17 Conference And 9 Exhibition Rubber And Related Industries
17 همایش و ۹ نمایشگاه لاستیک و صنایع وابسته
Iranmall
ایران مال
January 6-7 2026
۱۶ تا ۱۸ دی ماه ۱۴۰۴

بررسی روش های سبک رمزنگاری و احراز هویت داده ها در زیرساخت AI OT صنعتی مطالعه موردی در صنعت تایر

ضیاء احراری[۱] - سید محمدرضا جلالیان شهری[۲] - فرزین بیدختی[۳]
کارشناس سیستم‌های هوشمند[۱و۲و۳]،کویرتایر
۰۹۱۵۹۴۱۳۴۳۰ ضیاء احراری -Ahrari.ieee@gmail.com

چکیده:

تلفیق اینترنت اشیاء و هوش مصنوعی یا AIoT در صنعت تایرسازی، امکان جمع‌آوری و تحلیل داده‌های ماشین‌آلات پراکنده را در سرورهای مرکزی یا زیرساخت‌های ابری فراهم می‌سازد. این داده‌ها می‌توانند از طریق سیستم‌های صنعتی نظیر PLC و SCADA یا دستگاه‌های IoT تکمیلی دریافت شوند که روشی مقیاس‌پذیر و کم‌هزینه برای دیجیتال‌سازی خطوط تولید محسوب می‌شود. با این حال، انتقال داده در چنین محیط‌هایی در معرض تهدیداتی مانند دسترسی غیرمجاز، جعل داده و حملات میانجی قرار دارد. استفاده از الگوریتم‌های رمزنگاری سنگین همچون RSA یا AES-CBC، هرچند از نظر امنیتی مؤثر است، اما در دستگاه‌های کم‌منبع به دلیل مصرف بالای منابع و افزایش تأخیر، چندان عملیاتی نیست. در این مقاله، روش‌های رمزنگاری سبک یاLightweight Cryptography مناسب برای محیط‌های صنعتی بررسی شده‌اند. الگوریتم‌هایی نظیر AES-CCM، ChaCha۲۰-Poly۱۳۰۵ و رمزنگاری منحنی بیضوی ECC به دلیل ایجاد تعادل میان امنیت و کارایی معرفی شده‌اند. همچنین، استانداردسازی اخیر الگوریتم Ascon توسط NIST برای دستگاه‌های بسیار محدود، نقطه عطفی مهم در حوزه رمزنگاری سبک به شمار می‌رود. یک مطالعه موردی انجام شد که طی آن داده‌های ماشین پرس پخت، سامانه پایش عرض لایه و ویبره‌سنج موتور بنبوری تحت این روش‌ها ارزیابی گردید. نتایج کیفی نشان داد که ChaCha۲۰-Poly۱۳۰۵ با حفظ کارایی پردازشی و تأخیر پایین، در مقایسه با AES-CCM عملکرد متوازن‌تری ارائه می‌دهد و امنیت داده‌ها را بدون تحمیل فشار سنگین بر منابع تضمین می‌کند. این روش به‌ویژه برای داده‌های با نرخ بالا (مانند ارتعاشات) و دستگاه‌های IoT با منابع محدود، گزینه‌ای کارآمد و عملی محسوب می‌شود.

واژه‌های کلیدی: هوش مصنوعی اشیاء AIoT، امنیت داده، رمزنگاری سبُک، IoT

محور مقاله: فناوری ماشین آلات و قطعات تولیدی

مقدمه:

صنعت تایرسازی در حال گذار به سمت تولید هوشمند و انقلاب صنعتی چهارم است. در این مسیر، تلفیق اینترنت اشیا یا IoT و هوش مصنوعی یا AI به شکل AIoT (Artificial Intelligence of Things)، نقشی محوری در دیجیتال‌سازی خطوط تولید ایفا می‌کند. در این معماری، دستگاه‌های IoT وظیفه جمع‌آوری داده‌های عملیاتی از ماشین‌آلات را بر عهده دارند و این داده‌ها به سرورهای مرکزی منتقل می‌شوند. در اینجا، با استفاده از الگوریتم‌های هوش مصنوعی، تحلیل‌های پیش‌بینانه یا Predictive Maintenance، کنترل کیفیت، برنامه‌ریزی تولید و نظارت به صورت یکپارچه انجام می‌شود.[۱]

