یک معماری کارآمد و مبتنی بر ابر برای بهبود عملکرد شبکه هوشمند برق

محمد رسول مومنی[۱] - فاطمه حقیقت[۱] - محسن حقیقت[۲]
(۱) کارشناس ارشد - دانشکده فنی و مهندسی، دانشگاه گلپایگان، گلپایگان، ایران
(۲) کارشناس ارشد، شرکت توزیع نیروی برق تهران بزرگ، تهران، ایران

تاریخ دریافت: ۹۸/۵/۸ تاریخ پذیرش: ۹۸/۷/۲۰

خلاصه: رشد چشمگیر مشترکین، افزایش روزافزون تقاضای انرژی و همچنین نیاز به بالا بردن بهره‌وری و حفظ پایداری شبکه برق، شبکه هوشمند برق را تنها گزینه پیش روی متخصصان این حوزه قرار داده است. در واقع شبکه هوشمند برق یک سامانه فیزیکی- سایبری است که کارکردهای ارتباطی، پردازشی و کنترلی را به صورت یکپارچه و منسجم ارائه می‌دهد. شبکه هوشمند برق کنترل و مدیریت میلیون‌ها دستگاه در صنعت برق را به شیوه‌ای مطمئن، مقیاس‌پذیر و مقرون به صرفه به صورت بلادرنگ و دوطرفه فراهم می‌نماید. با توجه به رشد فزاینده تهدیدات سایبری در دهه اخیر، لزوم حفاظت از صنعت برق و سامانه‌های حیاتی آن بسیار ضروری به نظر می‌رسد. کوچک‌ترین اختلال در سامانه‌های صنعت برق منجر به بروز وقفه در عملکرد سایر صنایع، کاهش بهره‌وری و بروز نارضایتی می‌گردد. از این رو در این مقاله یک معماری کارای مبتنی بر فناوری رایانش ابری برای بهبود عملکرد در شبکه هوشمند برق ارائه شده است. معماری پیشنهادی با به کارگیری سیستم رمزنگاری منحنی بیضوی قادر به تأمین امنیت و حریم خصوصی داده‌ها در برابر انواع مختلف حملات سایبری نظیر حمله تکرار، تغییر و غیره می‌باشد.
کلمات کلیدی: شبکه هوشمند برق، رایانش ابری، امنیت، حریم خصوصی، داده، تهدیدات سایبری

An Efficient Cloud based Architecture to Improve Smart Grid Performance

Mohammad Rasoul Momeni[1] - Fatemeh Haghighat[1] - Mohsen Haghighat[2]
(1) MSc – Department of Electrical Engineering, Golpayegan University of Technology, Golpayegan, Iran
m.momeni@gut.ac.ir
haghighat@gut.ac.ir
(2) MSc - Great Tehran Electricity Distribution Company, Tehran. Iran
mhaghighat520@yahoo.com

Abstract: Due to explosive growth of users, increasing energy demand and also the need to improve efficiency and maintaining the stability of the electricity grid, smart grid is the only option available to electrical industry engineers. In fact, the smart grid is a physical-cyber system that provides coherent and integrated communication, processing and control functions. The smart grid provides control and management of millions of devices in the electricity industry in a reliable, scalable, cost-effective, real time and two-sided manner. Given the increasing growth of cyber threats in the last decade, the need to protect the electricity industry and its critical systems seems essential. The slightest disruption to the power industry's systems results in disruption to other industries, reduced productivity, and discontent. Hence we proposed an efficient cloud based architecture to improve smart grid performance. Proposed architecture uses elliptic curve cryptosystem and provides data security and privacy against different types of cyber-attacks such as replay attack, modification attack and so on.
Index Terms: Smart grid, cloud computing, security, privacy, data, cyber threats.

نویسنده مسئول: محمد رسول مومنی، کارشناس ارشد - دانشکده فنی و مهندسی، دانشگاه گلپایگان، گلپایگان، ایران، m.momeni@gut.ac.ir

