« به نام خدا »

محمدمهدی احمدیان

پژوهشگر ،مشاور و مدرس حوزه امنیت سامانه‌های کنترل صنعتی (کاندیدای دکتری تخصصی)

www.mmAhmadian.ir

Ahmadian.blog.ir

۰۹۱۲۰۴۶۲۴۹۵

https://t.me/MohammadMehdiAhmadian

mm.Ahmadian[at]aut[dot]ac[dot]ir

@mmAhmadian

نسخه:

این سند، نسخه‌ای عمومی از رزومه شخصی محمدمهدی احمدیان است که صرفاً جهت انتشار در وبگاه شخصی وی منتشرشده است و فاقد هر گونه ارزش دیگری است. هرگونه استفاده از آن بدون کسب مجوز کتبی از ایشان پیگرد قانونی دارد. در این رزومه به دلیل توافق‌نامه عدم افشاء(NDA) در برخی پروژه‌ها ، تنها محتوای فاقد طبقه‌بندی ذکرشده است.

(تاریخ به‌روزرسانی سند : ۱۳۹۸/۰۸/۰۶، تاریخ اعتبار سند: ۱۳۹۹/۰۸/۰۶)

معرفی مختصر:

(با حفظ گمنامی پروژه‌ها)

محمدمهدی احمدیان، پژوهشگر، مدرس و مشاور حوزه امنیت سامانه‌های کنترل صنعتی(ICS) و زیرساخت‌های حیاتی است که تحصیلات کارشناسی خود را در رشته مهندسی کامپیوتر(گرایش نرم‌افزار) و سپس کارشناسی ارشد خود را در رشته فناوری اطلاعات (گرایش امنیت اطلاعات) پشت سر گذاشته است و در حال حاضر کاندیدای دکتری تخصصی رشته فناوری اطلاعات(گرایش امنیت اطلاعات) دانشگاه صنعتی امیرکبیر و پژوهشگر مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق است. وی بالغ‌بر شش سال است که زیر نظر اساتید مجرب و حاذق کشور تحصیلات تخصصی خود را در حوزه امنیت اطلاعات ادامه داده است و در پروژه‌های متعدد امنیت سایبری و امنیت سایبر-فیزیکی در حوزه‌های کنترل صنعتی و زیرساخت‌های حیاتی در سطوح مختلف کشوری و در رده‌های گوناگون (مشاوره، نظارت، مدیریت، طراحی و اجرا) فعالیت داشته است.

حوزه‌های تحقیقاتی و اجرایی:

امنیت سامانه‌های سایبر- فیزیکی

امنیت سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی	★★★★★★★★★★
ارزیابی مخاطرات سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی	★★★★★★★★★☆
تحلیل آسیب‌پذیری‌های امنیتی سامانه‌های کنترل صنعتی	★★★★★★★★☆☆
طراحی و پیاده‌سازی معماری امن در سامانه‌های کنترل صنعتی	★★★★★★★☆☆☆
تحلیل جریان اطلاعات در سامانه‌های سایبر-فیزیکی	★★★★★★☆☆☆☆
مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی	★★★★★★☆☆☆☆

مدیریت امنیت اطلاعات

ارزیابی مخاطرات امنیتی سامانه‌های سایبری	★★★★★★☆☆☆☆

نسخه عمومی رزومه
طرح جهت انتشار در وبگاه شخصی
www.mmAhmadian.ir

تحلیل آسیب‌پذیری‌های امنیتی سامانه‌های سایبری ★★★★★☆☆☆☆☆

امنیت شبکه و سیستم‌عامل

تشخیص بدافزارها ★★★★☆☆☆☆☆☆

تحلیل بدافزارها ★★★☆☆☆☆☆☆☆

چرخه توسعه امن نرم‌افزار

طراحی امن نرم‌افزار ★★★★☆☆☆☆☆☆

پیاده‌سازی امن نرم‌افزار ★★☆☆☆☆☆☆☆☆

سوابق کاری:
(فاقد طبقه‌بندی)

پژوهشگر و مدرس مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور (پژوهشگاه نیرو- وزارت نیرو)(۱۳۹۷- تاکنون)

پژوهشگر و مدرس مرکز امنیت سایبر صنعتی گروه مپنا (۱۳۹۸- تاکنون)

مدیر فنی شرکت دانش‌بنیان مهندسی گسترش سامانه امن دانشگاه صنعتی امیرکبیر (۱۳۹۷- خرداد ۱۳۹۸)

مشاور امنیت اطلاعات سامانه‌های کنترل صنعتی شرکت گسترش فناوری پارس امین رای (۱۳۹۶-۱۳۹۵)

سرپرست تیم امنیت سایبری سامانه‌های کنترل صنعتی دانشگاه صنعتی امیرکبیر (۱۳۹۴-۱۳۹۵)

طراح آزمایشگاه تحلیل بدافزار سامانه‌های کنترل صنعتی مرکز اتوماسیون صنعتی و ارزیابی امنیتی دانشگاه خاتم (۱۳۹۵)

پژوهشگر و دستیار پژوهشی آزمایشگاه امنیت اطلاعات و تجارت الکترونیک دانشگاه صنعتی امیرکبیر (تاکنون-۱۳۹۴)

مدیر تیم امنیت اطلاعات پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر (۱۳۹۳-۱۳۹۴)

پژوهشگر و دستیار پژوهشی آزمایشگاه طراحی و تحلیل سیستم‌های امن دانشگاه صنعتی امیرکبیر (۱۳۹۲-۱۳۹۴)

پژوهشگر تیم امنیت کنترل صنعتی پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر (۱۳۹۲-۱۳۹۳)

مهارت‌ها:

