«پژوهشگر گرامی»

صفحاتی راکه مشاهده می فرمائید، گزیده ای محدود از یک سند پژوهشی طولانی است که شامل :

- صفحه روی جلد
- چکیده فارسی و انگلیسی
- صفحه اول مقدمه
- منابع
- فهرست مطالب
- پیشنهادات

برای مشاهده فرمت دیجیتالی پایان نامه ها / رساله ها می توانید به آدرس ذیل مراجعه کنید:

http://lib.uok.ac.ir:8080

در صورت به وجود آمدن هرگونه مشکل و پرسش در زمینه دسترسی، تهیه و استفاده از منابع الکترونیکی و دیجیتال به بخش پایان نامه ها و منابع دیجیتال کتابخانه مرکزی و مرکز اسناد مراجعه نموده و تماس بگیرید!

شماره تماس ۰۸۷-۳۳۶۲۴۰۰۶

دانشگاه کردستان
دانشکده مهندسی
گروه مهندسی برق (الکترونیک و مخابرات)

پایان نامه کارشناسی ارشد رشته مهندسی برق گرایش مخابرات-سیستم

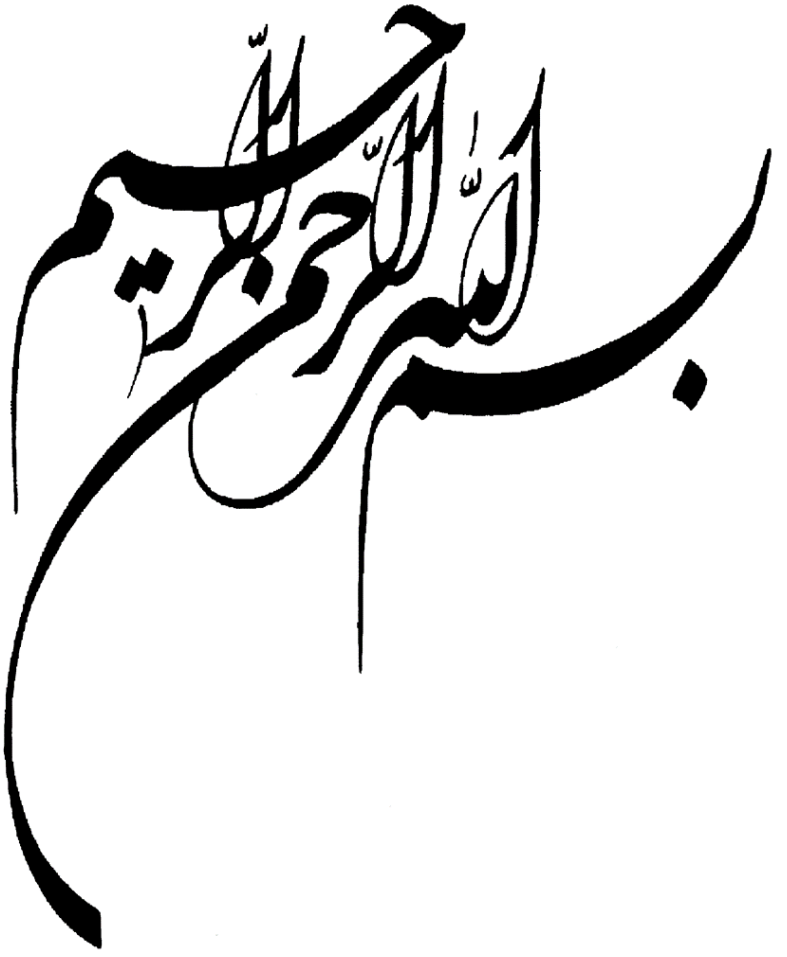
عنوان:

ارزیابی پروتکل‌های احراز هویت قابل اطمینان در اینترنت اشیاء صنعتی

پژوهشگر:
سجاد علی محمدی

اساتید راهنما:
دکتر محمد فتحی
دکتر سیروس فتحی منش

شهریور ۱۴۰۱



دانشگاه کردستان

دانشکده مهندسی

گروه مهندسی برق (الکترونیک و مخابرات)

