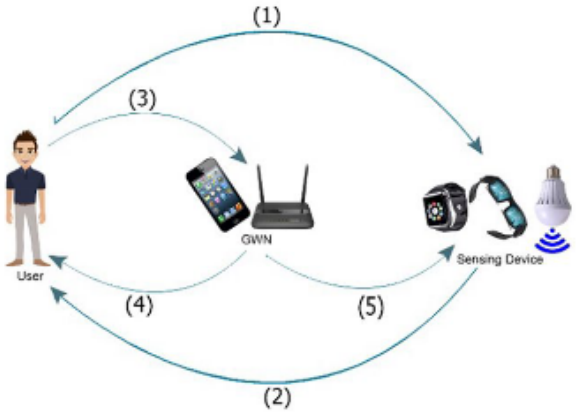
شکل ۵: معماری کلی سیستم مقاله [۲۰]

هویت قوی مورد نیاز است، زیرا دستگاه IoT دستگاهی با محدودیت منابع است. در طرح پیشنهادی آن‌ها، موجودیت‌های درگیر شامل: دستگاه‌های اینترنت اشیاء، سرور سازنده اینترنت اشیاء و سرور احراز هویت (AS) بوده که سرور AS می‌تواند خود دروازه اینترنت اشیاء باشد و Man.S تولید کننده دستگاه اینترنت اشیاء است. در روش ارائه شده فرض شده است که حملات تنها از نوع نرم افزاری بوده و حملات فیزیکی وجود ندارند. معماری کلی روش پیشنهادی آن‌ها در شکل (۵) نشان شده است:

یک پروتکل ساده احراز هویت و توافق کلید برای اینترنت اشیاء ناهمگن با توجه ویژه به دستگاه‌های حسگر و دروازه در [۲۱] ارائه شده است که در آن دروازه به عنوان یک مرجع قابل اعتماد با حداکثر حجم کار و دستگاه‌های حسگر با بالاترین محدودیت منابع در پروتکل پیشنهادی در نظر گرفته شده است. در این روش برای ایجاد امنیت از توابع درهم‌ساز استفاده شده است. اعتبارسنجی روش پیشنهادی از منطق BAN (Burrows–Abadi–Needham) و برای نشان دادن انعطاف‌پذیری در برابر حملات فعال موجود از ابزار

اعتبارسنجی اویسپا استفاده شده است. معماری کلی روش پیشنهادی آن‌ها در شکل (۶) نشان داده شده است: در این روش، کاربر، درخواست ارتباطی را به دستگاه حسگر ارسال می‌کند (مرحله ۱) و پس از دریافت پاسخ (مرحله ۲)، کاربر درخواست مشابه آنچه به دستگاه حسگر ارسال کرده را به دروازه ارسال می‌کند (مرحله ۳). دروازه درخواست را تأیید می‌کند و به طور جداگانه پاسخ احراز هویت را به کاربر برمی گرداند (مرحله ۴). در روش آن‌ها هدف حداقل کردن دخالت دستگاه‌های حسگر و دروازه به دلیل منابع محدود و حجم کاری سنگین است. روش پیشنهادی در[۲۱] شامل چهار مرحله است: مرحله ثبت (ثبت نام دستگاه حسگر و ثبت نام کاربر توسط دروازه در شبکه)، مرحله احراز هویت و توافق کلید، مرحله تغییر رمز عبور و اطلاعات بیومتریک و مرحله فعال سازی/تغییر نام کاربری می‌باشد. نویسندگان در [۲۲] یک روش جدید احراز هویت مبتنی بر چندجمله‌ای چبیشف (Chebyshev) ارائه دادند و در آن ادعا کردند عملکرد روش پیشنهادی آن‌ها بهتر بوده و میزان استفاده از حافظه و انرژی با عنایت به محدودیت تجهیزات IoT در مقایسه با سایرین کمتر می‌باشد. اثبات امنیت روش پیشنهادی آن‌ها با منطق BAN و ابزار Scyther انجام گرفته است. در این مقاله اشاره می‌شود که اکثر روش‌های احراز هویت در شبکه IoT شامل سه موجودیت، یعنی دروازه، دستگاه هوشمند و کاربر است. چهار گروه روش‌های احراز هویت در IoT وجود داشته که عبارتند از: رویکرد کاربر–دروازه–دستگاه، رویکرد کاربر–دستگاه–دروازه، رویکرد دستگاه به دستگاه و رویکرد مبتنی بر آشوب. در رویکردهای کاربر–دروازه–دستگاه، دستگاه به طور مستقیم در دسترس کاربر نیست اما مستقیماً با دروازه برای احراز هویت در تعامل است. مکانیسم‌های مختلف احراز هویت مبتنی بر پروتکل‌های رمزنگاری متقارن و مبتنی بر کلید عمومی در پیاده‌سازی این رویکرد به کار گرفته می‌شود. در رویکرد کاربر–دستگاه–دروازه، کاربر مستقیماً با دستگاه‌ها در تعامل است. اعتبار محرمانه کاربر توسط دروازه از طریق دستگاه‌ها ارسال و تایید می‌شود. نویسندگان با تاکید بر محدودیت منابع در اینترنت اشیاء روش مبتنی بر آشوب را ارائه داده که در روش آن‌ها فرآیند احراز هویت از هیچ کلید از پیش ثبت‌شده مشترکی توسط دروازه‌ها استفاده نمی‌کند و از همان مکانیسم مبتنی بر چند جمله‌ای چبیشف برای اجرای احراز هویت متقابل بین دستگاه و دروازه استفاده می‌شود.

