Security and privacy mechanisms of Internet of things in healthcare and non-healthcare industry

Somayeh Nasiri[1], Farahnaz Sadoughi [2*], Mohammad Hesam Tadayon[3], Afsaneh Dehnad[4]

Abstract

Introduction: Internet of things is a hot topic in the modern age of information and communication technology has become pervasive in various industries, particularly in healthcare sector. The security and privacy issue has attracted a lot of attention and has become a controversial issue in this area. The purpose of this study was to identify security mechanisms of Internet of things in health and non-healthcare industries.

Methods: The present study was a systematized review conducted by searching the Web of Science, Scopus, PubMed, IEEE Xplore, and ProQuest databases from 2005 to 2019. After the elimination of duplicate cases, studies related to the purpose of the study were selected on the basis of inclusion and exclusion criteria.

Results: We found 71 out of 2340 studies, related to security mechanisms of Internet of things in the healthcare (four studies) and non-healthcare (67 studies) industries, which were then reviewed. Security mechanisms have been organized into 11 major categories, including cryptography, key distribution and management mechanisms, digital identity management, and system life-cycle maintenance management, and secure routing in both the healthcare and non-healthcare industries. The findings showed that five types of security mechanisms, including energy saving, secure design and physical protection of system hardware, intrusion detection and prevention system, trust management, and fault detection and tolerance had not been addressed in the health industry.

Conclusion: Given the emergence of this technology in the healthcare industry and its security sensitivity to other industries, the findings of this study provide a broad insight for researchers, managers and information security professionals to encounter threats and attacks and develop a secure Internet of things architecture.

Keywords: Mechanism, Security, Privacy, Internet of Things, Healthcare, Non-Healthcare

● **Received:** 9/Nov/2019 ● **Modified:** 14/Dec/2019 ● **Accepted:** 18/Dec/2019

1. PhD candidate in Health Information Management, Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran; nasiri.him2015@gmail.com
2. Professor, Department of Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran; Corresponding author, Sadoughi.f@iums.ac.ir
3. Associate Professor, Iran Telecommunication Research Centre, Tehran, Iran; tadayon@itrc.ac.ir
4. Associate Professor, Department of English Language, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran; (dehnad.a@iums.ac.ir)

مکانیسم‌های امنیت و حریم خصوصی اینترنت اشیا در صنعت مراقبت سلامت و غیر سلامت

سمیه نصیری[۱]، فرحناز صدوقی[۲*]، محمد حسام تدین[۳]، افسانه دهناد[٤]

چکیده

مقدمه: اینترنت اشیا یکی از مباحث روز فناوری در عصر جدید اطلاعات و ارتباطات می‌باشد که با فراگیر شدن کاربرد آن در صنایع مختلف به ویژه مراقبت سلامت مسئله امنیت و حریم خصوصی آن توجه زیادی را به سمت خود جلب نموده است و به موضوعی بحث برانگیز در این حوزه تبدیل شده است. هدف از مطالعه حاضر، شناسایی مکانیسم‌های امنیت اینترنت اشیا در صنعت مراقبت سلامت و غیر سلامت می‌باشد.

روش‌ها: پژوهش حاضر یک مطالعه مروری نظام‌یافته است که با جستجو در پایگاه‌های داده وب آو ساینس، اسکوپوس، آی تریپل ای، پابمد و پروکوئست در بازه زمانی سال های ۲۰۰۵ تا ۲۰۱۹ انجام شد. پس از حذف موارد تکراری و ارزیابی یافته‌ها براساس معیار ورود و خروج، مطالعات مرتبط با هدف پژوهش انتخاب شد.