پایان‌نامه کارشناسی ارشد رشته مهندسی برق گرایش مخابرات-سیستم

عنوان:

ارزیابی پروتکل‌های احراز هویت قابل اطمینان در اینترنت اشیاء صنعتی

پژوهشگر:

سجاد علی محمدی

اساتید راهنما:

دکتر محمد فتحی

دکتر سیروس فتحی منش

شهریور ۱۴۰۱

باسمه تعالی

* تعهد نامه دانشجویان تحصیلات تکمیلی دانشگاه کردستان در انجام پایان نامه *

اینجانب سجاد علی محمدی دانشجوی مقطع کارشناسی ارشد رشته مهندسی برق گرایش مخابرات–سیستم متعهد میشوم:

۱- صداقت، امانتداری و بی طرفی را در انجام پژوهش و انتشار نتایج حاصل از آن رعایت نمایم.

۲- در نگارش نتیجه پژوهش های حاصل از موضوع پایان نامه، از باز نویسی نوشته های دیگران بدون ذکر منبع، بازی با الفاظ، زیاده نویسی، کلی گویی و جزم اندیشی و تصرف گرایی پرهیز نمایم و نتایج پژوهشی خود را در موعد مقرر و با اطلاع استاد راهنما منتشر نمایم.

۳-تمامی یافته های مستخرج از پایان نامه متعلق به دانشگاه کردستان بوده و لازم است در کلیه مقالات مستخرج از آنها نام دانشگاه کردستان را تحت عنوان ((دانشجوی دانشگاه کردستان)) یا ((دانش آموخته دانشگاه کردستان)) ذکر نمایم.

۴- در انتشار مقالات نام استاد (استادان) راهنما و استاد (استادان) مشاور را در لیست مولفین مقاله ذکر نمایم و از آوردن اسامی افرادی که نقش موثری در انجام پژوهش نداشته اند، جداً خودداری نمایم.

۵- در بخش سپاسگزاری مقاله، از تمامی افراد و سازمان هایی که در اجرای پژوهش مساعدتی مبذول داشته اند با ذکر نوع مشارکت تشکر و قدر دانی نمایم.

۶- از انتشار همپوشان یا ارسال همزمان یک مقاله به چند مجله و یا ارسال مجدد مقاله چاپ شده به مجلات دیگر خودداری نمایم.

۷- در صورت عدم رعایت موارد مذکور، دانشگاه کردستان مجاز خواهد بود تا برابر مقررات اقدام نماید.

امضاء دانشجو

دستور العمل نحوه برخورد با موارد تخطی دانشجویان تحصیلات تکمیلی در هنگام انتشار نتایج پژوهش

۱- درموارد زیر دانشگاه کردستان با مجله مربوطه مکاتبه و درخواست خارج نمودن مقاله را نموده و موضوع را به محل کار یا تحصیل بعدی دانشجو اطلاع خواهد داد.

الف: چاپ مقاله بدون اطلاع و تأیید استادان راهنما

ب: چاپ نتایج حاصل از پژوهش های انجام شده در دانشگاه کردستان بدون ذکر نام دانشگاه

۲- در صورت احراز تخلف از سایر موارد درج شده در تعهد نامه دانشجویی، دانشگاه ضمن مکاتبه با مجله مربوطه، حسب مورد تصمیم گیری خواهد نمود.

دانشگاه کردستان

دانشکده مهندسی

گروه مهندسی برق (الکترونیک و مخابرات)

پایان نامه کارشناسی ارشد رشته مهندسی برق گرایش مخابرات-سیستم

عنوان:

ارزیابی پروتکل‌های احراز هویت قابل اطمینان در اینترنت اشیاء صنعتی

پژوهشگر:

سجاد علی محمدی

در تاریخ ۱۴۰۱/۰۶/۰۲ توسط کمیته تخصصی وهیات داوران زیر مورد بررسی قرار گرفت و با درجه خیلی خوب به تصویب رسید.