یک روش اینترنت اشیاء اجتماعی صنعتی (IIoT) مبتنی بر مه در [۲۳] ارائه شده است که در آن احراز هویت متقابل، ناشناس بودن و ارتباط ایمن را از طریق توافق نامه کلید اعتماد بین اشیاء هوشمند اجتماعی و با استفاده از تابع درهم ساز، عملیات XOR و رمزنگاری متقارن برقرار می‌کند. این طرح به دلیل کاهش هزینه‌های سربار محاسباتی برای IIoT دارای محدودیت منابع، مناسب ذکر شده است. امنیت روش آن‌ها با منطق BAN و ابزار اویسپا اثبات شده است. در روش آن‌ها دستگاه‌های IoT همتا با پروفایل‌های اجتماعی مشابه در حال ارتباط از طریق سرور مه هستند. طرح پیشنهادی، ارتباط امنی را بین دستگاه‌های مورد اعتماد IIoT براساس مشخصات اجتماعی آن‌ها فراهم می‌کند. سه موجودیت روش آن‌ها شامل: یک مرجع سرور ابری، یک مرجع اعتماد است که حاوی یک سرور تولیدکننده کلید خصوصی بوده و دارای پایگاه داده حاوی تمام هویت‌های واقعی و قالب درهم شده هویت تجهیزات هوشمند و سرورهای مه می‌باشد. سرور مه؛ سروری که در لایه مه شبکه قرار دارد و تطبیق پروفایل اجتماعی و رویه احراز هویت بین تجهیزات هوشمند را تضمین می‌کند. تجهیزات هوشمند: نهادهای واقع در لبه شبکه بوده که آن‌ها می‌توانند تجهیزات هوشمند،



شکل ۶: مدل پیشنهادی تبادل پیام برای احرازهویت مقاله [۲۱]

ربات‌های صنعتی هوشمند، حسگرها، دوربین‌های نظارتی و غیره باشند.

در ادامه مقاله در ابتدا به معرفی نیازمندی‌های امنیتی و تعریف حملات در IoT پرداخته و سپس روش‌های احراز هویت ارائه شده در IoT را از نظر امنیت و کارایی با یکدیگر مقایسه می‌نماییم.

۳ نیازمندی‌های امنیتی

محرمانگی پیش رو (Perfect Forward Secrecy): تضمین می‌کند حتی اگر اطلاعات بلند مدت استفاده شده در طول تبادل کلید جلسه مانند کلید خصوصی سرور یا رمز عبور کاربر به سرقت رفته باشد، کلیدهای جلسه تحت تأثیر قرار نخواهند گرفت [۲۴].