یافته‌ها: از مجموع ۲۳٤۰ مطالعه، ۷۱ مطالعه مرتبط با مکانیسم‌های امنیت اینترنت اشیا در صنعت مراقبت سلامت (چهار مطالعه) و غیر سلامت (٦۷ مطالعه) بررسی شد. مکانیسم‌های امنیت در ۱۱ طبقه اصلی سازماندهی شد که مکانیسم‌های رمزنگاری، توزیع و مدیریت کلید، مدیریت هویت دیجیتال، مدیریت نگهداشت چرخه حیات سیستم و مسیریابی امن در هر دو صنعت سلامت و غیر سلامت توجه شده‌اند. یافته‌ها نشان داد که به پنج نوع مکانیسم امنیتی در صنعت سلامت پرداخته نشده است، این مکانیسم‌ها در ارتباط با صرفه جویی انرژی، طراحی فیزیکی امن، سیستم تشخیص نفوذ و پیشگیری، مدیریت اعتماد و تشخیص و تحمل خطا بودند.

نتیجه‌گیری: با توجه به نوظهور بودن این فناوری در صنعت مراقبت سلامت و حساس بودن امنیت آن نسبت به سایر صنایع، یافته‌های این مطالعه بینش وسیعی را برای پژوهشگران، مدیران و متخصصان امنیت اطلاعات در جهت مقابله با تهدیدات و حملات و توسعه یک معماری امن اینترنت اشیا فراهم می‌کند.

واژه های کلیدی: مکانیسم، امنیت، حریم خصوصی، اینترنت اشیا، مراقبت سلامت، غیر سلامت

• وصول مقاله:۹۸/۰۸/۱۸ اصلاح نهایی:۹۸/۰۹/۲۳ پذیرش نهایی: ۹۸/۰۹/۲۷

۱. دانشجوی دکترای تخصصی مدیریت اطلاعات سلامت، دانشکده مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران؛ nasiri.him2015@gmail.com

۲. استاد گروه مدیریت اطلاعات سلامت، دانشکده مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران؛ نویسنده مسئول، sadoughi.f@iums.ac.ir

۳. دانشیار، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران؛ tadayon@itrc.ac.ir

٤. دانشیار دپارتمان زبان انگلیسی، دانشکده مدیریت و اطلاع رسانی، دانشگاه علوم پزشکی ایران، تهران، ایران؛ dehnad.a@iums.ac.ir

مقدمه

اینترنت اشیا (Internet of Things (IoT)) شبکه‌ای است که هر شیء را به اینترنت وصل می‌کند و از ادغام و ترکیب چندین فناوری ازجمله شناسایی خودکار امواج رادیویی (Radio Frequency Automatic Identification (RFID))، ارتباطات میدان نزدیک (Near Field Communication (NFC))، حسگر، سیستم موقعیت‌یاب جهانی (Global Positioning System (GPS)) و اسکنرهای لیزری تشکیل شده است که باعث برقراری تبادل اطلاعات و ارتباطات می‌شود و هدف اصلی آن شناسایی هوشمند، ردیابی محل، نظارت و مدیریت است. [۱،۲]

اتحادیه بین المللی ارتباط از راه دور (International Telecommunication Union (ITU)) بیان نموده است که IoT در هر زمان و مکانی، برای هر کس و با هر شیء ارتباط برقرار می‌کند. [۱] IoT در صنایع مختلف کاربرد دارد ازجمله می‌توان به بخش خانه‌ها و شهرهای هوشمند، انرژی و بهره‌وری، حمل و نقل، بخش تولید و تدارکات، دام و حیوانات، کشاورزی و صنعت بیمه اشاره نمود. [۵-۳]

این فناوری نیز در بخش مراقبت سلامت به‌ویژه سلامت الکترونیک (eHealth) به عنوان یکی از ضروری‌ترین و پرکاربردترین موضوعات در چند سال اخیر مطرح شده است. [۶] IoT می‌تواند در زمینه‌های مختلف پزشکی ازجمله دستگاه‌های مراقبت از راه دور و هشداردهنده موارد اورژانسی، برنامه‌های تناسب اندام، بیماری‌های مزمن و مراقبت از سالمندان مورد استفاده قرار گیرد و کارکردهای مهمی را در حوزه سلامت اعم از: مدیریت مؤثر در کل موسسه مراقبت بهداشتی و درمانی، هماهنگی و برقراری ارتباط بین پزشک و بیمار به ارمغان گذارد. [۷] به‌طوری‌که داده‌های حاصل از علائم حیاتی به‌صورت خودکار از طریق پوشیدن لباس‌های هوشمند در وضعیت‌های مختلف (مثل قدم زدن، خوردن، خوابیدن و ورزش کردن) ثبت و گردآوری می‌شود و در صورت هرگونه تغییر در ارتباط با سبک زندگی و وضعیت سلامت به افراد هشدار می‌دهد. [۸]