تدریس دوره‌های آموزشی و کارگاه‌های تخصصی امنیت سامانه‌های کنترل صنعتی ★★★★★★★★★★

مشاوره و اجرای طرح‌های جامع امن سازی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی ★★★★★★★★★★

ارزیابی امنیتی سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی ★★★★★★★★★★

طراحی نقشه راه امن سازی سایبری سامانه‌های سایبری و سایبر-فیزیکی ★★★★★★★★★☆

مدل‌سازی امنیتی سامانه‌های سایبر- فیزیکی ★★★★★★★☆☆☆

تحلیل جریان اطلاعات در سامانه‌های سایبر-فیزیکی ★★★★★★☆☆☆☆

طراحی و راه‌اندازی آزمایشگاه‌های ارزیابی امنیتی سامانه‌های کنترل صنعتی ★★★★★★☆☆☆☆

نسخه عمومی رزومه
صرفاً جهت انتشار در وبگاه شخصی
www.m.m.Ahmadian.ir

سوابق تحصیلی:

مدرک تحصیلی	رشته تحصیلی و گرایش	تاریخ اخذ مدرک	نام دانشگاه	نوع پذیرش/سهمیه	معدل	افتخارات/ رتبه
دکتری تخصصی	فناوری اطلاعات – امنیت اطلاعات	۱۳۹۸ (مورد انتظار)	صنعتی امیرکبیر(تهران)	روزانه / استعدادهای درخشان	-	(۱ از ۱)
کارشناسی ارشد	فناوری اطلاعات – امنیت اطلاعات	۱۳۹۴	صنعتی امیرکبیر(تهران)	روزانه / کنکور سراسری	۱۸,۱۶	رتبه یک (ممتاز) (۱ از ۱۱)
کارشناسی	کامپیوتر- نرم‌افزار	۱۳۹۱	شمال(آمل)	غیرانتفاعی/ کنکور سراسری	۱۹,۵۶	رتبه یک (ممتاز) (۱ از ۹۵)
کاردانی	کامپیوتر- نرم‌افزار	۱۳۸۸	مرکز آموزش عالی امام علی(ع)(یزد)	روزانه / کنکور سراسری	۱۹,۰۸	رتبه یک (ممتاز) (۱ از ۳۵)

عناوین برخی فعالیت های کاری:

(فاقد طبقه‌بندی)

- همکاری با کارفرما در پروژه شناسایی دارایی‌های مبتنی بر ICT در سه نیروگاه نمونه و مدیریت مخاطرات امنیتی‌های مرتبط با امنیت (مشاور کارفرما از ۱۳۹۷- ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- سفارشی‌سازی دوره آموزشی با عنوان «امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی صنعت برق و راهکارهای ارتقاء آن (با تمرکز بر حوزه‌های برق حرارتی و منابع آب)» (مدرس: ۱۳۹۸) [کارگروه تخصصی آموزش و آگاهی‌رسانی امنیت صنعت برق]
- سفارشی‌سازی دوره آموزشی با عنوان «امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی صنعت برق و راهکارهای ارتقاء آن (با تمرکز بر حوزه‌های توزیع و انتقال)» (مدرس: ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- استخراج و تدوین محتوای آموزشی تجزیه‌وتحلیل حملات سایبری و سناریوهای نفوذ به صنعت برق (پژوهشگر و مدرس ۱۳۹۷- ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- همکاری در پروژه طراحی و اجرای پایلوت زیرسامانه‌های مبتنی بر ICT صنعتی نیروگاه و ارزیابی امنیتی آن‌ها (کارشناس پروژه از ۱۳۹۷- تاکنون) [مرکز توسعه امنیت صنعت برق کشور]
- تدوین محتوای آموزشی تجزیه‌وتحلیل حملات سایبری و سناریوهای نفوذ به صنعت برق (پژوهشگر و مدرس: ۱۳۹۷- تاکنون) [مرکز توسعه امنیت صنعت برق کشور]
- تدوین محتوای آموزشی تشریح و اجرای سناریوهایی حملات سایبری و تست نفوذ به سامانه‌های صنعتی حوزه انرژی
- (پژوهشگر و مدرس: ۱۳۹۷- تاکنون) [مرکز توسعه امنیت صنعت برق کشور]
- همکاری با کمیته امنیت توانیر در پروژه شناخت وضعیت امنیتی صنعت برق در حوزه برق‌های منطقه‌ای (مشاور و ارزیاب ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
  - ارزیابی امنیتی شرکت برق منطقه ای زنجان (لینک خبر)
  - ارزیابی امنیتی مرکز دیسپاچینگ پشتیبان زنجان
  - ارزیابی امنیتی پست برق معنوی - تهران

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

- تهیه‌کننده چک‌لیست ارزیابی امنیتی خاص شبکه‌های صنعتی و اسکادا صنعت برق [در قالب همکاری مشترک دانشگاه صنعتی امیرکبیر و مرکز توسعه امنیت صنعت برق کشور]