احراز هویت متقابل (Mutual authentication): ضروری ترین نیازمندی امنیتی است زیرا طرفین ارتباط باید یکدیگر را برای برقراری ارتباط امن احراز هویت کنند [۱۳]. احراز هویت متقابل از طریق ارائه یک قطعه اطلاعات محرمانه که فقط در اختیار طرفین ارتباط قرار می‌گیرد، به دست می‌آید.

محرمانه بودن (Confidentiality): محرمانه بودن با به حداقل رساندن تعداد پیام‌های متنی ساده و با اطمینان از اینکه هیچ اطلاعات قابل استفاده‌ای توسط استراق سمع غیرمجاز قابل خواندن نیست، به دست می‌آید. معمولا در روش‌های ارائه شده؛ محرمانگی با استفاده از رمزنگاری و توابع درهم ساز در ارسال پیام در کانال عمومی انجام می‌شود [۱۳].

تمامیت و یکپارچگی (Integrity): اطمینان از هویت طرف مقابل ارتباط.

گمنامی/ناشناس بودن: عدم ارسال شناسه کاربر/دستگاه به صورت متن آشکار در کانال عمومی. ناشناس بودن به این معنی است که مهاجم نباید بتواند هویت دستگاه اینترنت اشیاء/کاربر را بدست آورد. به طور خاص، اگر مهاجم پیام‌های رد و بدل شده بین دستگاه IoT و سرور را استراق سمع کند، نباید بتواند شناسه دستگاه تعبیه‌شده/کاربر را بدست آورد[۱۵].

محرمانگی در روش‌های سه عاملی: پروتکل‌هایی که به سه عامل امنیتی در فرآیند پی راستی‌آزمایی نیاز دارند، حتی در صورت افشای دو عامل باید ایمن باقی بمانند [۲۱]

شناسایی سریع برای ورود غیرمجاز: مکانیزم تشخیص برای ورود غیر مجاز به دستگاه اجازه می‌دهد تا ورود غیرمجاز را در زمانی که کاربر اطلاعات اشتباه وارد می‌کند، رد کند و در شروع مرحله ورود و احراز هویت، هزینه‌های ارتباطی و محاسباتی غیر ضروری را کاهش می دهد [۱۵].

۴ تعریف حملات در اینترنت اشیاء

حمله مرد میانی (man in the middle) MITM: اگر مهاجم در مرحله احراز هویت ما بین دو موجودیت قانونی قرار بگیرد و بتواند با شنود کانال عمومی به سرقت اطلاعات محرمانه پرداخته و یا با کمک حمله دیگر؛ کلید جلسه را بیابد. گاهی مهاجم با کمک این حمله؛ هویت موجودیت‌های قانونی را جعل می‌نماید.

حمله تکرار: در این حمله مهاجم پیام‌های ارسالی گذشته بین دو موجودیت را باز ارسال می‌کند و با انجام این عمل و صرف وقت و منابع از موجودیت مقابل باعث حمله منع سرویس می‌گردد.

حمله جعل هویت گره IoT: در این حمله مهاجم سعی دارد خود را به عنوان گره قانونی IoT معرفی کرده و ارتباطات را به جای او با سایر موجودیت‌ها برقرار نماید.

دزدیده شدن یا گم شدن کارت هوشمند: اگر کارت هوشمند کاربر به سرقت برود و مهاجم با حملات تحلیل توان قادر به استخراج اطلاعات آن باشد.

حمله تشخیص رمز عبور غیر بر خط: در این حمله مهاجم می‌تواند به راحتی رمز عبور را در زمان چند جمله ای با استفاده از brute force حدس بزند، یا ممکن است رمز عبور را در هر حالت غیر برخط رهگیری کند.

حمله جعل هویت دروازه: مهاجم ممکن است با ادعای دروغین خود را به عنوان یک دروازه معتبر معرفی کرده و سعی نماید پیام ارسال شده را به عنوان پیام معتبر از دروازه اصلی معرفی نماید [۱۹].