با این حال، تجمیع داده‌ها از بخش‌های مختلف خط تولید و وابستگی تصمیم‌گیری‌های هوشمند به این داده‌ها، امنیت و صحت انتقال داده را به یک الزام حیاتی تبدیل می‌کند. حتی اگر داده‌ها شنود نشوند، احتمال دستکاری، جعل، حمله بازیابی یا Replay یا از دست رفتن بسته‌ها وجود دارد که می‌تواند منجر به خطاهای جدی در کنترل فرآیند، تخریب تجهیزات یا تولید محصول معیوب شود. اهمیت این موضوع در بخش‌های مختلف تولید متفاوت است؛ مثلاً داده‌های ویبره الکتروموتور بنبوری نیازمند سرعت بالا و تأخیر پایین هستند، در حالی که داده‌های پرس پخت به دلیل ارتباطشان با فرمولاسیون تایر، حساسیت بالایی به دستکاری و نیازمند محرمانه‌سازی قوی می‌باشند.

از سوی دیگر، دستگاه‌های IoT مورد استفاده در خط تولید (مانند ماژول‌های ESP۳۲ یاRaspberry Pi) اغلب دارای CPU ضعیف، حافظه کم و محدودیت انرژی هستند. بنابراین، استفاده از روش‌های رمزنگاری سنگین مانند RSA یا AES در مد CBC، اگرچه از نظر فنی امکان‌پذیر است، اما در دستگاه‌هایی بدون شتاب‌دهنده رمزنگاری سخت‌افزاری به دلیل مصرف بالای منابع و تأخیر قابل توجه، چالش‌برانگیز است.[۲]

در این راستا، رمزنگاری سبک (Lightweight Cryptography) به عنوان راهکاری مؤثر برای حفظ تعادل بین امنیت و کارایی مطرح شده است. در نوامبر ۲۰۲۴، NIST پیش‌نویس اولیه استاندارد SP ۸۰۰-۲۳۲ را منتشر کرد که بر اساس خانواده الگوریتم Ascon، راهکارهای استانداردی برای رمزنگاری اصالت‌دار با داده همراه (ADAE) ، هش و توابع خروجی گسترش‌پذیر برای دستگاه‌های بسیار محدود ارائه می‌دهد. این اقدام نشان‌دهنده تحولی مهم در حوزه امنیت سیستم‌های تعبیه‌شده یا Embedded systems است. در این مقاله، به بررسی روش‌های سبک رمزنگاری مناسب برای صنعت تایرسازی پرداخته و یک مطالعه موردی از پیاده‌سازی یکی از این روش‌ها در یک خط تولید واقعی ارائه می‌شود.[۳]

بخش تجربی:

۱- تهدیدات امنیتی در انتقال داده‌های صنعتی:

در خط تولید تایر، داده‌های جمع‌آوری شده از طریق PLC ماشین آلات و دستگاه‌هایIoT ، علاوه بر حجم بالا، دارای حساسیت‌های متفاوت امنیتی هستند. تهدیدات اصلی شامل:

- دسترسی غیرمجاز به داده‌های عملیاتی حساس (مانند پارامترهای وولکانیزاسیون که مربوط به فرمولاسیون تایر است).
- جعل داده یا Data Tampering در فیدبک کنترلی ماشین‌آلات (مثلاً تغییر داده عرض لایه و منجر شدن به تولید محصول معیوب).
- حمله بازیابی یا Replay Attack در داده‌های ویبره‌سنج که می‌تواند باعث فریب سیستم نگهداری پیش‌بینانه شود.
- سرقت کلید رمزنگاری از دستگاه‌های فیلدی با دسترسی فیزیکی آسان.
- حمله میانجی یا MITM در شبکه‌های بی‌سیم یا کابلی صنعتی.

این تهدیدات نشان می‌دهند که امنیت لایه انتقال داده ضروری است، صرف‌نظر از اینکه داده از طریقPLC ، SCADA یا دستگاه IoT جمع‌آوری شده باشد.