هیات داوران	نام و نام خانوادگی	مرتبه علمی	امضاء
۱ـ استاد راهنما	دکتر محمد فتحی	دانشیار	
۲ـ استاد راهنما	دکتر سیروس فتحی منش	استادیار	
۳ـ استاد داور خارجی	دکتر سید مسعود میررضایی	استادیار	
۴ـ استاد داور داخلی	دکتر فریدون حسین پناهی	استادیار	

Signer ID: DOZ28PH578...

مهر و امضاء مدیر گروه

دانشگاه کردستان
دانشکده مهندسی
گروه مهندسی برق الکترونیک و مخابرات

معاون آموزشی و تحصیلات تکمیلی دانشکده

دانشگاه کردستان

چکیده

امنیت و احراز هویت یک هدف اصلی در طراحی سیستم‌های محاسبات فعلی، از جمله سیستم‌های تعبیه شده، سیستم‌های سایبر فیزیکی و دستگاه‌های اینترنت اشیای صنعتی می‌باشد. با توجه به پیشرفت‌های روزافزون مبتنی بر حملات مخرب و کاهش امنیت تکنیک‌های تحمل پذیر خطا در اینترنت اشیاء، بکارگیری و ارائه روش‌هایی که بتوانند احراز هویت را در برابر حملات وارد بر شبکه نظیر حملات سایبری تضمین کرده و یا خطا را به حداقل برسانند، لازم و ضروری است. در این پژوهش به منظور افزایش دقت سیستم تشخیص نفوذ اینترنت اشیای صنعتی در برابر حملات سایبری، از روش ترکیبی مبتنی بر الگوریتم های فراابتکاری گرگ خاکستری (GWO) و شبیه سازی تبرید (SA) و الگوریتم های طبقه بندی DT، ANN و KNN استفاده شد. ابتدا داده های مربوط به حملات سایبری پس از مراحل پیش پردازش، نرمال سازی شد. در مرحله بعد با استفاده از الگوریتم های DT، ANN و KNN و ترکیب آن ها با الگوریتم های شبیه سازی تبرید و گرگ خاکستری، داده ها مورد آزمون و ارزیابی قرار گرفت.

از مجموعه داده KDD Cup 99 برای ارزیابی مدل‌های پیشنهادی استفاده شده است.

بر مبنای نتایج بدست آمده مشخص گردید که استفاده از الگوریتم ترکیبی GWO-ANN با دقت ۹۳/۲۲۷۳ درصد از نظر دقت در انتخاب ویژگی و همچنین میزان تشخیص حملات عملکرد بهتری دارد. همچنین می‌توان این مورد راه هم استنتاج کرد که الگوریتم ANN نسبت به الگوریتم‌های DT و KNN در تلفیق با الگوریتم‌های GWO و شبیه سازی تبرید دارای دقت بالاتری است. پس از الگوریتم ANN، الگوریتم درخت تصمیم (DT) در مرتبه دوم قرار می‌گیرد، و الگوریتمی که در تلفیق با دو الگوریتم GWO و SA دارای خطای محاسباتی بیشتری می‌باشد، الگوریتم KNN است.

همچنین نتایج مقایسه‌ای ما با مقاله‌ای که از الگوریتم CFA استفاده کرده بیانگر آن است که روش پیشنهادی در مقایسه با روش CFA حدود ۱/۱۷۶۳ درصد بهبود را نشان می‌دهد.

کلمات کلیدی: اینترنت اشیای صنعتی – احراز هویت – امنیت – حملات سایبری – الگوریتم گرگ خاکستری – شبکه عصبی – درخت تصمیم - KNN