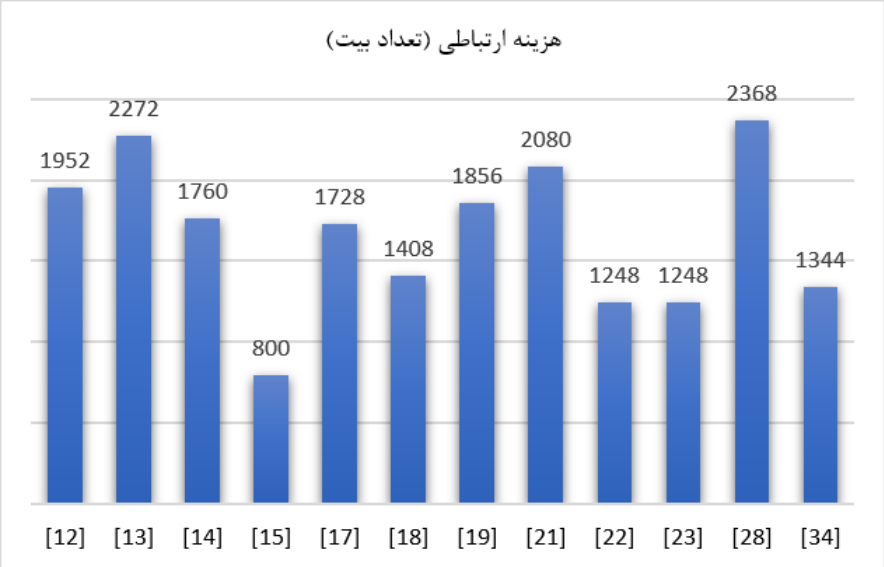
حمله دور زدن دروازه: به معنی دور زدن فرایند احراز هویت است.

حمله‌ی افشای پارامترهای تصادفی جلسه (Known-session-specific temporary information attack): فرض در این حمله بر این است که اگر تمام پارامترهای تصادفی یک جلسه (شامل اعداد تصادفی و مهر زمانی) افشا شوند نباید امنیت کلید آن جلسه به خطر بیفتد [۳۱]، [۲۵].

حمله به گمنامی کاربر و قابلیت پیگیری (traceability): مهاجم با رهگیری پیام‌های ارسالی بر روی کانال عمومی هویت کاربر را یافته و فعالیت‌های انجام شده او را پیگیری نماید [۳۲].

حمله جلسه موازی: اگر مهاجم درخواست ورود یک کاربر معتبر حاوی شناسه و رمزعبور کاربر را دریافت کند و بر این اساس یک جلسه موازی را آغاز کند، این حمله رخ می‌دهد. برای جلوگیری از این حمله از پارامتر بیومتریک کاربر نیز به عنوان فاکتور احراز هویت استفاده شده که قابلیت جعل را ندارد و منحصر بفرد است [۱۹].

حمله تجزیه و تحلیل خطا: یک ابزار قدرتمند برای استخراج اطلاعات مخفی به طور جزئی یا کامل با بهره



شکل ۷: مقایسه هزینه ارتباطی روش‌های ارائه شده در IoT

برداری از خطاهای رخ داده در پیاده سازی سیستم رمزنگاری است و عمدتاً برای حمله به سیستم رمزنگاری مانند سیستم‌های رمز پایه منحنی بیضوی و سیستم رمزنگاری RSA استفاده می‌شود [۱۷].

حمله گره شبیه سازی شده: حمله ای به دستگاه‌های اینترنت اشیاء است که به طور خاص مکانیسم احراز هویت را هدف قرار می‌دهد. این حمله به عنوان حمله تکراری دستگاه یا حمله شبیه سازی دستگاه نیز شناخته می‌شود. از آنجایی که یک گره شبیه سازی شده به تمام اطلاعات محرمانه (کدها و کلیدهای احراز هویت) دسترسی دارد، مانند گره‌های قانونی رفتار می‌کند [۳۳].