البته در کنار کاربردهای IoT در نظام مراقبت سلامت و به‌منظور محقق شدن وعده‌های آن یکسری چالش‌ها و موانع امنیتی مطرح است. [۵] برخی از این مشکلات و چالش‌های امنیتی ناشی از ویژگی‌ها و قابلیت‌های IoT (اعم از ناهمگونی، سیار بودن (تحرک)، مقیاس‌پذیری، آدرس‌دهی و شناسایی و محدودیت منابع) است. [۹] ازآنجاکه صنعت مراقبت سلامت با جان یک انسان سروکار دارد و نقش امنیت IoT در حوزه پزشکی نسبت به سایر صنایع اهمیت بیشتری پیدا می‌کند. [۷] این موضوع به ویژه در هنگام جمع‌آوری داده‌های بلادرنگ و تحلیل داده‌ها در برنامه‌های کاربردی محسوس‌تر است و مفاهیم امنیتی مورد توجه قرار می‌گیرد. [۱۰] زیرا تجهیزات و برنامه‌های کاربردی دربرگیرنده اطلاعات خصوصی و حیاتی بیمار مثل داده‌های مراقبت سلامت فردی هستند. [۷]

واژه امنیت در IoT گستره بزرگی از مفاهیم و الزامات امنیتی همچون محرمانگی، تصدیق یا احراز هویت، تمامیت، اعطای مجوز و قابلیت دسترسی را در برمی‌گیرد که این الزامات با استفاده از مکانیسم‌های مختلف امنیتی فراهم می‌شود. [۱۱، ۷] وضعیت امنیت IoT با توجه به ماهیت آن در نظام سلامت نسبت به سیستم‌های فعلی شرایط را به مراتب پیچیده و حساس‌تر می‌کند. زیرا با گسترش IoT در سلامت الکترونیک تهدیدات امنیتی در حال پیشرفت است و دستگاه‌های هوشمند دائم مورد حمله قرار می‌گیرند. [۱۲،۱۳] به‌گونه‌ای که ممکن است یک مهاجم با دستکاری فیزیکی در تجهیزات پزشکی و استخراج کدهای رمزنگاری برنامه را تغییر داده و/یا دستگاه‌ها را تخریب نماید. [۷] از طرف دیگر، براساس گزارش گارتنر (Gartner) بیش از ۵۰ درصد اتصالات اینترنت بین IoT است تا سال ۲۰۲۰ پیش‌بینی‌شده که ۲۶ بیلیون وسیله به اینترنت وصل خواهد شد. [۱۴] حال باتوجه به این حجم وسیع دستگاه‌های متصل‌به‌هم و انتقال و تبادل اطلاعات بین آن‌ها نگرانی‌هایی امنیتی و ناتوانی افراد در کنترل حریم خصوصی شکل می‌گیرد. [۱۵،۱۶]

درکنار استفاده گسترده از IoT در مراکز مختلف به‌منظور به حداقل رساندن چالش‌های امنیتی و نگرانی‌های به وجود آمده در زمینه حریم خصوصی افراد، نفوذ هکرها به شبکه‌های