فهرست مطالب

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فصل اول:
مقدمه و کلیات

۱-۱- مقدمه

در بحث شبکه هایی که بر پایه اینترنت اشیا[1] (IOT) بنا نهاده شده اند و در آنها جهت سهولت در مدیریت ارتباط بین اشیاء با محیط بیرون صورت میگیرد، حفظ امنیت و مراقبت از حریم خصوصی از اهمیت زیادی برخوردار است. قطعا مدیران و طراحان این شبکه ها دوست ندارند شبکه آنها توسط سایر افراد و سازمانهای غیر مجاز مورد پایش قرار گرفته و کنترل شبکه را در دست بگیرند. زیرا اگر چنین شرایطی ایجا گردد آنها خواهند توانست به اطلاعات کابران دسترسی پیدا نموده و باعث ایجاد اختلال و یا از کار افتادن شبکه و دستگاههای آن شوند. در شبکه اینترنت اشیاء با توجه به محدودیت هایی از قبیل تامین انرژی، اغلب از دستگاه‌هایی استفاده می شود که دارای قدرت پردازشی کم، جهت مدیریت منابع تامین انرژی هستند. بنابراین یک شرایط مناسب جهت اجرای حملاتی از قبیل کانال جانبی را در اختیار افراد غیر مجاز قرار می‌دهد. از این رو برقراری یک محیط امن به منظور جلوگیری از فاش شدن اطلاعات، امری ضروری است که در این پژوهش به دنبال استفاده از الگوریتم‌های مبتنی بر هوش مصنوعی به منظور افزایش امنیت و احراز هویت در اینترنت اشیاء صنعتی[2] (IIOT) هستیم. در این فصل به بررسی کلیات پژوهش پرداخته می‌شود.

---

[1]. Internet Of Things
[2]. Industrial Internet Of Things

۱-۲- بیان مسئله

اینترنت اشیاء (IOT) به عنوان یک پلتفرم ذخیره و انتقال داده، که به کاربران اجازه دسترسی به منابع محاسباتی از راه دور را می‌دهد ظهور کرده است. با توجه به کاربرد اینترنت اشیاء در حوزه‌های مختلفی همچون صنعت [۱]، آموزش[۲]، سلامت[۳]، کشاورزی[۴, ۵] و [۵] ، تجارت[۶, ۷] و غیره، داده‌های بسیار زیاد، حجیم و مهمی از این کاربردها تولید می گردد که بایستی در یک شبکه بی‌سیم منتقل شوند. وجود این داده‌های حجیم، منجر به بروز چالش‌هایی مانند پردازش حجم بالایی از داده و ذخیره‌سازی آن، برقراری امنیت در پردازش، احراز هویت و انتقال شده است. از طرفی، ارتباطات پیچیده شبکه و وجود میزان اطلاعات حجیم در این شبکه ها، مدیریت داده‌ها را بسیار دشوار کرده است. از آنجا که مورد حمله قرار گرفتن شبکه ارتباطی اجتناب ناپذیر است، در نتیجه شناسایی سریع در کمترین زمان ممکن، احراز هویت و بازیابی اطلاعات در شبکه از قابل اطمینان‌ترین مواردی هستند که برای یک عملیات با سرعت بالا ضروری می‌باشند[۸].

با توسعه فناوری‌های مختلف و ظهور مفاهیم نوآورانه مانند کلان داده، محاسبات ابری، سیستم فیزیکی سایبری(CPS)[1] و غیره، صنعت مدرن به سطح جدیدی ارتقا یافته است. در نتیجه، سیستم‌های صنعتی هوشمند، با اینترنت اشیاء صنعتی به عنوان هسته، با هدف تحقق تولید هوشمند، پدید آمده اند.

از طریق اینترنت اشیاء صنعتی (IIoT)، انواع مختلف تجهیزات صنعتی در یک مکان صنعتی هوشمند تعامل خوشه‌ای را با سایر دستگاه‌ها برقرار می کنند، و در این مکان که تعامل خوشه‌ای برقرار گردیده داده‌های دستگاه‌ها دیگر مستقل نیستند. از طریق برخورد و تلفیق داده‌ها، می‌توان دگرگونی و به روزرسانی فرآیند تولید هوشمند و شبکه‌ای را ارتقاء داد. در حقیقت، روندها و ابتکارات فعلی صنعت با هدف استفاده از اینترنت برای اتصال اشیای غیرمرتبط در صنعت و تحقق چهارمین انقلاب صنعتی است[۹].

در دهه‌های گذشته، مهندسی تولید کلاسیک، اتوماسیون و سیستم‌های محاسباتی هوشمند در اینترنت اشیا صنعتی (IIoT) ادغام شدند. تعداد اجزای محاسباتی ادغام شده در سیستم‌های کنترل صنعتی، سیستم‌های تولید و کارخانه‌ها به طور پیوسته در حال افزایش است. کنترل‌کننده‌های منطقی قابل برنامه‌ریزی با سیستم‌های فیزیکی سایبری پیشرفته‌تر (CPS) جایگزین شده‌اند که سبب شده تا دستگاه‌های تعبیه‌شده بصورت آزادانه قابل برنامه‌ریزی باشند که فرآیندهای فیزیکی را کنترل کنند.