۵ مقایسه‌ی امنیت و کارایی روش‌های احراز هویت

برای ارزیابی کارایی از مقادیر گزارش شده در مقاله [۳۴] و همچنین مجموعه نمادهای تعریف‌شده $T_{ECM}, T_{eca}, T_{sed}, T_h, T_{fe}, T_{exp}, T_{pke}, T_{pkd}$ به‌ترتیب برای نشان دادن زمان ضرب نقطه‌ای روی منحنی بیضوی (0.063075 s)، زمان عملیات جمع نقطه‌ای روی منحنی بیضوی (0.010875 s)، زمان رمزنگاری و رمزگشایی متقارن (0.0087 s)، زمان توابع درهم‌ساز (0.0005 s)، عملیات استخراج فازی (0.063075 s)، زمان مورد نیاز برای توان ماژولار(0.522 s)، زمان رمزگذاری کلید عمومی و رمزگشایی(0.87 s)، استفاده شده است. هزینه‌های ارتباطی، تعداد پیام‌های مبادله شده و تعداد کل بیت‌ها برای احراز هویت متقابل موفق در مرحله احراز هویت و توافق کلید بوده و براساس مقادیر ارائه شده در مقاله [۳۵] برای ارسال شناسه و اعداد تصادفی ۱۲۸ بیت، مهر زمانی ۳۲ بیت، خروجی توابع درهم ساز ۱۶۰ بیت و حاصل رمزنگاری/رمزگشایی متقارن ۱۲۸ بیت در نظر گرفته شده است. براساس مقاله [۱۴] هزینه ارسال پارامتر ساخته شده براساس منحنی بیضوی نیز ۳۲۰ بیت می‌باشد. در جدول شماره (۳)، هزینه محاسباتی برخی از روش‌های احراز

هویت ارائه شده در IoT ذکر شده است. مقایسه‌ی هزینه ارتباطی (ارسال پیام در کانال عمومی) روش‌های احرازهویت IoT در نیز در شکل ۷ نمایش داده شده است. در جدول شماره (۴)، حملات وارد به روش‌های احراز هویت در IoT بیان شده است. در این جدول * به معنای وارد بودن آن حمله و - به معنای وارد نبودن حمله می‌باشد.

جدول ۳: مقایسه هزینه محاسباتی روش‌های ارائه شده در IoT

مرجع	هزینه محاسباتی (ثانیه)
[۱۲]	$۱۹T_h + ۸T_{\text{sed}}$
[۱۳]	$۹T_h + ۷T_{\text{ecm}}$
[۱۴]	$۷T_h + ۸T_{\text{ecm}}$
[۱۷]	$۱۶T_h + ۳T_{\text{ecm}}$
[۱۸]	$۱۲T_h$
[۱۹]	$۵T_h + ۲T_{\text{ecm}} + ۸T_{\text{sed}}$
[۲۱]	$۲۹T_h$
[۲۲]	$۲۰T_h$
[۲۳]	$۱۱T_h + ۱T_{\text{sed}}$
[۱۵]	$۱۸T_h + ۶T_{\text{sed}}$
[۲۸]	$۲۱T_h + ۲T_{\text{ecm}}$
[۳۴]	$۵T_h + ۶T_{\text{ecm}} + ۴T_{\text{sed}}$

۶ نتیجه‌گیری

در این مقاله در ابتدا به انواع روش‌های احراز هویت در اینترنت اشیاء اشاره و در ادامه نحوه‌ی تبادل پیام بین موجودیت‌های مختلف شرکت کننده در فرآیند احراز هویت بیان گردید. در بخش سوم و چهارم مقاله، نیازمندی‌های امنیتی و حملات رایج در پروتکل‌های احراز هویت اینترنت اشیاء شرح داده شد. در پایان

جدول ۴: بررسی حملات وارده به روش‌های احراز هویت در IoT

مرجع	[۷]	[۸]	[۹]	[۱۱]	[۱۳]	[۱۴]	[۱۸]	[۱۹]	[۲۸]	[۳۲]
تکرار	–	–	–	*	–	*	–	–	–	*
مرد میانی	–	–	*	*	–	–	–	–	–	–
لو رفتن پارامتر تصادفی	–	–	–	–	–	*	*	*	–	*
جعل هویت	*	*	–	–	–	–	–	–	*	*
سرقت اطلاعات تاییدکننده‌ها	*	*	*	–	*	*	–	–	–	*
شکست در گمنامی	–	–	–	*	*	–	–	*	*	*
شکست در احراز هویت متقابل	*	–	–	–	*	–	–	–	–	–
حمله شخص داخلی	–	–	*	*	*	–	–	–	*	–
حدس رمز عبور غیر بر خط	–	*	–	–	*	–	–	–	–	–

روش‌های احراز هویت از نظر هزینه‌های محاسباتی و ارتباطی مقایسه و انواع حملات به آن‌ها نیز ارزیابی شد.