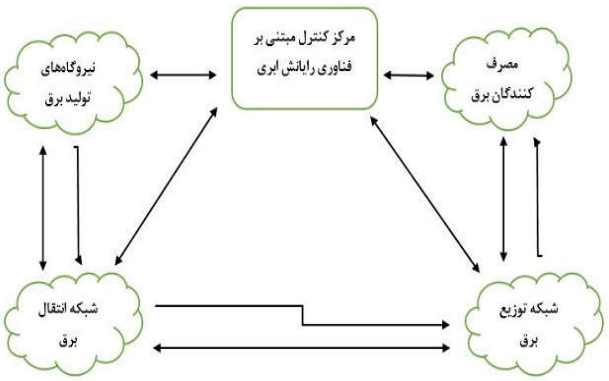
۱- مقدمه

تغییرات نیازمندی‌ها در صنعت برق از قبیل نیاز به بازده بالاتر، پایداری شبکه، مدیریت بهینه دستگاه‌ها، افزایش چشمگیر حجم داده‌ها، تأمین فراگیر امنیت داده‌ها و غیره منجر به گذر از شبکه سنتی به شبکه هوشمند گردید. در شبکه هوشمند برق نظارت پیوسته شبکه به صورت هوشمند و بلادرنگ صورت می‌پذیرد، در نتیجه کوچک‌ترین اختلال به آسانی قابل تشخیص و اقدام است. در این شبکه حجم عظیمی از داده‌ها تولید می‌شود که با به کارگیری فناوری رایانش ابری ذخیره‌سازی و پردازش داده‌ها به نحو مطلوبی صورت می‌پذیرد. در واقع رایانش ابری یعنی دسترسی آسان و مبتنی بر تقاضا از طریق شبکه به مخزن اشتراکی از منابع پردازشی و قابل پیکربندی از قبیل شبکه، سرور، فضای ذخیره-سازی، برنامه و خدمات [۱]. یکی دیگر از مزایای مهم فناوری رایانش ابری، مجازی‌سازی می‌باشد که در سطوح مختلف شبکه، سیستم عامل و غیره قابل اجرا بوده و ضمن افزایش بهره‌وری، کاهش هزینه‌ها را از طریق کاهش وابستگی به سخت‌افزار به دنبال دارد [۲]. ارتباطات در شبکه هوشمند برق به صورت چند جهته و دو طرفه بین دستگاه‌های مختلف وجود دارد که سبب می‌شود پاسخ‌گو بودن که از مهم‌ترین نیازمندی‌های شبکه هوشمند برق است، محقق شود. نیازمندی مهم دیگر شبکه هوشمند برق قابلیت دسترسی بالا می‌باشد که به کمک فناوری رایانش ابری فراهم می‌گردد. کارهای پیشین در این حوزه به صورت خلاصه بررسی می‌شود. فانگ و همکاران روشی برای استفاده از فناوری رایانش ابری در شبکه هوشمند برق ارائه نمودند [۳]. در روش آن‌ها کاربرد ویژگی‌های مختلف فناوری رایانش ابری مانند ذخیره‌سازی ابری، ماشین‌های مجازی به صورت دقیق و تحلیلی در شبکه هوشمند برق بررسی شد. همچنین در روش فوق امنیت فناوری رایانش ابری نیز مورد بررسی قرار گرفت. در این مقاله کاربرد حوزه‌های مختلف فناوری رایانش ابری در شبکه هوشمند برق بررسی شده و در انتها امنیت ابر نیز به صورت مختصر بررسی شده است. هیچ‌گونه چهارچوب مدونی به منظور ارتقای امنیت شبکه هوشمند برق پیشنهاد نشده است. دمیر و همکاران برای بهبود امنیت شبکه هوشمند برق از فناوری رایانش ابری استفاده نموده‌اند [۴]. آن‌ها به صورت خاص بر روی حمله ممانعت از خدمات توزیع شده و مقابله با آن تمرکز داشته‌اند و در این راستا دو تکنیک توسط آن‌ها ارائه شده است. رویکرد جامعی برای ارتقای امنیت در شبکه هوشمند برق با استفاده از فناوری رایانش ابری در این مقاله وجود ندارد و تنها بر روی مقابله با یک حمله خاص تمرکز شده است. عبدالرحمان و همکاران به صورت دقیق و جزئی به بررسی چالش‌های امنیتی پیش روی شبکه هوشمند برق پرداخته‌اند [۵]. آن‌ها چالش‌های شناسایی شده را براساس منابع تهدید به دقت طبقه‌بندی و مورد تحلیل قرار داده‌اند. در انتهای مقاله نیز چهارچوبی برای دستیابی به امنیت بیشتر در شبکه هوشمند برق پیشنهاد داده‌اند. چهارچوب پیشنهاد شده در این مقاله بسیار کلی و مبهم بوده و نیاز به بررسی و متمرکز شدن روی حوزه‌های مشخصی از شبکه هوشمند برق دارد. در واقع نویسندگان راهکار و تکنیک مشخصی ارائه نداده‌اند.

در این مقاله یک معماری کارآمد و مبتنی بر فناوری رایانش ابری برای تأمین امنیت داده‌ها در شبکه هوشمند برق ارائه شده است. معماری پیشنهادی در برابر حملات مختلف سایبری از قبیل حملات تکرار، ممانعت از خدمات، شخص میانی و غیره مقاوم می‌باشد. تحلیل‌های امنیتی انجام شده صحت موارد فوق را تأیید می‌نماید. قابل بیان است که معماری پیشنهادی ضمن تأمین امنیت، بسیار کارآمد نیز می‌باشد، تحلیل‌های کارایی صورت گرفته مؤید این مطالب است. این مقاله دارای نوآوری‌هایی نظیر استفاده از هویت پویا و عدم افشای هویت حقیقی، استفاده از مکانیزم بیت وضعیت و وارد نبودن حمله ورود تعداد زیادی کاربر می‌باشد.

۲- معماری شبکه هوشمند برق مبتنی بر ابر

در این بخش معماری پیشنهادی در زیربخش‌های مختلف به صورت دقیق ارائه می‌شود. در شکل (۱) معماری پیشنهادی ترسیم شده است. جریان داده در معماری پیشنهادی از طریق زیرساخت فیبر نوری منتقل می‌شود که ضمن قابلیت اطمینان بالا، سرعت انتقال زیادی را نیز تضمین می‌نماید. قابل ذکر است که در شکل (۱) خطوط صاف و دو جهته نمایانگر جریان اطلاعات و خطوط دارای انحنا و یک جهته نمایانگر جریان برق می‌باشند.