- انجام خدمات مشاوره به شرکت توزیع نیروی برق شمال استان کرمان (مشاور و مدرس ۱۳۹۸)
- تهیه متدولوژی تلفیقی مدیریت مخاطرات امنیتی مربوط به اتوماسیون شبکه توزیع برق (مدیر فنی و مشاور: ۱۳۹۸) [شرکت مهندسی گسترش سامانه امن]
- همکاری در پروژه طراحی و پیاده‌سازی یک محصول ارزیابی امنیتی (مدیر پروژه: ۱۳۹۸) [شرکت مهندسی گسترش سامانه امن]
- همکاری با کارفرما در پروژه پایگاه دانش آسیب‌پذیری‌های امنیتی، تهدیدات، حملات و بدافزارهای سامانه‌های کنترل و اتوماسیون صنعت برق (مشاور کارفرما از ۱۳۹۷- ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- همکاری با کارفرما در پروژه طراحی و تدوین سازوکار ایجاد ساختار تنظیم مقررات امنیتی و نظارت بر اجرای آن در صنعت برق (مشاور کارفرما از ۱۳۹۷- ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- مأموریت بررسی اضطراری حوادث قطع برق سراسری ونزوئلا و تهیه گزارش برای وزیر محترم نیرو (کارشناس فنی: ۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]
- بررسی تخصصی و داوری سند «الزامات امنیتی عملیاتی زیرساخت‌های حیاتی (فاوا و صنعتی)» (خدمت مشاوره ۱۳۹۷) [مرکز توسعه امنیت صنعت برق کشور]*
- بررسی و داوری سند «طرح‌های پاسخ اضطراری سایبری در حوزه انرژی همراه با الگوی کلی رزمایش سایبری در دستگاه‌های اجرایی» (خدمت مشاوره: ۱۳۹۷) [مرکز توسعه امنیت صنعت برق کشور]*
- بررسی و داوری «راه‌حل جامع امنیت سایبری استقرار سیستم مانیتورینگ و داده‌برداری در نیروگاه‌های پایلوت فریم ۹» (خدمت مشاوره محدود: ۱۳۹۷-۱۳۹۸) [مرکز توسعه امنیت صنعت برق کشور]*
- بررسی و داوری «طرح امن سازی زیرساخت‌های حیاتی در قبال حملات الکترونیکی» (خدمت مشاوره: ۱۳۹۷) [مرکز توسعه امنیت صنعت برق کشور]*
- تهیه پیشنهاد فنی ارزشیابی مخاطرات امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی یکی از مناطق عملیاتی انتقال گاز کشور (مدیر فنی و مشاور: ۱۳۹۷)[شرکت مهندسی گسترش سامانه امن]
- ارائه پیشنهاد فنی تحلیل تهدیدات و ارزشیابی مخاطرات امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی یکی از شرکت‌های ملی نفت جنوب (مدیر فنی و مشاور: ۱۳۹۷) [شرکت مهندسی گسترش سامانه امن]
- داوری مقاله در حوزه امنیت سامانه‌های کنترل و اتوماسیون صنعتی، کنفرانس بین‌المللی حفاظت و اتوماسیون در سیستم‌های قدرت (IPAPS 2019)، دانشگاه صنعتی شریف (خدمت مشاوره ۱۳۹۷) [مرکز توسعه امنیت صنعت برق کشور]
- همکاری در طراحی مفهومی آزمایشگاه تحلیل و تشخیص بدافزارها و تحلیل آسیب‌پذیری‌های سامانه‌های کنترل صنعتی (کارشناس و مشاور: ۱۳۹۵) [آزمایشگاه اتوماسیون صنعتی و ارزیابی امنیتی دانشگاه خاتم]
- عضو گروه ارزیاب امنیتی مرکز دیسپاچینگ ملی برق ایران (۱۳۹۵- با شرکت همکار)
- همکاری در پروژه طراحی و توسعه نرم‌افزار ارزیاب امنیت سامانه‌های کنترل صنعتی (کارشناس، سرپرست گروه امنیت و برنامه‌نویسی از ۱۳۹۲ تا ۱۳۹۴) [تیم امنیت سایبری سامانه‌های صنعتی دانشگاه صنعتی امیرکبیر]
- همکاری در پروژه طراحی و توسعه پایگاه دانش آسیب‌پذیری‌ها، تهدیدات و بدافزارهای حوزه سامانه‌های کنترل صنعتی (کارشناس، سرپرست گروه امنیت و برنامه‌نویسی از ۱۳۹۳ تا ۱۳۹۵) [تیم امنیت سایبری سامانه‌های صنعتی دانشگاه صنعتی امیرکبیر]
- ...

نسخه عمومی وبگاه شخصی
مرجع جمع آوری و انتشار دکتر م. م. احمدیان
www.mmahmadian.ir

دوره‌ها و دروس امنیتی/مرتبط با امنیت گذرانده شده:

عنوان درس/دوره	مدرس	محل ارائه	سال	نمره
مدل‌های فورمال و امنیت اطلاعات	دکتر مهران سلیمان فلاح	دانشگاه صنعتی امیرکبیر	۱۳۹۵	B
امنیت سیستم‌های نرم‌افزاری	دکتر مهران سلیمان فلاح	دانشگاه صنعتی امیرکبیر	۱۳۹۵	A
امنیت تجارت الکترونیکی	دکتر حمیدرضا شهریاری	دانشگاه صنعتی امیرکبیر	۱۳۹۵	A
امنیت شبکه	دکتر سیاوش خرسندی	دانشگاه صنعتی امیرکبیر	۱۳۹۴	B
مباحث ویژه (تحلیل آسیب‌پذیری نرم‌افزار)	دکتر حمیدرضا شهریاری	دانشگاه صنعتی امیرکبیر	۱۳۹۳	A
مباحث پیشرفته در امنیت اطلاعات	دکتر مهدی شجری	دانشگاه صنعتی امیرکبیر	۱۳۹۳	A
امنیت پایگاه داده‌ها	دکتر حمیدرضا شهریاری	دانشگاه صنعتی امیرکبیر	۱۳۹۳	A
پروتکل‌های امنیتی	دکتر بابک صادقیان	دانشگاه صنعتی امیرکبیر	۱۳۹۳	B
سیستم‌های کامپیوتری امن	دکتر مهدی شجری	دانشگاه صنعتی امیرکبیر	۱۳۹۲	A
مبانی امنیت اطلاعات	دکتر مهران سلیمان فلاح	دانشگاه صنعتی امیرکبیر	۱۳۹۲	A
معما شناسی کاربردی	دکتر بابک صادقیان	دانشگاه صنعتی امیرکبیر	۱۳۹۲	B
سیستم‌های پرداخت الکترونیکی	دکتر مهدی شجری	دانشگاه صنعتی امیرکبیر	۱۳۹۵	A
شبکه‌های کامپیوتری پیشرفته	دکتر سیاوش خرسندی	دانشگاه صنعتی امیرکبیر	۱۳۹۴	B
دوره فورنسیک مقدماتی	دکتر بابک صادقیان و همکاران	آپا دانشگاه صنعتی امیرکبیر	۱۳۹۳	بدون آزمون
دوره فورنسیک پیشرفته	دکتر بابک صادقیان و همکاران	آپا دانشگاه صنعتی امیرکبیر	۱۳۹۲	بدون آزمون
دوره تست نفوذ پیشرفته وب	مهندس دهکردی	آپا دانشگاه صنعتی امیرکبیر	۱۳۹۳	بدون آزمون