[1]. Cyber Physical System

در زمینه سیستم‌های کنترل صنعتی، مفهوم امنیت به طور سنتی تقریباً همان معنای ایمنی را دارد، یعنی حفاظت از انسان، محیط زیست و ماشین‌ها در برابر پیامدهای خرابی سیستم[۱۰].

با وجود شرایط توسعه و پیشرفت‌های عرصه سایبری، برقراری امنیت کافی برای زیرساخت‌های اینترنت اشیاء که در صنعت مورد استفاده قرار می‌گیرند، روز به روز بر اهمیت شان افزوده می‌شود. برنامه هایی که در زمینه صنعت بر پایه اینترنت اشیاء استفاده می‌شوند در برابر هرگونه حمله، اختلال و سرقت اطلاعات، آسیب‌پذیر می‌باشند. اینترنت اشیاء نقش مهمی در اتصال تقریبا همه وسایل (دستگاه‌های موبایل، دوربین‌ها، لوازم خانگی، دستگاه‌های بهداشتی، تجهیزات نظامی (از جمله بی سیم‌های نظامی و غیره)) به اینترنت، از طریق فن آوری‌های مختلف ارتباطی مانند Wi-Fi خواهد داشت. برخی از این اطلاعات که از طریق اینترنت اشیاء به هم مرتبط هستند. این وسایل ممکن است بسیار حساس باشند و حریم خصوصی و امنیت آنها نباید به خطر افتاده باشد. یکی از چالش‌های مهم جامعه بشری با توجه به پیشرفت‌های تکنولوژی امروز, حفظ حریم خصوصی و احراز هویت در تبادل اطلاعات می‌باشد که سرقت رفتن آن‌ها می تواند آسیب‌های جبران ناپذیری را به بار آورد[۱۱].

از این رو در این پژوهش تلاش می‌گردد که به مساله امنیت و احراز هویت در اینترنت اشیای صنعتی که از اهمیت بالایی بدلیل ماهیت صنعتی بودن آن برخوردار است، پرداخته شود و با استفاده از تکنیک‌های هوش مصنوعی و یادگیری ماشین در این حوزه، به این مساله پرداخته شود.

۱-۳- اهمیت و ضرورت پژوهش

امنیت و احراز هویت یک هدف اصلی در طراحی سیستم‌های محاسبات فعلی، از جمله سیستم‌های تعبیه شده، سیستم‌های سایبر فیزیکی و دستگاه‌های IIoT است. در طول سال‌ها، تکنیک‌های مختلف طراحی، تجزیه- تحلیل، احراز هویت و تست امنیت سیستم ارائه شده است. احراز هویت تضمین می‌کند که یک سیستم در حضور خطا هم بدون وقفه کار می‌کند. اینترنت اشیاء (IoT) به سرعت در حال رشد و یک فناوری در سطح جهانی است. اینترنت اشیاء امکان اتصال دستگاه‌های هوشمند، حسگرها، دستگاه‌های محاسبه و غیره را از طریق فن‌آوریهای مدرن شبکه فراهم می‌کند. در اینترنت اشیاء به منظور افزایش امنیت و قابلیت اطمینان، احراز هویت مطمئن داده‌ها مورد توجه قرار گرفته است. بر این اساس ایجاد مکانیزم احراز هویت قابل اطمینان و به موقع در اینترنت اشیاء از الزامات امنیتی این فناوری محسوب می‌شود، که با توجه به اهمیت زمان در صنعت بایستی در کمترین زمان ممکن صورت بپذیرد. از این رو، با توجه به پیشرفت‌های روزافزون مبتنی

الگوریتم گرگ خاکستری در انتخاب ویژگی بسیار موفق می‌باشد، که با مقایسه آن با الگوریتم شبیه سازی تبرید در راستای انتخاب ویژگی، ثابت شد که با انتخاب تعداد ویژگی‌های بهینه می‌تواند نرخ تشخیص حملات را بهبود بخشد.