۲- ویژگی‌های داده‌های صنعتی در خط تولید تایر:

در این مطالعه، سه نوع داده صنعتی طبق جدول ۱ با ویژگی‌های متفاوت مورد بررسی قرار گرفتند:

جدول۱: نوع داده و ویژگی‌ها

نوع داده	ویژگی‌های فنی	حساسیت امنیتی	نیاز امنیتی
ماشین پرس پخت	دمای ، فشار ، زمان چرخه (هر ۱۰ ثانیه)	بالا (کیفیت تایر)	محرمانه‌سازی بالا، یکپارچگی
سیستم پایش عرض لایه	عرض لایه (هر ۲ ثانیه)، خطای انحراف	بالا (کیفیت نیم ساخته)	یکپارچگی بالا، مقاومت در برابر جعل
ویبره‌سنج موتور بنبوری	شتاب‌سنج ، فرکانس ارتعاش (هر ۱۰۰ms)	متوسط (پایش وضعیت)	تأخیر پایین، مقاومت در برابر حمله بازیابی

این تنوع نشان می‌دهد که نیاز به یک رویکرد تطبیقی یا Adaptive Security در رمزنگاری وجود دارد، نه یک روش یک‌اندازه برای همه انواع داده.

۳- مطالعه موردی: ارزیابی عملکرد روش‌های رمزنگاری سبک در خط تولید تایر:

یک مطالعه میدانی در خط تولید تایر انجام شد تا عملکرد روش‌های رمزنگاری سبک در شرایط واقعی ارزیابی شود. سه دسته داده فوق از طریق ماژول‌های ESP۳۲-WROOM جمع‌آوری شدند. این ماژول‌ها نماینده بیشترین نوع دستگاه‌های IoT کم‌هزینه و کم‌منبع در محیط‌های صنعتی هستند.

داده‌ها از طریق شبکه Wi-Fi صنعتی (۸۰۲.۱۱n) به یک سرور در دیتاسنتر کارخانه ارسال شدند.

روش آزمایش:

- سه سناریوی رمزنگاری مقایسه شد:
  ۱) بدون رمزنگاری (پایه).
  ۲) AES-۱۲۸-CCM با طول برچسب ۶۴ بیت.
  ۳) ChaCha۲۰-Poly۱۳۰۵.
- تمام دستگاه‌ها از کتابخانه mbed TLS v۳,۵,۰ با بهینه‌سازی برای حافظه کم استفاده کردند.
- کلیدهای جلسه با ECDH روی منحنی Curve۲۵۵۱۹ تبادل شدند.

نتایج بررسی به‌صورت کیفی در جدول ۲ خلاصه شده است. همان‌طور که مشاهده می‌شود، AES-۱۲۸-CCM به دلیل ساختار بلوکی و نیاز به حافظه بیشتر، فشار زیادی بر منابع CPU و RAM وارد می‌کند و تأخیر بالاتری دارد، در حالی که ChaCha۲۰-Poly۱۳۰۵ با ساختار مبتنی بر عملیات جمع، جابجایی، چرخش (ARX) کارآمدتر بوده و تعادل مناسبی بین امنیت و کارایی ایجاد می‌کند. روش بدون رمزنگاری نیز از نظر مصرف منابع بهینه است، اما در برابر حملات جعل و Replay هیچ مقاومتی ندارد.

جدول ۲ نتایج تست در روش‌های مورد بررسی

معیار	بدون رمزنگاری	AES-۱۲۸-CCM	ChaCha۲۰-Poly۱۳۰۵
مصرفCPU	بسیار کم	زیاد (بار پردازشی بالا)	کم تا متوسط (کارآمد روی ۳۲بیتی)
تأخیر انتقال(Latency)	کم	بالا	متوسط (قابل قبول)
مصرف حافظهRAM	کم	زیاد	متوسط
مقاومت در برابر حملات جعل/Replay	ندارد	بالا (دارای احراز اصالت پیام)	بالا (دارای احراز اصالت پیام)
قابلیت بازیابی داده سالم	بالا (ولی قابل جعل)	بالا (با رد داده جعلی)	بالا (با رد داده جعلی)
مناسب بودن برای دستگاه‌های کم‌منبع	بسیار مناسب	محدودیت‌زا برایMCU ضعیف	مناسب (متعادل)

یافته‌های کلیدی:

- ChaCha۲۰-Poly۱۳۰۵ در تمام معیارها عملکرد بهتری نسبت به AES-CCM داشت.
- مصرف CPU در ChaCha۲۰ به‌دلیل ساختار جمع، جابجایی، چرخش (ARX) در پردازنده‌های ۳۲ بیتی بسیار کارآمدتر است.
- استفاده از Curve۲۵۵۱۹ برای تبادل کلید، با کاهش حجم داده نسبت به۲۰۴۸-RSA، انتقال اولیه را تسریع کرد.