مراجع

[1] R. Kandaswamy and D. Furlonger. Blockchain-Based Transformation. Accessed: Jun. 5, 2018. [Online]. Available: https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insightreport/

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges", *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, Aug. 2018, doi: 10.1109/jiot.2017.2767291.

[3] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures", *IEEE Access*, vol. 7, pp. 82721–82743, Jan. 2019, doi: 10.1109/access.2019.2924045.

[4] N. L. Li, "Study on security architecture in the Internet of Things", *Proceedings of 2012 International Conference on Measurement, Information and Control*, May 2012, doi: 10.1109/mic.2012.6273274.

[5] O. Bamasag and K. Y. Toumi, "Efficient multicast authentication in internet of things", *IEEE Xplore*, Oct. 2016, doi: 10.1109/ictc.2016.7763512.

[6] T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism", *IEEE Access*, vol. 7, pp. 151054–151089, Jan. 2019, doi: 10.1109/access.2019.2947723.

[7] M. L. Das, A. Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629–631, May 2004, doi: 10.1109/tce.2004.1309441.

[8] Y.-Y. Wang, J.-Y. Liu, F.-X. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", *Computer Communications*, vol. 32, no. 4, pp. 583–585, Mar. 2009, doi: 10.1016/j.comcom.2008.11.008.

[9] S. K. Sood, A. K. Sarje, and K. Singh, "An improvement of Xu et al.'s authentication scheme using smart cards", Jan. 2010, doi: https://doi.org/10.1145/1754288.1754303.

[10] R. Martínez-Peláez, F. Rico-Novella, J. Forné, and P. Velarde-Alvarado, "Security improvement of two dynamic ID-based authentication schemes by Sood-Sarje-Singh", *Journal of Applied Research and Technology*, vol. 11, no. 5, pp. 755–763, Oct. 2013, doi: 10.1016/s1665-6423(13)71583-9.

[11] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications", *IEEE Xplore*, Apr. 2014, doi: 10.1109/wcnc.2014.6952860.

[12] K. Chatterjee, A. Singh, N. Neha, and K. Yu, "A Multifactor Ring Signature based Authentication Scheme for Quality Assessment of IoMT Environment in COVID-19 Scenario", *Journal of Data and Information Quality*, vol. 15, no. 2, pp. 1–24, Jun. 2023, doi: 10.1145/3575811.

[13] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers", *Pervasive and Mobile Computing*, vol. 24, pp. 210–223, Dec. 2015, doi: 10.1016/j.pmcj.2015.08.001.

[14] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers", *The Journal of Supercomputing*, vol. 74, no. 12, pp. 6428–6453, Apr. 2017, doi: 10.1007/s11227-017-2048-0.

[15] M. Nikooghadam and H. Amintoosi, "Secure communication in CloudIoT through design of a lightweight authentication and session key agreement scheme", *International Journal of Communication Systems*, vol. 36, no. 1, Feb. 2020, doi: 10.1002/dac.4332.

[16] M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "An ensemble learning based intrusion detection model for industrial IoT security", *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 273–287, Sep. 2023, doi: 10.26599/bdma.2022.9020032.

[17] M. Shuai, N. Yu, H. Wang, and L. Xiong, "Anonymous authentication scheme for smart home environment with provable security", *Computers & Security*, vol. 86, pp. 132–146, Sep. 2019, doi: 10.1016/j.cose.2019.06.002.

[18] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment", *Internet of Things*, vol. 9, p. 100158, Mar. 2020, doi: 10.1016/j.iot.2020.100158.

[19] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography", *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114–1151, May 2020, doi: 10.1007/s11227-020-03318-7.