شکل (۱): معماری شبکه هوشمند برق مبتنی بر رایانش ابری
Fig (1): Architecture of Cloud based Smart Grid

۲-۱- ذخیره‌سازی در معماری مبتنی بر ابر

در شبکه هوشمند برق با رشد نمایی داده‌ها از منابع مختلف مانند شبکه انتقال، شبکه توزیع، کنتورهای هوشمند و غیره روبرو مواجه هستیم. همچنین این حجم عظیم داده باید با سرعت قابل قبولی پردازش و تحلیل گردد. بدون استفاده از فناوری رایانش ابری انجام چنین اموری بسیار دشوار بوده و با کندی صورت می‌گیرد. با بهره‌گیری از فناوری رایانش ابری فضای نامحدودی از لحاظ ذخیره‌سازی فراهم می‌شود. همچنین سرورهای قدرتمند محیط ابر می‌توانند پردازش و تحلیل این حجم عظیم از داده‌ها را با سرعت انجام دهند و در نتیجه کنترل بلادرنگ تجهیزات گوناگون در محیط‌های مختلف به سادگی امکان‌پذیر شود. یکی دیگر از مزایای مهم بهره‌گیری از ذخیره‌سازی ابری، تحمل‌پذیری بالای خطا از طریق افزونگی سرورها است. ذخیره‌سازی ابری امنیت داده‌ها را از طریق

مدیریت یکپارچه و پشتیبان‌گیری در مکان‌های متفاوت تضمین می‌نماید. به عنوان مثال مرکز دیسپاچینگ در سطوح مختلف می‌توانند داده‌های خود را روی سرورهای مختلف پشتیبان‌گیری و مدیریت نمایند. در این سناریو اگر یک مرکز با حملات سایبری روبرو شود، پس از دفع حمله به سادگی با داده‌های پشتیبان گرفته شده می‌تواند کار خود را شروع نماید. به صورت خلاصه ذخیره‌سازی ابری هوشمند، خودکار و توزیع شده می‌باشد که تحولی شگرف به شمار می‌آید.

۲-۲- مجازی‌سازی در معماری مبتنی بر ابر

استفاده از فناوری مجازی‌سازی در سطوح مختلف شبکه، سیستم عامل و ماشین‌های مجازی برای سامانه‌های مختلف شبکه هوشمند برق منجر به افزایش بهره‌وری و کاهش چشمگیر هزینه‌ها از طریق کاهش وابستگی به سخت‌افزار می‌شود. در دهه اخیر مجازی‌سازی به صورت فزاینده‌ای توسط سازمان‌ها و شرکت‌ها به عنوان شیوه‌ای مطمئن برای کاهش هزینه‌ها اتخاذ شده است. به عنوان مثال شرکت تأمین انرژی شنژن چین در سال ۲۰۰۹ توسط فناوری مجازی‌سازی توانست ۶۰ سرور مجازی را با تنها ۴ سرور فیزیکی راه‌اندازی نماید و مصرف انرژی خود را تا ۹۰ درصد کاهش دهد [۶].

در فناوری مجازی منابع ذخیره‌سازی و پردازشی به صورت پویا، بلادرنگ و مبتنی بر تقاضا تخصیص می‌یابند و در نتیجه بازده عملیاتی سیستم افزایش می‌یابد.

۲-۳- امنیت در معماری مبتنی بر ابر

مدیریت یکپارچه رایانش ابری یکی از عوامل کلیدی در تأمین امنیت داده‌ها محسوب می‌شود. همچنین فناوری رایانش ابری فاکتور زمان را در سناریوهای بازیابی فاجعه را به صورت چشمگیری بهبود می‌بخشد. دلیل این بهبود نیز ویژگی‌های رایانش ابری مانند قابلیت دسترسی بالا، قابلیت اطمینان بالا و توزیع شدگی می‌باشد [۷].

۳- روش پیشنهادی

در این بخش یک چهارچوب امنیتی ابری مبتنی بر سیستم رمزنگاری منحنی بیضوی جهت صیانت از امنیت داده‌ها و حریم خصوصی در شبکه هوشمند برق ارائه می‌شود.

۳-۱- مبانی روش پیشنهادی

با توجه به استفاده از سیستم رمزنگاری منحنی بیضوی، در این بخش توصیف مختصری از این روش ارائه خواهیم داد. سیستم رمزنگاری منحنی بیضوی که در سال ۱۹۸۵ توسط نیل کوبلیتز [۸] و ویکتور میلر [۹] به صورت مستقل از هم ارائه شد امروزه به عنوان جزء جدایی‌ناپذیر رمزنگاری مدرن مطرح است.

از زمان ارائه تاکنون پژوهش‌های بسیاری در رابطه با آن صورت پذیرفته که همگی حاکی از اثبات کارایی بالای محاسباتی آن است. ویژگی طول کلید کوچکتر برای سیستم رمزنگاری منحنی بیضوی دارای مزایایی چون سرعت بالا و مصرف بهینه توان، پهنای باند و فضای ذخیره‌سازی است. در کنار این مزایا امنیت بالایی هم برای این روش در مقایسه با دیگر روش‌های رمزنگاری نامتقارن وجود دارد، به صورتی که در سیستم رمزنگاری منحنی بیضوی کلیدی (مبتنی بر لگاریتم گسسته روی منحنی بیضوی) به طول ۱۶۰ بیت قادر به ایجاد امنیتی معادل با کلیدی به طول ۱۰۲۴ بیت در سیستم رمزنگاری RSA[1] (مبتنی بر مسئله فاکتورگیری صحیح) است [۱۰].