۵-٤- پیشنهادات

جهت ادامه این پژوهش پیشنهاد می‌گردد موارد زیر انجام گیرند:

استفاده از ترکیب الگوریتم ANN و الگوریتم کلونی مورچگان و مقایسه نتایج با نتایج بدست آمده از این پژوهش.

بررسی دقت عملکرد سیستمهای تشخیص نفوذ توسط عاملهای متحرک با الگوریتم PSO&ANN

منابع

[1]. Deshpande, A., P. Pitale, and S. Sanap, Industrial automation using Internet of Things (IOT). International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2016. 5(2): p. 266-269.

[2]. AjazMoharkan, Z., et al. Internet of Things and its applications in E-learning. in 2017 3rd international conference on computational intelligence & communication technology (CICT). 2017. IEEE.

[3]. Scarpato, N., et al., E-health-IoT universe: A review. management, 2017. 21(44): p. 46.

[4]. Gondchawar, N. and R. Kawitkar, IoT based smart agriculture. International Journal of advanced research in Computer and Communication Engineering, 2016. 5(6): p. 838-842.

[5]. Shenoy, J. and Y. Pingle. IOT in agriculture. in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). 2016. IEEE.

[6]. Singh, S. and N. Singh. Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. in 2015 International conference on green computing and internet of things (ICGCIoT). 2015. Ieee.

[7]. Sohaib, O., H. Lu, and W. Hussain. Internet of Things (IoT) in E-commerce: For people with disabilities. in 2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA). 2017. IEEE.

[8]. Fei, X. and G. Tian, Optimization of communication network fault identification based on NB-IoT. Microprocessors and Microsystems, 2021. 80: p. 103531.

[9]. Wan, J., et al., A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Transactions on Industrial Informatics, 2019. 15(6): p. 3652-3660.

[10]. Sadeghi, A.-R., C. Wachsmann, and M. Waidner. Security and privacy challenges in industrial internet of things. in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). 2015. IEEE.

[11]. Sengupta, J., S. Ruj, and S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 2020. 149: p. 102481.

[12]. Eesa, A.S., Z. Orman, and A.M.A. Brifcani, A novel feature-selection approach based on the cuttlefish optimization algorithm for intrusion detection systems. Expert systems with applications, 2015. 42(5): p. 2670-2679.

[13]. Zhou, J., et al., Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine, 2017. 55(1): p. 26-33.

[14]. Zolanvari, M., et al., Machine learning-based network vulnerability analysis of industrial Internet of Things. IEEE Internet of Things Journal, 2019. 6(4): p. 6822-6834.

[15]. Zhu, B., A. Joseph, and S. Sastry. A taxonomy of cyber attacks on SCADA systems. in 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. 2011. IEEE.

[16]. Karthikeyan, S., R. Patan, and B. Balamurugan, Enhancement of security in the Internet of Things (IoT) by using X. 509 authentication mechanism, in Recent Trends in Communication, Computing, and Electronics. 2019, Springer. p. 217-225.

[۱۷]. سبحان, ا., بررسی حفره های اهنیتی هوجود در فناوری های ارتباطی هورد استفاده در اینترنت اشیاء in ,سومین کنفرانس بین المللی پژوهشهای کاربردی در مهندسی کامپیوتر و فن آوری اطلاعات. ۱۳۹۴.

[18]. Sicari, S., et al., Security, privacy and trust in Internet of Things: The road ahead. Computer networks, 2015. 76: p. 146-164.

[19]. Bugeja, J., A. Jacobsson, and P. Davidsson. On privacy and security challenges in smart connected homes. in 2016 European Intelligence and Security Informatics Conference (EISIC). 2016. IEEE.

[20]. Nour, B., et al., Security and privacy challenges in information-centric wireless internet of things networks. IEEE Security & Privacy, 2019. 18(2): p. 35-45.

[21]. Hossain, M.M., M. Fotouhi, and R. Hasan. Towards an analysis of security issues, challenges, and open problems in the internet of things. in 2015 ieee world congress on services. 2015. IEEE.