[20] I. Alshawish and A. Al-Haj, "An efficient mutual authentication scheme for IoT systems", *The Journal of Supercomputing*, vol. 78, no. 14, pp. 16056–16087, Apr. 2022, doi: 10.1007/s11227-022-04520-5.

[21] R. Hajian, S. H. Erfani, and S. Kumari, "A lightweight authentication and key agreement protocol for heterogeneous IoT with special attention to sensing devices and gateway", *The Journal of Supercomputing*, vol. 78, no. 15, pp. 16678–16720, May 2022, doi: 10.1007/s11227-022-04464-w.

[22] R. Krishnasrija, A. Kr. Mandal, and A. Cortesi, "A lightweight mutual and transitive authentication mechanism for IoT network", *Ad Hoc Networks*, vol. 138, p. 103003, Jan. 2023, doi: 10.1016/j.adhoc.2022.103003.

[23] A. B. Amor, S. Jebri, M. Abid, and A. Meddeb, "A secure lightweight mutual authentication scheme in Social Industrial IoT environment", *The Journal of Supercomputing*, vol. 79, no. 12, pp. 13578–13600, Mar. 2023, doi: 10.1007/s11227-023-05176-5.

[24] V. Thakur, G. Indra, N. Gupta, P. Chatterjee, O. Said, and A. Tolba, "Cryptographically secure privacy-preserving authenticated key agreement protocol for an IoT network: A step towards critical infrastructure protection", *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 206–220, Sep. 2021, doi: 10.1007/s12083-021-01236-w.

[25] N. Ravanbakhsh, M. Mohammadi, and M. Nikooghadam, "Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme", *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11129–11153, Sep. 2018, doi: 10.1007/s11042-018-6620-2.

[26] M. Luo, Y. Wen, and H. Zhao, "An Enhanced Authentication and Key Agreement Mechanism for SIP Using Certificateless Public-key Cryptography", *2008 the 9th International Conference for Young Computer Scientists*, Nov. 2008, doi: 10.1109/icycs.2008.311.

[27] M. Sarvabhatla, M. C. M. Reddy, and C. S. Vorugunti, "A robust remote user authentication scheme resistant to known session specific temporary information attack", *IEEE Xplore*, Feb. 2015, doi: 10.1109/aimoc.2015.7083847.

[28] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments", *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, Feb. 2018, doi: 10.1016/j.jnca.2017.07.001.

[29] M. Nikooghadam, H. Amintoosi, and S. Kumari, "A provably secure ECC-based roaming authentication scheme for global mobility networks", *Journal of Information Security and Applications*, vol. 54, p. 102588, Oct. 2020, doi: 10.1016/j.jisa.2020.102588.

[30] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, "Robust session key generation protocol for social internet of vehicles with enhanced security provision", *The Journal of Supercomputing*, vol. 77, no. 3, pp. 2511–2544, Jun. 2020, doi: 10.1007/s11227-020-03363-2.

[31] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems", *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, Aug. 2019, doi: 10.1007/s10207-019-00464-9.

[32] A. Kumar, K. Abhishek, X. Liu, and A. Haldorai, "An efficient Privacy-Preserving ID centric authentication in IoT based cloud servers for sustainable smart cities", *Wireless Personal Communications*, vol. 117, no. 4, pp. 3229–3253, Nov. 2020, doi: 10.1007/s11277-020-07979-8.

[33] K. Hameed, S. Garg, M. B. Amin, B. Kang, and A. Khan, "A context-aware information-based clone node attack detection scheme in Internet of Things", *Journal of Network and Computer Applications*, vol. 197, p. 103271, Jan. 2022, doi: 10.1016/j.jnca.2021.103271.

[34] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-COAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things", *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867–1896, Sep. 2020, doi: 10.1007/s11277-020-07769-2.

[35] U. Chatterjee, S. Ray, M. K. Khan, M. Dasgupta, and C.-M. Chen, "An ECC-based lightweight remote user authentication and key management scheme for IoT communication in context of fog computing", *Computing*, vol. 104, no. 6, pp. 1359–1395, Feb. 2022, doi: 10.1007/s00607-022-01055-8.