نسخه عمومی رزومه
صرفاً جهت انتشار در وبگاه شخصی
www.mmAhmadian.ir

دوره تست نفوذ مقدماتی	دکتر نیک صفت و همکاران	آپا دانشگاه صنعتی امیرکبیر	۱۳۹۲	A

مقالات کنفرانس:

- Saeid Salehi, Hamidreza Shahriari, Mohammad Mehdi Ahmadian, Ladan Tazik, **A Novel Approach for Detecting DGA-based Ransomwares**. In Information Security and Cryptology (ISCISC), 2018 15th International Iranian Society of Cryptology Conference on 2018 Sep 28-29. IEEE.*(link)*
- Ahmadian M. M, *Rezazadeh B. , Dezfouli M., Shajari M,* **Towards Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats** *[In Persian]*. In Information Security and Cryptology (ISCISC), 2017 14th International Iranian Society of Cryptology Conference on 2017 Sep 6-7. IEEE.*(link)*
- N. Mousavi ,*Shajari M* ,Ahmadian M. M, **Implementation of the software testing environment for attacks against the Modbus Protocol** *[In Persian]*. In Information Security and Cryptology (ISCISC), 2017 14th International Iranian Society of Cryptology Conference on 2017 Sep 6-7. IEEE.*(link)*
- Nasiri A., Hajatipour M, Ahmadian M. M., **Combination of Fault Tolerant Controller and Gyro Bias Observer in Satellite Attitude Determination System**, 21st Computer Science and Software Engineering Conference (CSSE 2017), Shiraz, Iran, Oct. 2017.*(link)*
- *Ahmadian MM, Shahriari HR, Ghaffarian SM.* ***Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares****. In Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on 2015 Sep 8 (pp. 79-84). IEEE.(link)*
- *Ahmadian MM, Shahriari HR.* ***2entFOX: A framework for high survivable ransomwares detection****. InInformation Security and Cryptology (ISCISC), 2016 13th International Iranian Society of Cryptology Conference on 2016 Sep 7 (pp. 79-84). IEEE.(link)*
- *Ahmadian MM, Shahriari HR.* ***A framework for Detecting High Survivable Ransomwares using hybrid behavioral analysis and Bayesian network****(In Persian) ,, 21st National CSI Computer Conference , Iran (Islamic Republic of) , 08 March2016 _ 10 March2016*
- *Ahmadian MM, Sadra Kardan,* ***Propose a new algorithm for calculating the value of nodes in search strategies (Case Study:8-Puzzle problem)*** *[In Persian], International Conference on Nonlinear Modeling & Optimization, Amol, Iran, Aug 2012(link)*
- *Ahmadian MM, Sadra Kardan,* ***Propose a new Algorithm for Decreasing Time Complexity in A-Star Informed search (Case Study:8-Puzzle problem)*** *[In Persian], International Conference on Nonlinear Modeling & Optimization, Amol, Iran, Aug 2012(link)*
- *Sadra Kardan, Ahmadian MM,* ***Propose a new algorithm for decreasing space complexity in A-Star Informed search (Case Study:8-Puzzle problem)*** *[In Persian], International Conference on Nonlinear Modeling & Optimization, Amol, Iran, Aug 2012.(link)*

مقالات ژورنال:

- *Ahmadian M.M., et al.* ***High Survivable Ransomwares Detection Using Bayesian Belief Network and Hybrid Behavioral Analysis Features****, Journal of Computer Virology and Hacking Techniques,[Under Review].Submission Date: Jan 31, 2018.*

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

- *Ahmadian M.M. , Mehdi Shajari. , IEC 60870-5-104 Protocol Security Challenges and Countermeasures Identification [In Persian]. Biannual Journal Monadi for Cyberspace Security (AFTA) , . 2019; 7 (2) :30-15 (Link).*
- *Ahmadian M.M. , Mehdi Shajari. Shafeie MA , **Industrial Control Systems Security: An Analytical Incidents Survey and a Taxonomic Framework**.* International Journal of Critical Infrastructure Protection (Elsevier) *, [Under Revision].Submission Date:* Aug *12,2018.*

طرح‌های کلان ملی:

نام طرح	وزارت خانه متولی	دستاوردها	سمت در طرح
طرح کلان ملی راه‌اندازی مرکز ملی دفاع سایبری(پروژه طراحی و راه‌اندازی سامانه جامع مقابله با بدافزارها در زیرساخت‌های حیاتی کشور)	وزارت علوم تحقیقات و فناوری	• تدوین نقشه راه وضعیت امنیت سایبری سامانه‌های صنعتی • طراحی و پیاده‌سازی پروژه نرم‌افزار ارزیاب امنیت سامانه‌های کنترل صنعتی • طراحی و پیاده‌سازی پایگاه دانش آسیب‌پذیری ها،تهدیدات و بدافزارهای حوزه سامانه‌های کنترل صنعتی • طراحی مفهومی آزمایشگاه تحلیل و تشخیص بدافزارها و تحلیل آسیب‌پذیری‌های سامانه‌های کنترل صنعتی	سرپرست گروه امنیت اطلاعات در تیم امنیت سایبری سامانه‌های صنعتی دانشگاه صنعتی امیرکبیر
طرح و پروژه ملی راه‌اندازی اینترانت ملی	وزارت ارتباطات و فناوری اطلاعات	• توسعه اینترانت ملی در کلیه نواحی و حوزه‌های درگیر در محدوده واگذارشده.	سرپرست و مجری

نسخه عمومی رزومه صفا جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

کتب:

عنوان کتاب	تألیف یا ترجمه	نام نویسندگان به ترتیب ذکرشده در شناسنامه کتاب	سال انتشار
پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری	تألیف و گرداوری	محمدمهدی احمدیان ، بابک رضازاده	۱۳۹۶
هنر امنیت ؛ ۱۰۰ نکته در حوزه امنیت سایبری	تألیف و گرداوری	محمدمهدی احمدیان	۱۳۹۸(در حال گذر مراحل چاپ)
دست‌نوشته‌های شکست ،پلی تا موفقیت	تألیف	محمدمهدی احمدیان	۱۳۹۱

سوابق پژوهشی (سخنرانی، ارائه علمی، دوره آموزشی و نشست علمی):

عنوان	عنوان انگلیسی	وابسته به	محل ارائه	زمان	اسلاید یا خبر
سمینار امنیت سایبری در سامانه‌های کنترل صنعتی صنعت برق	*Industrial Control Systems Cyber Security in Power Industry*	مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور	شرکت توزیع نیروی برق شمال استان کرمان	۱۷ شهریور ۱۳۹۸	
نشست طرح مسئله امنیت اتوماسیون صنعتی و اینترنت اشیاء	*ICS Security Session : Industrial Automation Cyber Security and Internet of Things*	پژوهشگاه نیرو و دبیرخانه انجمن رمز ایران	شانزدهمین کنفرانس بین‌المللی انجمن رمز، تهران، دانشگاه فردوسی مشهد	۷ شهریور ۱۳۹۸	لینک خبر
دوره آموزشی « تجزیه‌وتحلیل حملات سایبری و سناریوهای نفوذ به صنعت برق: نکته‌ها و آموزه‌ها»	*Analysis of cyber attacks and intrusion scenarios in power industry: tips and tricks*	مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور (پژوهشگاه نیرو)	شانزدهمین کنفرانس بین‌المللی انجمن رمز، تهران، دانشگاه فردوسی مشهد	۵ شهریور ۱۳۹۸	لینک خبر
دوره آموزشی سه روزه تئوری و عملی امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی صنعت برق و راهکارهای ارتقاء آن (با تمرکز بر حوزه‌های توزیع و انتقال)	*Cybersecurity in Industrial Automation and Control Systems Of The Power Industry (Case Study: Power Distribution And Transmission)*	مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور (پژوهشگاه نیرو)	آموزشگاه رایان کالج و پژوهشگاه نیرو (مجموعا ۱۲ روز)	هفته اول تا هفته آخر مرداد ۱۳۹۸	لینک خبر
کارگاه کالبدشکافی حملات سایبری به صنعت برق و پیاده سازی عملی حملات پایه به شبکه اتوماسیون توزیع	*Workshop on Dissection of Cyber Attacks on Power Industry beside Hacking the Electrical Distribution Networks*	مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور (پژوهشگاه نیرو)	بیست و چهارمین کنفرانس شبکه های توزیع نیروی برق (epdc24 2019) ، دانشگاه لرستان	۳۰ خرداد ۱۳۹۸	لینک آگهی
اجرای عملی سناریوی نمونه حملات سایبری و تست نفوذ به سامانه‌های اسکادا حوزه انرژی	*Hacking and Penetration Testing Scenarios of SCADA Systems of Energy*	مرکز توسعه امنیت فناوری اطلاعات و ارتباطات صنعت برق کشور (پژوهشگاه نیرو)	کنفرانس بین‌المللی حفاظت و اتوماسیون در سیستم‌های قدرت (IPAPS 2019) ، دانشگاه صنعتی شریف	۱۹ و ۲۰ دی‌ماه ۱۳۹۷	لینک آگهی
دوره آموزشی دو روزه پدافندغیرعامل و امنیت سایبری در سامانه‌های کنترل و اتوماسیون صنعتی (محتوای ۱۶ ساعته)	*Passive Defense and Cyber Security in Industrial Control & Automation Systems*	راهبران پتروشیمی	پتروشیمی خارک	۲۲ و ۲۳ آذر ماه ۱۳۹۷	لینک آگهی