[22]. Falco, G., C. Caldera, and H. Shrobe, IIoT cybersecurity risk modeling for SCADA systems. IEEE Internet of Things Journal, 2018. 5(6): p. 4486-4495.

[23]. Osanaiye, O., K.-K.R. Choo, and M. Dlodlo, Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications, 2016. 67: p. 147-165.

[24]. Spcht, S.M. and R.B. Lee. Taxonomies of Attacks Tools and Countermeasures. in Proc. PDCS. 2004.

[25]. Zargar, S.T., J. Joshi, and D. Tipper, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE communications surveys & tutorials, 2013. 15(4): p. 2046-2069.

[26]. Mirjalili, S., S.M. Mirjalili, and A. Lewis, Grey wolf optimizer. Advances in engineering software, 2014. 69: p. 46-61.

[27]. Muro, C., et al., Wolf-pack (Canis lupus) hunting strategies emerge from simple rules in computational simulations. Behavioural processes, 2011. 88(3): p. 192-197.

[۲۸]. رضا, آ and .ب. علی, ارائه روشی برای احراز هویت در اینترنت اشیاء مبتنی بر موقعیت گیرنده های Wi-Fi و فناوری زنجیره بلوکی in ,پنجمین کنفرانس ملی محاسبات توزیعی و پردازش داده های بزرگ. ۱۳۹۸.

[۲۹]. سید علیرضا سید, ت and .پ. رضا, رمزگذاری در احراز هویت سیستم های اینترنت اشیا , inچهارمین کنفرانس ملی ایده های نوین در فنی و مهندسی. ۱۳۹۸.

[۳۰]. عیسی لو, ح and .ع. سلیمانی, ارائه روشی کم بار برای احراز هویت اشیاء در اینترنت اشیاء , inکنگره ملی تحقیقات بنیادین در مهندسی کامپیوتر و فن اوری اطلاعات. ۱۳۹۸.undefined , .

[۳۱]. حیدر محمد علی الحکیم, ش and .م. نیکوقدم, ارائه طرحی برای احراز هویت متقابل گمنام و توافق کلید بین دستگاه ها در اینترنت اشیا in ,پنجمین کنگره بین المللی مهندسی برق، کامپیوتر و مکانیک. ۱۳۹۹.undefined , .

[۳۲]. نیکویی, م and .ع. چاله چاله, بررسی و ارزیابی روش های احراز هویت برای دسترسی به وسایل خانگی هوشمند در بستر اینترنت اشیا in ,هفتمین کنگره ملی تازه یافته های مهندسی برق ایران. ۱۳۹۹.undefined , ,

[33]. Eigner, O., P. Kreimel, and P. Tavolato. Detection of man-in-the-middle attacks on industrial control networks. in 2016 International Conference on Software Security and Assurance (ICSSA). 2016. IEEE.

[34]. Bakhshi, Z., A. Balador, and J. Mustafa. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. in 2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW). 2018. IEEE.

[35]. Lin, C., et al., BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of network and computer applications, 2018. 116: p. 42-52.

[36]. Alves, T., R. Das, and T. Morris, Embedding encryption and machine learning intrusion prevention systems on programmable logic controllers. IEEE Embedded Systems Letters, 2018. 10(3): p. 99-102.

[37]. Tawalbeh, M., M. Quwaider, and A.T. Lo'ai. Authorization model for IoT healthcare systems: case study. in 2020 11th International Conference on Information and Communication Systems (ICICS). 2020. IEEE.

[38]. Putra, G.D., et al., Trust-based blockchain authorization for iot. IEEE Transactions on Network and Service Management, 2021. 18(2): p. 1646-1658.

[39]. Cup, K., Available on: http://kdd. ics. uci. edu/databases/kddcup99/kddcup99. html. 2007, Ocotber.

[40]. Harper, P.R., A review and comparison of classification algorithms for medical decision making. Health policy, 2005. 71(3): p. 315-331.

[41]. AlJarullah, A., Decision tree discovery for the diagnosis of type II diabetes. Int Con Inform Technol 2011; 3: 303-7. doi. 10.1109. INNOVATIONS, 2011. 8.