مجموع این ویژگی‌ها سبب شده تا در سناریوهایی که نیاز ایجاد امنیت بالاتری داریم، از این تکنیک برتر رمزنگاری استفاده کنیم. از این رو بهترین گزینه برای تأمین امنیت در شبکه هوشمند برق مبتنی بر فناوری رایانش ابری استفاده از سیستم رمزنگاری منحنی بیضوی است. در ضمن با استانداردسازی آن امروزه در محصولات تجاری بسیاری نیز استفاده می‌شود. امنیت سیستم رمزنگاری منحنی بیضوی به سختی حل مسئله لگاریتم گسسته روی منحنی بیضوی (ECDLP) بستگی دارد. این مسئله این چنین تعریف می‌شود:

اگر P و Q نقاط روی یک منحنی بیضوی باشند و رابطه (۱) را نیز داشته باشیم:

$$Q = nP \qquad (۱)$$

آنگاه با معلوم بودن دو نقطه‌ی P و Q، پیدا کردن مقدار n در عمل بسیار مشکل است. موضوع بسیار مهم در مورد مسئله لگاریتم گسسته روی منحنی بیضوی این است که هیچ رابطه‌ی مستقیمی برای محاسبه‌ی آن وجود ندارد، یعنی برای حل آن فقط باید از آزمون و خطا استفاده کرد. حال اگر n عددی بزرگ مثلا ۱۶۰ بیتی و بیشتر باشد، حل مساله لگاریتم گسسته روی منحنی بیضوی بسیار دشوارتر نیز خواهد شد، زیرا جستجوی فضایی به این بزرگی هزاران سال طول خواهد کشید. در نتیجه امنیت سیستم‌های رمزنگاری مبتنی بر منحنی بیضوی در عدم وجود رابطه مستقیم برای محاسبه مسئله لگاریتم گسسته روی منحنی بیضوی می‌باشد. حال به تعریف نقطه اساسی در منحنی بیضوی می‌پردازیم.

نقطه اساسی: نقطه‌ای روی منحنی می‌باشد که بیشترین مرتبه را دارد. این نقطه اهمیت بالایی دارد، زیرا بیشترین پیمایش را روی منحنی انجام می‌دهد و می‌توان دیگر نقاط منحنی را از روی آن به دست آورد.

مرتبه نقطه: تعداد دفعاتی که می‌توان یک نقطه (مانند P) را با خودش جمع کرد تا به بی‌نهایت برسیم.

ضرب اسکالر: اساسی‌ترین عملیات در سیستم رمزنگاری منحنی بیضوی است و به صورت جمع یک نقطه مانند P با خودش به تعداد k مرتبه است. معادله آن به صورت رابطه (۲) است:

$$Q = k.P = \underbrace{P + P + \ldots + P}_{k} \qquad (۲)$$

مسئله مهم دیگری که نیاز به ذکر آن در این بخش می‌باشد، مسئله دیفی-هلمن محاسباتی (CDHP) است. تعریف آن به این صورت است: اگر (P, aP, bP) را داشته باشیم آنگاه محاسبه abP بسیار مشکل است. از این مسئله در اثبات امنیت طرح پیشنهادی استفاده خواهیم نمود.

نمادهای به کار رفته در چهارچوب امنیتی پیشنهادی در جدول (۱) آورده شده‌اند.

Table (1): Symbols
جدول (۱): نمادها

توصیف	نماد
هویت کاربر	ID_U
رمز عبور کاربر	PW_U
کلید خصوصی سرور	S
کلید عمومی سرور	$Q = S.P$
کلید احراز هویت	$AK_U = S.Z_U$
تصدیق‌کننده رمز عبور	$Z_U = PW_U.P$
هویت پویای کاربر	DID_U
نقطه اساسی	P
عملگر الحاق	$\|\|$
تابع درهم ساز	$H(\ )$
اعداد تصادفی	r_1 , r_2
تابع رمزنگاری متقارن	$E_{AK}(\ )$

۳-۲- مرحله ثبت‌نام

در این مرحله کاربر از طریق کانال امن عملیات ثبت‌نام را انجام می‌دهد. توجه داشته باشید که این مرحله فقط یک بار انجام می‌گیرد در حالی که مرحله احراز هویت می‌تواند بارها تکرار شود. پس از پایان موفقیت-آمیز این مرحله است که مرحله بعد یعنی احراز هویت می‌تواند صورت پذیرد. جزئیات این مرحله به شرح زیر است.

گام اول: کاربر، هویت و تصدیق‌کننده رمز عبور خود را به سمت سرور احراز هویت می‌فرستد.

گام دوم: سرور هویت ارسالی کاربر را بررسی می‌کند و اگر چنین هویتی در پایگاه داده‌اش موجود باشد، تقاضای ثبت‌نام را رد می‌کند. سرور به کاربر اطلاع می‌دهد که باید با یک هویت منحصربه فرد و غیرتکراری عملیات ثبت‌نام را انجام دهد. به این ترتیب عملیات مدیریت هویت به صورت شایسته‌ای صورت می‌گیرد. در صورت تکراری نبودن هویت ارسالی از سوی کاربر، سرور کلید احراز هویت را به ترتیب زیر تولید می‌کند.

$$AK_U = S.Z_U \qquad (۳)$$

در ضمن هویت کاربر به همراه تصدیق‌کننده رمز عبور و بیت وضعیت در جدولی به نام جدول کاربران ذخیره می‌شود.

گام سوم: سپس سرور کلید احراز هویت را به سوی کاربر می‌فرستد.

بیت وضعیت نمایانگر وضعیت کاربر است. یعنی اگر کاربر وارد سیستم شده باشد بیت وضعیت برابر با یک خواهد بود. در غیر این صورت مقدار آن صفر می‌باشد. نمونه‌ای از جدول کاربران در جدول (۲) آمده است.