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.Ahmadian.ir

های کنترل سخنرانی امنیت سامانه صنعتی و ارتقاء آن	*Cyber Security Hardening in Industrial Control Systems*	افتای ریاست جمهوری و سازمان پدافند غیرعامل. برگزاری سمینار به نمایندگی شرکت پارس آوان	اهواز	۲۱ آبان ۱۳۹۷	لینک خبر
حملات کنترل صنعتی، از حرف تا عمل (پیاده سازی حملات پایه در شبکه های کنترل صنعتی به همراه اجرای راهکارهای مقابله)	*Hacking Exposed Industrial Control Systems*	---- (عدم انتشار در نسخه عمومی دوره)	پانزدهمین کنفرانس بین‌المللی انجمن رمز، تهران، دانشگاه شهید رجایی	۷ شهریور ۱۳۹۷	لینک آگهی ارائه با (با همکار)
های کنترل سخنرانی امنیت سامانه (همراه با اجرای عملی دو صنعتی ساعته حملات سایبری به سامانه‌های اتوماسیون صنعتی)	*Cyber Security in Industrial Control Systems*	افتای ریاست جمهوری	مشهد، سالن همایش‌های سازمان مدیریت وبرنامه ریزی خراسان رضوی	۶ شهریور ۱۳۹۷	ارائه با (با همکار)
سخنرانی چالش‌های امنیتی در سامانه‌های سایبر-فیزیکی (با محوریت تحلیل جریان اطلاعات در خطوط لوله نفت و گاز)	*Cyber–Physical Systems Security Challenges (Case study: Information Flow Security Analysis in Natural Gas and Oil Pipeline System)*	آزمایشگاه امنیت اطلاعات و تجارت الکترونیک، دانشگاه صنعتی امیرکبیر	ششمین کنفرانس فناوری اطلاعات و ارتباطات در نفت، گاز ،پالایش و پتروشیمی، تهران، دانشگاه شهید بهشتی	۲۷ دی‌ماه ۱۳۹۶	لینک
شناسایی تهدیدات و آسیب‌پذیری‌های امنیتی پروتکل IEC 60870-5-104 کنترل صنعتی	*Towards the Identification of IEC 60870-5-104 Protocol Security Vulnerabilities and Threats*	---- (عدم انتشار در نسخه عمومی دوره)	چهاردهمین کنفرانس بین‌المللی انجمن رمز، شیراز، دانشگاه شیراز	۱۶ شهریور ۱۳۹۶	لینک آگهی
کارگاه آموزشی امنیت اطلاعات در سامانه‌های کنترل صنعتی : چالش‌ها و راهکارها	*Information Security in Industrial Control Systems: Challenges and Solutions*	---- (عدم انتشار در نسخه عمومی دوره)	چهاردهمین کنفرانس بین‌المللی انجمن رمز شیراز، دانشگاه شیراز	۱۴ شهریور ۱۳۹۶	لینک آگهی
ارائه علمی تحلیل و وارسی صوری امنیت جریان اطلاعات در سامانه‌های سایبری-فیزیکی، مطالعه موردی : سامانه انتقال(خطوط لوله) گاز	*Formal Analysis and Verification of information flow security in cyber–physical systems, Case study: natural gas pipeline system*	آزمایشگاه امنیت اطلاعات و تجارت الکترونیک، دانشگاه صنعتی امیرکبیر	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۵	
ارائه علمی درآمدی بر سامانه‌های سایبری-فیزیکی و چالش‌های	*Introduction to cyber–physical systems and their security*	آزمایشگاه امنیت اطلاعات و تجارت	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۵	

نسخه عمومی رزومه
صرفاً جهت انتشار در وبگاه شخصی
www.MAhmadian.ir

امنیتی آن‌ها، حوزه محوری: سامانه‌های کنترل صنعتی	*challenges, Case study: ICSs*	الکترونیک، دانشگاه صنعتی امیرکبیر			
سخنرانی چالش‌ها و راهکارهای امنیتی در سامانه‌های کنترل صنعتی	*security challenges and solutions in ICSs*	---- (عدم انتشار در نسخه عمومی دوره)	---- (عدم انتشار در نسخه عمومی دوره)	آبان ۱۳۹۵	
مقدمه‌ای بر خط‌مشی‌های امنیتی پویا	*An Introduction to Dynamic Security Policy (a sub-class of Dynamic Security)*	آزمایشگاه امنیت اطلاعات و تجارت الکترونیک، دانشگاه صنعتی امیرکبیر	دانشگاه صنعتی امیرکبیر	بهمن و اسفند ۱۳۹۵	
صحت جریان کنترل	*Control Flow Integrity*	آزمایشگاه امنیت اطلاعات و تجارت الکترونیک، دانشگاه صنعتی امیرکبیر	دانشگاه صنعتی امیرکبیر	اسفند ۱۳۹۵	لینک
به‌منظور ***2entFOX***چارچوب تشخیص باجگیرافزارهای بقاپذیر	*2entFOX: A Framework for High Survivable Ransomwares Detection*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	سیزدهمین کنفرانس بین‌المللی انجمن رمز، تهران، دانشگاه شهید بهشتی	شهریور ۱۳۹۵	لینک
بررسی برخی تهدیدات امنیتی در طراحی بیتکوین ، امکان‌سنجی حملات مرتبط با آن‌ها و طرح چند ابهام امنیتی		آزمایشگاه امنیت اطلاعات و تجارت الکترونیک، دانشگاه صنعتی امیرکبیر	دانشگاه صنعتی امیرکبیر	تیر ۱۳۹۵	
کارگاه آموزشی امنیت سایبری در سامانه‌های کنترل صنعتی	*Cyber Security in Industrial control systems*	تیم امنیت سایبری سامانه‌های کنترل صنعتی دانشگاه صنعتی امیرکبیر (به سرپرستی دکتر احمد افشار)	شرکت ملی گاز ایران، تهران	اسفند ۱۳۹۴	لینک
چارچوبی به‌منظور تشخیص باجگیرافزارهای بقاپذیر به کمک تحلیل ترکیبی رفتاری برنامه‌ها و شبکه بیزی	*A framework for Detecting High Survivable Ransomwares using hybrid behavioral analysis and Bayesian network*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	بیست‌ویک مین کنفرانس ملی سالانه انجمن کامپیوتر ایران، تهران، پژوهشگاه دانش‌های بنیادی	اسفند ۱۳۹۴	
چارچوبی به‌منظور تشخیص باجگیرافزارها به کمک تحلیل رفتار پویای برنامه	*A Framework for Ransomware Detection Based on Behavioral Analysis*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	مهر ۱۳۹۴	