[42]. Farhangfar, A., L. Kurgan, and J. Dy, Impact of imputation of missing values on classification error for discrete data. Pattern Recognition, 2008. 41(12): p. 3692-3705.

[43]. Kamel, S.R., R. YaghoubZadeh, and M. Kheirabadi, Improving the performance of support-vector machine by selecting the best features by Gray Wolf algorithm to increase the accuracy of diagnosis of breast cancer. Journal of Big Data, 2019. 6(1): p. 1-15.

Abstract

Security and authentication is a major goal in the design of current computing systems, including embedded systems, cyber-physical systems, and industrial Internet of Things devices. Considering the ever-increasing developments based on malicious attacks and the reduction of security of error-tolerant techniques in the Internet of Things, applying and providing methods that can guarantee authentication against attacks on the network such as cyber attacks or minimize the error it is necessary and essential. In order to increase the accuracy of the industrial Internet of Things intrusion detection system against cyber attacks, a combined method based on meta-heuristic algorithms and DT, ANN and KNN classification algorithms was used. First, the data related to cyber attacks were normalized after pre-processing steps. In the next step, using DT, ANN and KNN algorithms and combining them with refrigeration simulation (SA) and gray wolf (GWO) algorithms, the data were tested and evaluated.

The KDD Cup 99 dataset has been used to evaluate the proposed models.

Based on the obtained results, it was found that the use of GWO-ANN integrated algorithm with 92/9545 percent accuracy has the best performance in terms of feature selection accuracy and attack detection. On the other hand, another issue that can be derived from these results is that the ANN algorithm is more accurate than the DT and KNN algorithms in combination with the GWO and SA algorithms. After the ANN algorithm, the DT algorithm is ranked second. It can also be seen that the use of ANN algorithm in combination with both GWO and SA algorithms has more calculation error.

Also, our comparative results with an article that used the CFA algorithm show that the proposed method shows an improvement of about 1.1763 percent compared to the CFA method.

Keywords: Industrial Internet of Things - Authentication - Security - Cyber Attacks - DDoS - Gray Wolf Algorithm - Neural Network - Decision Tree - KNN

University of Kurdistan
Faculty of Electronics and Telecommunications
Department of Electrical Engineering

A Thesis Submitted to the Postgraduate Studies Office in Partial Fulfillment of the Requirements for the Degree of MSC in Electrical Engineering

Title:
Designing reliable authentication system for Industrial Internet of Things (IIoT)

By:
Sajad Alimohamadi

The above thesis was evaluated and approved by the following members of the thesis committee with very good quality on August 24, 2022.

Position	Name and Title	Signature
Supervisor1:	Mohammad Fathi	Associate professor
Supervisor2:	Sirous Fathi Manesh	Assistant professor
External Examiner:	Seyyed Masoud Mirrrzaei	Assistant professor
Internal Examiner:	Fereydoun Hossein Panahi	Assistant professor

Head of Department

دانشگاه کردستان
دانشکده مهندسی
گروه مهندسی برق، الکترونیک و مخابرات

Faculty Graduate Coordinator

University of Kurdistan
Faculty of Electronics and Telecommunications
Department of Electrical Engineering

A Thesis

A Thesis Submitted to the Postgraduate Studies Office in Partial Fulfillment of the Requirements for the Degree of MSC in Electrical Engineering

Title:
Evaluation of reliable authentication protocols in the Industrial Internet of Things (IIoT)

By:
Sajad Alimohamadi

Supervisor:
Dr. Mohammad Fathi
Dr. Sirous Fathi Manesh

August , 2022

University of Kurdistan
Faculty of Electronics and Telecommunications
Department of Electrical Engineering

A Thesis

A Thesis Submitted to the Postgraduate Studies Office in Partial Fulfillment of the Requirements for the Degree of MSC in Electrical Engineering

Title:
Evaluation of reliable authentication protocols in the Industrial Internet of Things (IIoT)

By:
Sajad Alimohamadi

Supervisors:
Dr. Mohammad Fathi
Dr. Sirous Fathi Manesh

August , 2022