Table (2): Table of Users
جدول (۲): جدول کاربران

هویت	تصدیق‌کننده رمز عبور	بیت وضعیت
ID_A	$Z_A = PW_A.P$	۰-۱
ID_B	$Z_B = PW_B.P$	۰-۱
ID_C	$Z_C = PW_C.P$	۰-۱

۳-۳- مرحله احراز هویت دو طرفه و توافق کلید جلسه

هر زمان که کاربر بخواهد از منابع ابر استفاده کند باید از طریق گام‌های زیر خودش را برای سرور، احراز هویت کند. البته کاربر نیز می‌تواند سرور را احراز هویت کند، یعنی فرآیند احراز هویت، دو طرفه است.

گام اول: کاربر با شناسه کاربری و رمز عبور خود وارد سیستم می‌شود. سپس عدد تصادفی r_1 را انتخاب نموده و مقدار $R = r_1.Q$ را محاسبه می‌کند. همچنین مقدار $M = r_1.PW_U.P$ به همراه هویت پویا محاسبه می‌شود. از آنجا که کانال ارتباطی در این مرحله امن نیست، هویت پویا به منظور گمنامی کاربر محاسبه می‌شود. روش محاسبه هویت پویای کاربر به این صورت است:

$$DID_U \ H(AK_U \| R) \oplus ID_U \qquad (۴)$$

در نهایت کاربر سیار پیام M_1 را به صورت زیر به سمت سرور می‌فرستد.

گام $M_1 = (DID_U, E_{AK}(R, M), H(DID_U, E_{AK}(R, M))) \qquad (۵)$

دوم: در این گام سرور احراز هویت با استفاده از DID_U و $E_{AK}(R, M)$ مقدار $H(DID_U, E_{AK}(R, M))$ را محاسبه نموده و با $H^*(DID_U, E_{AK}(R, M))$ دریافتی مقایسه می‌کند. این عمل به منظور بررسی وقوع یا عدم وقوع حمله تغییر صورت می‌گیرد. اگر این دو مقدار برابر باشند وقوع حمله تغییر منتفی است ولی اگر این دو مقدار متفاوت باشند حمله تغییر اتفاق افتاده و سرور احراز هویت این جلسه را در همین مرحله لغو می کند. لغو جلسه و رد درخواست احراز هویت منجر به جلوگیری از حمله ممانعت از خدمات می‌شود. اگر حمله تغییر تشخیص داده نشود، سرور احراز هویت با عمل رمزگشایی R و M را به دست می‌آورد. نکته‌ای که اینجا حائز اهمیت است آن است که با انجام عمل رمزگشایی به نوعی هویت کاربر برای سرور تایید می‌شود. زیرا مخاطب ارتباط همان کاربر مورد نظر است که کلید احراز هویت در مرحله ثبت‌نام به او ارائه شده بود و او توانسته است به این وسیله پارامترهای دلخواهش را رمزنگاری کند. سپس در همین گام سرور از روی هویت پویا، هویت اصلی کاربر را به صورت زیر تعیین می‌کند.

$$ID_U = H(AK_U \| R) \oplus DID_U \qquad (۶)$$

پس از به دست آوردن هویت اصلی (ID_U)، آن را از طریق هویت‌های موجود در جدول کاربران اعتبارسنجی می‌کند. پس از برآورده شدن همه شرایط ذکر شده سرور احراز هویت عدد تصادفی r_2 را انتخاب کرده و $N = r_2.Q$ را محاسبه می‌کند. در انتهای این گام سرور احراز هویت پیام M_2 را به سوی کاربر سیار ارسال می‌کند.

$$M_2 = ((M+N), H(N)) \qquad (۷)$$

گام سوم: در این گام کاربر سیار با محاسبه M+N-M مقدار N را به دست می‌آورد. سپس $H^*(N)$ را محاسبه نموده و این مقدار را با $H(N)$ مقایسه می‌کند تا وقوع یا عدم وقوع حمله تغییر را تشخیص دهد. مطابق آن‌چه در گام دوم بیان شد، اگر این دو مقدار متفاوت باشند حمله تغییر رخ داده و این جلسه در همین جا لغو می‌شود تا امکان بروز حمله ممانعت از خدمات از بین برود. در صورت برآورده شدن این شرایط، کاربر اقدام به محاسبه پیام M_3 جهت ارسال به سرور احراز هویت می‌نماید. در ضمن کلید جلسه نیز در این گام محاسبه می‌شود.