بحث و نتیجه‌گیری:

جمع‌آوری داده‌های عملیاتی در صنعت تایرسازی امری حیاتی است، صرف‌نظر از اینکه این داده‌ها از طریق PLC یا دستگاه‌های IoT مکمل جمع‌آوری شوند. در سیستم‌های مدرن، دستگاه‌های IoT به‌عنوان یک راهکار مقیاس‌پذیر و انعطاف‌پذیر برای دیجیتال‌سازی ماشین‌های قدیمی یا ماشین‌های فاقد شبکه، نقش مهمی ایفا می‌کنند. با این حال، انتقال داده از هر منبعی باید امن باشد.

مطالعه موردی نشان داد که روش‌های رمزنگاری سبک می‌توانند تعادل مناسبی بین امنیت و کارایی ایجاد کنند، به‌ویژه در دستگاه‌های با منابع محدود. در این میان،ChaCha۲۰-Poly۱۳۰۵ با حفظ تأخیر پایین و کاهش فشار پردازشی نسبت به AES-۱۲۸-CCM، گزینه‌ای کارآمدتر محسوب می‌شود. این روش به‌ویژه برای داده‌های با نرخ بالا (مانند ویبره‌سنج‌ها) و داده‌های حساس (مانند پرس پخت) مناسب است. در مقابل،AES-CCM با وجود امنیت بالا، به دلیل مصرف منابع بیشتر، بیشتر برای دستگاه‌های قدرتمندتر قابل توصیه است. همچنین، استفاده ازECC (به‌ویژهCurve۲۵۵۱۹) برای تبادل کلید، به دلیل طول کلید کوتاه و امنیت بالا، راهکاری عملی و بهینه به شمار می‌آید.

با توجه به انتشار پیش‌نویس اولیه استاندارد SP ۸۰۰-۲۳۲ توسط NIST در نوامبر ۲۰۲۴ و معرفی Ascon به‌عنوان الگوریتم استاندارد رمزنگاری سبک، آینده امنیت دستگاه‌های بسیار محدود روشن‌تر خواهد بود. با این حال، در دستگاه‌های با پردازنده ۳۲ بیتی و بدون واحد رمزنگاری سخت‌افزاری، ChaCha۲۰-Poly۱۳۰۵ همچنان گزینه‌ای عملی و متوازن است.

در نهایت، پیشنهاد می‌شود:

- در خطوط تولید تایر، از پروتکل‌های امن مبتنی بر DTLS یا TLS ۱,۳ با cipher suite سبک استفاده شود.
- مدیریت کلیدها به صورت متمرکز و امن (مثلاً با استفاده ازHSM) انجام شود.
- تست‌های امنیتی دوره‌ای برای شناسایی آسیب‌پذیری‌های شبکه انجام شود.
- از رویکردهای امنیت تطبیقی استفاده شود تا سطح رمزنگاری با حساسیت داده تنظیم شود.

این راهکارها می‌توانند به افزایش امنیت سایبری، قابلیت اطمینان تولید و حفظ مالکیت معنوی فرآیندهای صنعتی کمک کنند.

مراجع:

[۱] Lee, J., Bagheri, B., & Kao, H. A. (۲۰۱۵). A cyber-physical systems architecture for industry ٤,٠-based manufacturing systems. Manufacturing Letters, ۳, ۱۸-۲۳.

[۲] I. Radhakrishnan, S. Jadon, and P. B. Honnavalli, “Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices,” Sensors, vol. ۲٤, p. ٤۰۰۸, ۲۰۲٤

[۳] National Institute of Standards and Technology (NIST). (۲۰۲۴). Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions (Initial Public Draft of SP ۸۰۰-۲۳۲). https://csrc.nist.gov/Projects/Lightweight-Cryptography