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

نظارت بر ارتباط و قطع ارتباط : رویکردی نوین جهت پیشگیری و تشخیص باجگیرافزارهای بقاپذیر	*Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares.*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دوازدهمین کنفرانس بین‌المللی انجمن رمز، گیلان، دانشگاه رشت	شهریور ۱۳۹۴	
سخنرانی امنیت سایبری سامانه‌های کنترل صنعتی در صنایع نفت، گاز، پالایش و پتروشیمی		پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر (به سرپرستی دکتر احمد افشار)	سومین کنفرانس و نمایشگاه فناوری اطلاعات و ارتباطات در صنایع نفت، گاز، پالایش و پتروشیمی ، تهران، دانشگاه شهید بهشتی	دی ۱۳۹۳	لینک
قلاب سازی در تحلیل و طراحی بدافزار	*Hooking in malware design and analysis*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	آذر ۱۳۹۳	لینک
حفظ حریم خصوصی در خدمات مکان-مبنا	*Privacy Preserving in Location-Based Services*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	آذر ۱۳۹۳	لینک
روش‌های تحلیل بدافزار	*malware analysis methods*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	آذر ۱۳۹۳	
روش‌های تشخیص بدافزار (با محوریت تشخیص رفتاری پویا)	*malware detection methods*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	شهریور ۱۳۹۳	
بیت کوین و مسائل امنیتی آن	*Bitcoin Security Challenges*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	مرداد ۱۳۹۳	لینک
رویکرد معنایی در سیستم‌های تشخیص نفوذ مبتنی بر میزبان با استفاده از الگوهای فراخوان سیستمی پیوسته و ناپیوسته	*A Semantic Approach to Host-Base Intrusion Detection systems using Contiguous and discontinuous system call patterns*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	تیر ۱۳۹۳	لینک
بهره‌برداری از آسیب‌پذیری پایگاه داده MySQL	*MySQL Vulnerabilities Exploitation*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	تیر ۱۳۹۳	لینک
هک پایگاه داده و راهکارهای ای، با محوریت بدافزارهای مقابله سرور SQL اوراکل و	*Databases hacking, safeguards and countermeasures ,Case*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	خرداد ۱۳۹۳	لینک

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

	study : Oracle & SQL server malwares				
تحلیل تفاضلی و خطی الگوریتم و تست بهمنی آن LOKI97	*linear and differential analysis of LOKI97 beside Strict Avalanche Criteria*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر		
معرفی رمزکار ویروس شناسی ،تهدیدات امنیتی، راهکاری‌های حفاظت و مقابله با آن‌ها	*Cryptovirology Introduction, Security Threats, Safeguards and Countermeasures)*	آزمایشگاه طراحی و تحلیل سیستم‌های امن	دانشگاه صنعتی امیرکبیر	دی ۱۳۹۲	لینک
***OAارائه الگوریتم جدید به‌منظور کاهش پیچیدگی مکانی و *Aزمانی جست‌وجوی آگاهانه**	*Propose OA* new algorithm for decreasing space complexity and time complexity in A-Star Informed search*	---	کنفرانس بین‌المللی مدل‌های غیرخطی و بهینه‌سازی ،آمل ،دانشگاه شمال	شهریور ۱۳۹۱	

اسناد فنی و تحلیلی منتشرشده:

(فاقد طبقه‌بندی)

نام سند	زیرموضوعات	تاریخ انتشار	لینک دسترسی
ویژه‌نامه گزارش بررسی «حادثه قطع برق سراسری ونزوئلا»	• *مروری به وضعیت صنعت برق در ونزوئلا* • *حواشی سیاسی و اخبار حاصله از آن* • *جزئیات ماجرای قطع برق ونزوئلا* • *تکرار قطع برق در ونزوئلا* • *مقایسه حادثه قطع برق ونزوئلا با قطع برق سراسری آمریکای شمالی* • *تبعات و خسارات گزارش‌شده* • *آیا واقعاً حمله سایبری دلیل قطع برق ونزوئلا بوده است؟* • *درس‌هایی از این حادثه*	*۱۲ اردیبهشت ۹۸*	لینک
ویژه‌نامه گزارش حمله بدافزار GreyEnergy به سامانه های کنترل صنعتی (کد سند: ICS-SR-MMA-970801)	• *حمله بدافزار GreyEnergy به زیرساخت‌های حیاتی صنعتی* • *معرفی دوره آموزشی (۴۰ ساعته): «الزامات امنیت در سامانه‌های کنترل صنعتی و اسکادا»*	*۱ آبان ماه ۱۳۹۷*	لینک
گزارش آسیب پذیری و حملات بدافزاری VPN فیلتر به تجهیزات صنایع و زیرساخت های حیاتی (کد سند: ICS-SR-MMA-970502)	• *حمله بدافزار VPNFilter به سایت صنعتی تولید کلر در اوکراین* • *ارائه «حملات کنترل صنعتی، از حرف تا عمل»* • *بررسی اجمالی آسیب‌پذیری مسیریاب‌های میکروتیک*	*۳ شهریور ماه ۱۳۹۷*	لینک

صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

بررسی اجمالی افشاء اطلاعات پروژه دیسپچینگ ملی گاز از طریق مستند تلویزیونی	---	*۲۲ تیرماه ۱۳۹۷*	*لینک* *(حذف سند به دلیل درخواست شرکت پیمانکار)*
ویژه‌نامه گزارش بررسی اجمالی آسیب‌پذیری سوئیچ‌های صنعتی زیمنس (CVE-2018-4833)	• *بررسی اجمالی آسیب‌پذیری سوئیچ‌های صنعتی زیمنس* • *سوء برداشتی در بین برخی مدیران صنایع و زیرساخت‌های حیاتی* • *معیارهای گزینش دوره‌های پیشرفته امنیت کنترل و اتوماسیون صنعتی در کشور* • *معرفی مجموعه فیلم حوادث و حملات سایبر-فیزیکی به سامانه‌های صنعتی*	*۱۸ تیرماه ۱۳۹۷*	*لینک*
بررسی اجمالی مستند «آفتاب نهان» از زاویه نشت اطلاعات سایبر-فیزیکی صنایع و زیرساخت‌های حیاتی کشور	---	*اردیبهشت ۱۳۹۷*	*لینک*
گزارش بررسی آسیب‌پذیری‌های تجهیزات شبکه و توجه به اهمیت آن	• *به مناسبت خروج آمریکا از برجام (عدم اهمیت شناسایی استاکس‌نت* • *گزارش بررسی اجمالی آسیب‌پذیری‌های تجهیزات موکسا* • *گزارش اجمالی آسیب‌پذیری کارت‌های شبکه زیمنس* • *گزارشی اجمالی از حمله به تجهیزات سیسکو*	*۲۸ اردیبهشت ۱۳۹۷*	*لینک*
گزارش آسیب‌پذیری حیاتی در PLC WAGO CoDeSys	---	*۶/اردیبهشت ۱۳۹۷*	*لینک*
بررسی اجمالی تجهیزات Lantronix کنترل صنعتی متصل به اینترنت	---	*۳۱ فروردین ۱۳۹۷*	*لینک*

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mAhmadian.ir

جوایز و افتخارات:

عنوان	سال
کسب عنوان دانشجوی ممتاز(رتبه اول) در دوره کارشناسی ارشد دانشگاه صنعتی امیرکبیر با معدل ۱۸,۱۶	۱۳۹۴
کسب سهمیه دکتری بدون آزمون دانشگاه صنعتی امیرکبیر در گرایش امنیت اطلاعات (استعدادهای درخشان)	۱۳۹۴

کسب عنوان دانشجوی ممتاز(رتبه اول) در دوره کارشناسی ناپیوسته دانشگاه شمال با معدل ۱۹,۵۶	۱۳۹۱
کسب عنوان دانشجوی ممتاز(رتبه اول) در دوره کاردانی دانشگاه امام علی یزد با معدل ۱۹,۰۸	۱۳۸۸
کسب سهمیه شرکت در مسابقات بین‌المللی ربات‌های شبیه‌ساز سه‌بعدی فوتبالیست (Soccer 3D Simulation) در سال ۲۰۰۹(Iran Open 2009) در قالب تیم Angel و کسب گواهی بین‌المللی شرکت در این مسابقات و سمپوزیوم آن.	۱۳۸۷
کسب رتبه اول مسابقات تست نفوذ در مسابقه دوره آموزشی تست نفوذ در آپای دانشگاه صنعتی امیرکبیر (تیم دونفره، به همراه مهندس سجاد حسین زاده)	۱۳۹۲

زبان انگلیسی :

MCHE Certified

Reading ★★★★★★★★★★

Listening ★★★★★★★★★☆

Speaking ★★★★★★★★☆☆

Writing ★★★★★★★☆☆☆

مقالات سایر حوزه‌ها:

- **«ملّا شدن چه آسان است، آدم شدن چه مشکل». احمدیان، محمد مهدی،نشریه پویش، شماره۳۰،شورای صنفی دانشکده کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر تهران، مهر ۱۳۹۵، ص ۸. (لینک)**
- **«درخت هر چه پربارتر، افتاده تر!». احمدیان، محمد مهدی،هفته نامه بابک زمین، شماره ۵۷۹، سه شنبه ۶ مهر ۱۳۹۵.(لینک)**
- **«اگر شکست نخورده اید، نخوانید! ». احمدیان، محمد مهدی،هفته نامه بابک زمین، شماره ---، ۱۳۹۱.(لینک)**

صفحات شخصی :

صفحات شخصی :

QR Code	لینک	حوزه	نام صفحه شخصی با شبکه اجتماعی
	mmAhmadian.ir	اطلاع‌رسانی	Website
	Ahmadian.blog.ir	اطلاع‌رسانی	Weblog

نسخه عمومی رزومه صرفاً جهت انتشار در وبگاه شخصی www.mmAhmadian.ir

Google Scholar	کتب، مقالات و سایر پژوهش‌های معتبر بین‌المللی	Link	
Researchgate profile	کتب، مقالات و سایر پژوهش‌ها	Link	
شناسه OrcID	شناسه پژوهشی	0000-0002-5833-3858	
Twitter Official Page	اطلاع‌رسانی	@mmAhmadian	
Instagram Official Page	اطلاع‌رسانی تصاویر	@mmAhmadian	
LinkedIn Page	شبکه حرفه‌ای	@mmAhmadian	
Aparat Page	فیلم‌های آموزشی	@mmAhmadian	
Telegram Channel	اطلاع رسانی جامع	@MohammadMehdiAhmadian	
Sorush Channel	اطلاع رسانی محدود	@mmAhmadian	

گواهی‌ها: گزیده‌ای از مدارک و گواهی‌ها در سند پیوست رزومه درج شده‌است.

نسخه عمومی رزومه
صرفاً جهت انتشار در وبگاه شخصی
www.mmAhmadian.ir