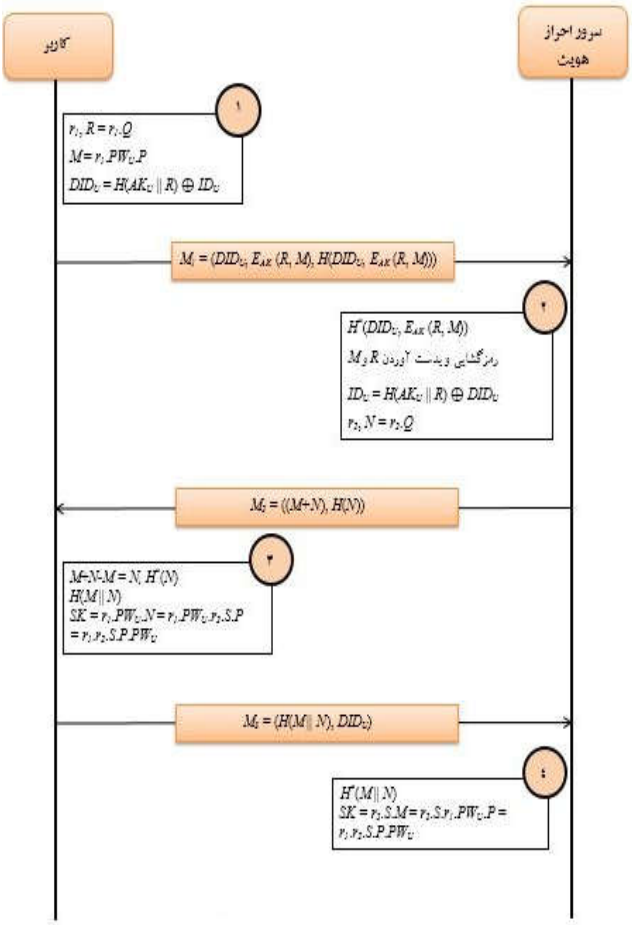
$$M_3 = (H(M \| N), DID_U) \qquad (۸)$$

$$SK = r_1.PW_U.N = r_1.PW_U.r_2.S.P = r_1.r_2.S.P.PW_U \quad (۹)$$

گام چهارم: سرور احراز هویت پس از دریافت پیام M_3 از کاربر سیار، مقدار $H^*(M \parallel N)$ را محاسبه نموده و آن را با $H(M \parallel N)$ دریافتی مقایسه می‌کند تا طبق گام‌های پیشین وقوع یا عدم وقوع حمله تغییر را تشخیص دهد. اگر این دو مقدار با هم برابر باشند وقوع حمله تغییر منتفی است و سرور احراز هویت به صورت زیر اقدام به محاسبه کلید جلسه می‌کند.

$$SK = r_2.S.M = r_2.S.r_1.PW_U.P = r_1.r_2.S.P.PW_U \quad (۱۰)$$

چنان‌چه دو مقدار با هم متفاوت بودند سرور احراز هویت متوجه وقوع حمله تغییر شده و جلسه را در همین نقطه لغو می‌کند تا از بروز حمله ممانعت از خدمات جلوگیری شود. پس از توافق روی یک کلید جلسه، هر دو طرف از این کلید جهت رمزنگاری پیام‌های ارسالی و داشتن ارتباطی امن استفاده می‌کنند. توجه داشته باشید که کلید جلسه در هر جلسه تغییر می‌کند. یعنی فقط برای همان جلسه خاص معتبر است. نمایی از فرآیند احراز هویت دو طرفه و توافق کلید جلسه در شکل (۲) نشان داده شده است.



شکل (۲): فرآیند احراز هویت دو طرفه و توافق کلید جلسه

Fig (2): Mutual Authentication and Session Key Agreement

۳-۴- مرحله تغییر رمز عبور

فراهم آوردن امکان تغییر رمز عبور کاربر موجب می‌شود تا امنیت و کاربرپسند بودن طرح پیشنهادی در سطح بالایی تضمین گردد. بهتر است مرحله تغییر رمز عبور بدون مداخله سرور احراز هویت راه دور طراحی شود تا از کارایی و امنیت بالایی برخوردار باشد. در طرح پیشنهادی نیز کاربر پس از انتخاب رمز عبور جدید و محاسبه تصدیق‌کننده برای آن، فقط تصدیق‌کننده رمز عبور را برای سرور می‌فرستد. توجه داشته باشید که کانال ارتباطی در این مرحله امن است. این مرحله از گام‌های زیر تشکیل شده است.

گام اول: کاربر هویت و تصدیق‌کننده رمز عبور خود را همراه با درخواست تغییر کلمه عبور به سمت سرور احراز هویت می‌فرستد.

گام دوم: سرور احراز هویت عملیات مدیریت هویت را با بررسی هویت ارسالی کاربر انجام می‌دهد. در صورت تایید شدن هویت کاربر، سرور مقدار $H(ID_U \parallel SK)$ را محاسبه نموده و آن را برای کاربر سیار ارسال می‌کند.

گام سوم: کاربر مقدار $H^*(ID_U \parallel SK)$ را محاسبه نموده و آن را با $H(ID_U \parallel SK)$ دریافتی از سرور مقایسه می‌کند. در صورت برابر بودن این دو مقدار، کاربر نیز از هویت سرور اطمینان حاصل می‌کند و به صورت زیر اقدام به محاسبه تصدیق‌کننده رمز عبور جدید می‌نماید.

$$Z_U^* = PW_U^*.P \quad (۱۱)$$

سپس این تصدیق‌کننده رمز عبور را برای سرور احراز هویت می‌فرستد تا در جدول کاربران جایگزین تصدیق‌کننده رمز عبور قدیمی شود. با تغییر تصدیق‌کننده رمز عبور، کلید احراز هویت جدیدی توسط سرور محاسبه می‌شود.

۵-۳- مرحله اخراج کاربر

در طرح پیشنهادی امکان اخراج کاربران متخلف توسط سرور فراهم شده است. برای این منظور سرور باید سطر مربوط به کاربر یا کاربران مورد نظر را از جدول کاربران حذف کند. اگر کاربر یا کاربران اخراج شده سعی در ورود به سیستم داشته باشند ناکام می‌مانند. دلیل آن هم این است که در گام دوم مرحله احراز هویت و توافق کلید جلسه، ID_U محاسبه شده توسط سرور (از روی DID_U) اعتبارسنجی می‌شود و سرور متوجه می‌شود که چنین هویتی در جدول کاربران موجود نیست. در نتیجه کاربر یا کاربران اخراج شده قادر به ورود به سیستم و بهره‌گیری از منابع نیستند.

۴- تحلیل کارایی

در این قسمت به بیان و شرح ویژگی‌هایی می‌پردازیم که نمایانگر کارایی بالای طرح پیشنهادی است.

۱-۴- اجتناب از مسئله همزمان‌سازی ساعت

بسیاری از طرح‌های احراز هویت پیشنهاد شده جهت جلوگیری از حمله تکرار از مکانیزم مهر زمان بهره می‌برند. اما باید توجه داشت که مکانیزم مهر زمان در سیستم‌های توزیع شده دارای سربار عملیاتی بالا است [۱۱]. به منظور اجتناب از این سربار عملیاتی بالا و نیز کاربرپسند بودن طرح پیشنهادی، به جای برچسب زمان از اعداد تصادفی در طرح ارائه شده استفاده کرده‌ایم.

۲-۴- پهنای باند اندک

روش پیشنهادی با استفاده از سیستم رمزنگاری منحنی بیضوی پیاده‌سازی شده که در بین انواع روش‌های رمزنگاری نامتقارن طول کلید

کوچکتری را دارا است. این ویژگی علاوه بر ایجاد سرعت بالا موجب استفاده کمتر از پهنای باند خواهد شد. در ضمن در قسمتی از روش پیشنهادی رمزنگاری متقارن هم استفاده شده است و می‌دانیم که متن رمز شده در این حالت با تعداد بیت‌های کمتری تولید می‌شود. در نتیجه پیام‌هایی که در این روش مبادله می‌شوند دارای طول کوچکتری بوده و بنابراین نیازمندی‌های پهنای باند و هزینه ارتباطی اندک می‌باشد.

۴-۳- مدیریت هویت

در مرحله ثبت‌نام طرح ارائه شده بررسی می‌شود که هویت فراهم شده برای سرور تکراری نباشد. همچنین در گام دوم مرحله احراز هویت و توافق کلید جلسه نیز هویت محاسبه شده از روی هویت پویا اعتبارسنجی می‌شود. به این وسیله عملیات مدیریت هویت به بهترین نحو توسط طرح پیشنهادی پشتیبانی می‌شود.

۴-۴- مقیاس‌پذیر و سریع

استفاده از یک مرکز مستقل جهت احراز هویت باعث مقیاس‌پذیری طرح ما شده است و در این حالت پردازش اضافه‌ای بر روی سرور وجود نخواهد داشت. همچنین استفاده از سیستم رمزنگاری منحنی بیضوی که به دلیل دارا بودن طول کلید کوچکتر، سرعت بالایی دارد موجب شده روش پیشنهادی سریع و کاربرپسند باشد.

۴-۵- گمنامی کاربر

گمنامی کاربر یعنی حفظ حریم خصوصی او و در برابر عموم مطرح می‌شود نه سرور مربوطه [۱۲]. دلیل آن هم این است که سرور باید هویت کاربر را به منظور ارائه خدمات و عملیات حسابرسی شناسایی و اعتبارسنجی کند. روش ارائه شده از گمنامی کاربر پشتیبانی می‌کند، زیرا در مراحل ثبت‌نام و تغییر رمز عبور که هویت اصلی فرستاده می‌شود کانال امن است و در مرحله احراز هویت و توافق کلید جلسه هم که کانال ناامن است از هویت پویا استفاده می‌شود.

۵- تحلیل امنیتی

در این قسمت به بیان و شرح ویژگی‌هایی می‌پردازیم که نمایانگر کارایی بالای طرح پیشنهادی است.

۵-۱- حمله حدس رمز عبور

این حمله یکی از شایع‌ترین حملات وارد بر طرح‌های احراز هویت مبتنی بر رمز عبور است. یکی از دلایل آن می‌تواند تمایل کاربران به انتخاب رمز عبور ضعیف باشد که حدس آن نیز برای افراد متخاصم بسیار ساده است. در طرح پیشنهادی آن‌چه که مورد استفاده سرور قرار می‌گیرد و در جدول کاربران ذخیره می‌شود، رمز عبور نیست بلکه تصدیق‌کننده رمز عبور است. استخراج رمز عبور از تصدیق‌کننده‌اش برابر با حل مسئله لگاریتم گسسته روی منحنی بیضوی است که در عمل بسیار مشکل است و با سیستم‌های محاسباتی فعلی هزاران سال طول می‌کشد. در نتیجه این حمله به این طرح وارد نیست.

۵-۲- حمله تکرار

طرح پیشنهادی از مکانیزم اعداد تصادفی به منظور جلوگیری از وقوع حمله تکرار استفاده می‌کند. حدس زدن مقادیر اعداد تصادفی برای دشمن کار بسیار مشکلی است، زیرا آن‌ها در هر جلسه و هر مرتبه احراز هویت به روز شده و تغییر می‌کنند. یعنی به نوعی یک بار استفاده هستند. در نتیجه این حمله به طرح ارائه شده وارد نمی‌باشد.

۵-۳- حمله تغییر

به منظور اجتناب از وقوع حمله تغییر از یک تابع درهم ساز یک طرفه عاری از برخورد استفاده شده است. اگر دشمن یک پیام تغییر یافته را بفرستد، مخاطب به سادگی با بررسی مقادیر دو تابع درهم ساز حمله تغییر را تشخیص می‌دهد. در نتیجه این حمله به طرح پیشنهادی وارد نیست.

۵-۴- حمله اطلاعات موقتی ویژه جلسه شناخته شده

این حمله بیان می‌کند اگر اطلاعات موقتی و مخفی یک جلسه خاص افشا شود امنیت کلید جلسه به خطر خواهد افتاد. در تولید کلید جلسه طرح پیشنهادی اگر اعداد تصادفی افشا شوند کلید جلسه لو نخواهد رفت، زیرا در تولید کلید جلسه مولفه‌های دیگری نظیر رمز عبور کاربر و کلید خصوصی سرور به کار رفته‌اند که دشمن آن‌ها را نمی‌داند. از دیگر سو برای محاسبه کلید جلسه دشمن باید $PW_U.S.P$ را از زوج $(PW_U.P,S.P)$ محاسبه کند که معادل با حل مسئله دیفی- هلمن محاسباتی است و می‌دانیم که حل این مسئله در عمل بسیار مشکل است.

۵-۵- حمله جعل سرور

در این حمله فرد متخاصم سعی در جا زدن خود به جای سرور دارد. این حمله به روش پیشنهادی وارد نیست، زیرا فرد متخاصم مقدار کلید خصوصی سرور را نمی‌داند و در نتیجه قادر نیست کلید احراز هویت را به دست آورد. نداشتن کلید احراز هویت یعنی عدم توانایی رمزگشایی و به دست آوردن R و M در گام دوم فرآیند احراز هویت و توافق کلید جلسه. همچنین در صورت نبود کلید احراز هویت محاسبه هویت حقیقی کاربر سیار (ID_U) امکان‌پذیر نیست. به این صورت فرد متخاصم در همان ابتدای کار شکست خورده و توانایی ادامه کار را نخواهد داشت.

۶- نتیجه‌گیری

در این مقاله یک معماری کارآمد و مبتنی بر فناوری رایانش ابری برای بهبود عملکرد در شبکه هوشمند برق ارائه شده است. به دلایلی مانند رشد چشمگیر مشترکین، افزایش روزافزون تقاضای انرژی و همچنین نیاز به بالا بردن بهره‌وری و حفظ پایداری شبکه برق، امروزه شبکه هوشمند برق تنها راه مدیریت مطلوب شبکه برق به شمار می‌رود. معماری پیشنهادی با بهره مندی از ویژگی‌های فناوری رایانش ابری ضمن داشتن کارایی بالا، قادر به تأمین امنیت و حریم خصوصی داده‌ها در برابر انواع مختلف حملات سایبری نظیر حمله تکرار، تغییر و غیره می‌باشد. در معماری پیشنهادی از سیستم رمزنگاری منحنی بیضوی استفاده شده است که علاوه بر تضمین امنیت بیشتر، طول کلید کوچکتری داشته و پهنای باند کمتری مصرف می‌نماید. تحلیل‌های کارایی و امنیتی صورت گرفته نیز موید این ادعا است که ضمن تضمین کارایی بالا، امنیت معماری پیشنهادی بسیار خوب بوده و در برابر حملات مختلف سایبری نیز مقاوم است.

پی‌نوشت:

1. Rivest, Shamir, Adelman

References

[1] P. Mell, T. Grance, The NIST definition of cloud computing (draft), 2011, Available: http://csrc.nist.gov/publications/drafts/800–145/Draft-SP-800-145_cloud-definition.pdf.

[2] M. R. Momeni. "A survey of mobile cloud computing: advantages, challenges and approaches". InternationalJournal of Computer Science and Business Informatics, Vol. 15, No. 4, pp. 14-28, 2015.

[3] B. Fang, X. Yin, Y. Tan, C. Li, Y. Gao, Y. Cao, J. Li, "The contributions of cloud technologies to smart grid", Renewable and Sustainable Energy Reviews, Vol. 59, pp. 1326-1331, June 2016 (doi:10.1016/j.rser.2016.01.032).

[4] K. Demir, H. Ismail, T. Gurova, N. Suri, "Securing the cloud-assisted smart grid", International Journal of Critical Infrastructure Protection, pp. 100-111, Dec. 2018 (doi:10.1016/j.ijcip.2018.08.004).

[5] A. O. Otuoze, M. W. Mustafa, R. M. Larik, "Smart grid security challenges: Classification by sources of threat", Journal of Electrical Systems and Information Technology, Vol. 5, No. 3, pp. 468-483, Dec. 2018 (doi:10.1016/j.jesit.2018.01.001).

[6] T. Li," How to build the virtual system in power enterprise information system", Electr. Power Inf. Technol, 2009.

[7] Z. Hua, Z. Nan, "Cloud computing based data storage and disaster recovery", Proceeding of the IEEE/ICFCSE, 629-632, Aug. 2011 (doi:10.1109/ICFCSE.2011.157).

[8] N. Koblitz, "Elliptic curve cryptosystem", Journal of Mathematics Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[9] V. Miller, Use of elliptic curves in cryptography, Advances in Cryptology, pp. 417-426, 1985.

[10] D. Hankerson, A. Menzes, S. Vanston, Guide to elliptic curve cryptography, New York, USA: Springer-Verlag, 2004.

[11]R. Baldoni, A. Corsaro, L. Querzoni, S. Scipioni, S. Piergiovanni, "Coupling-based internal clock synchronizationfor large-scale dynamic distributed systems", IEEE Trans. on Parallel and Distributed Systems, Vol. 21, No. 5, pp. 607–619, May 2010 (doi:10.1109/TPDS.2009.111).

[12] Z. Tan, "A user anonymity preserving three-factorauthentication scheme for telecare medicine informationsystems", Journal of Medical Systems, Vol. 38, No. 3, pp. 1-9, March 2014 (doi:10.1007/s10916-014-0016-2).