بیمارستان و اختلال در تجهیزات پزشکی نیاز به تلاش و اقدامات قانونگذاران و سیاست گذاران و مداخله طراحان سیستم جهت شناسایی راهکارها و مکانیسم‌های مقابله‌ای در برابر تهدیدات و حملات دارد. [۱۴،۱۷] بنابراین، قبل از طراحی معماری امنیت در IoT لازم است تا چارچوبی ارائه شود که تمام زوایا و عوامل مرتبط با امنیت به همراه مکانیسم‌های آن شناسایی شود. لذا، شناسایی تمام عوامل مرتبط با امنیت در IoT می‌تواند از بروز تهدیدات و حملات پیشگیری نماید که باعث تأمین امنیت در رمزگذاری داده‌ها در دستگاه‌ها و مسیر انتقال شبکه، داده‌های جمع‌آوری‌شده توسط حسگرها، داده‌های ذخیره‌شده در پایگاه‌های داده و امنیت در خدمات‌رسانی شود. [۱۴،۱۸،۱۹]

بررسی پژوهشگر نشان داد مطالعه جامعی در زمینه مکانیسم‌های امنیت IoT انجام نشده است. بنابراین، پژوهش حاضر با هدف شناسایی مکانیسم‌های امنیت و حریم خصوصی IoT در صنعت مراقبت سلامت و غیر سلامت تدوین شده است.

روش‌ها

پژوهش حاضر از نوع مطالعه مرور نظام‌یافته است که در سال ۱۳۹۸ انجام شد. تمام مقالات (اصیل و مروری) چاپ شده در مجلات و ارائه‌شده در همایش‌ها و پایان‌نامه‌ها در بازه زمانی ۲۰۰۵ تا ۲۰۱۹ میلادی بررسی شد که با توجه به معیارهای ورود و خروج مطالعه در پنج پایگاه داده وب آو ساینس، اسکوپوس، پروکوئست، آی تریپل ای و پابمد نمایه شدند. معیارهای ورود و خروج مطالعات در جدول یک نشان داده شده است.

جدول ۱: معیارهای ورود و خروج مطالعات

معیارهای ورود	معیارهای خروج
• منابع مرتبط منتشر شده در مجلات، همایش‌ها و پایان‌نامه‌ها • بازه زمانی بین سال‌های ۲۰۰۵ تا ۲۰۱۹ • انگلیسی بودن زبان نشر منابع مورد بررسی • دسترسی به متن کامل منابع • مطالعاتی که مکانیسم‌های امنیت IoT را به صورت لایه‌ای بررسی کرده‌اند. • بررسی امنیت در صنعت مراقبت سلامت و غیر سلامت • انواع مطالعات اولیه (کمی و کیفی) و ثانویه (انواع مروری)	• نامه به سردبیر، پوستر، کتاب، گزارش‌ها و روزنامه • مطالعاتی که مکانیسم‌های امنیت را به صورت غیر لایه‌ای بررسی کردند.

ابزار گردآوری داده در این مرحله فرم استخراج داده بود که ابتدا با استفاده از کلیدواژه‌های مناسب و از طریق تنظیمات پیشرفته، رشته‌های جستجو در هر پایگاه داده ایجاد و سپس مطالعات مرتبط با هدف پژوهش استخراج شد. دامنه جستجو در مجموع محدود به عنوان، چکیده و واژه‌های کلیدی در پایگاه‌های داده بود. خلاصه‌ای از استراتژی جستجو به تفکیک پایگاه داده در جدول دو نمایش داده شده است. این کلیدواژه‌ها با استفاده از عملگرهای بولین AND و OR، عملگر کوتاه‌سازی (علامت ستاره *)، جستجوی عبارتی (علامت گیومه " ") و محدودیت‌ها انجام شد که برای انتخاب کلیدواژه‌های استاندارد از سرعنوان موضوعی پزشکی (Mesh) و کلیدواژه‌های منابع مرتبط استفاده شد. بعد از بازیابی منابع براساس استراتژی جستجو، ابتدا مطالعات تکراری با استفاده از نرم‌افزار EndNote حذف شد. سپس، با توجه به معیارهای ورود و خروج، عناوین و چکیده مطالعات بررسی شد و منابع غیرمرتبط حذف شد. پس از آن، متن کامل مطالعات بررسی

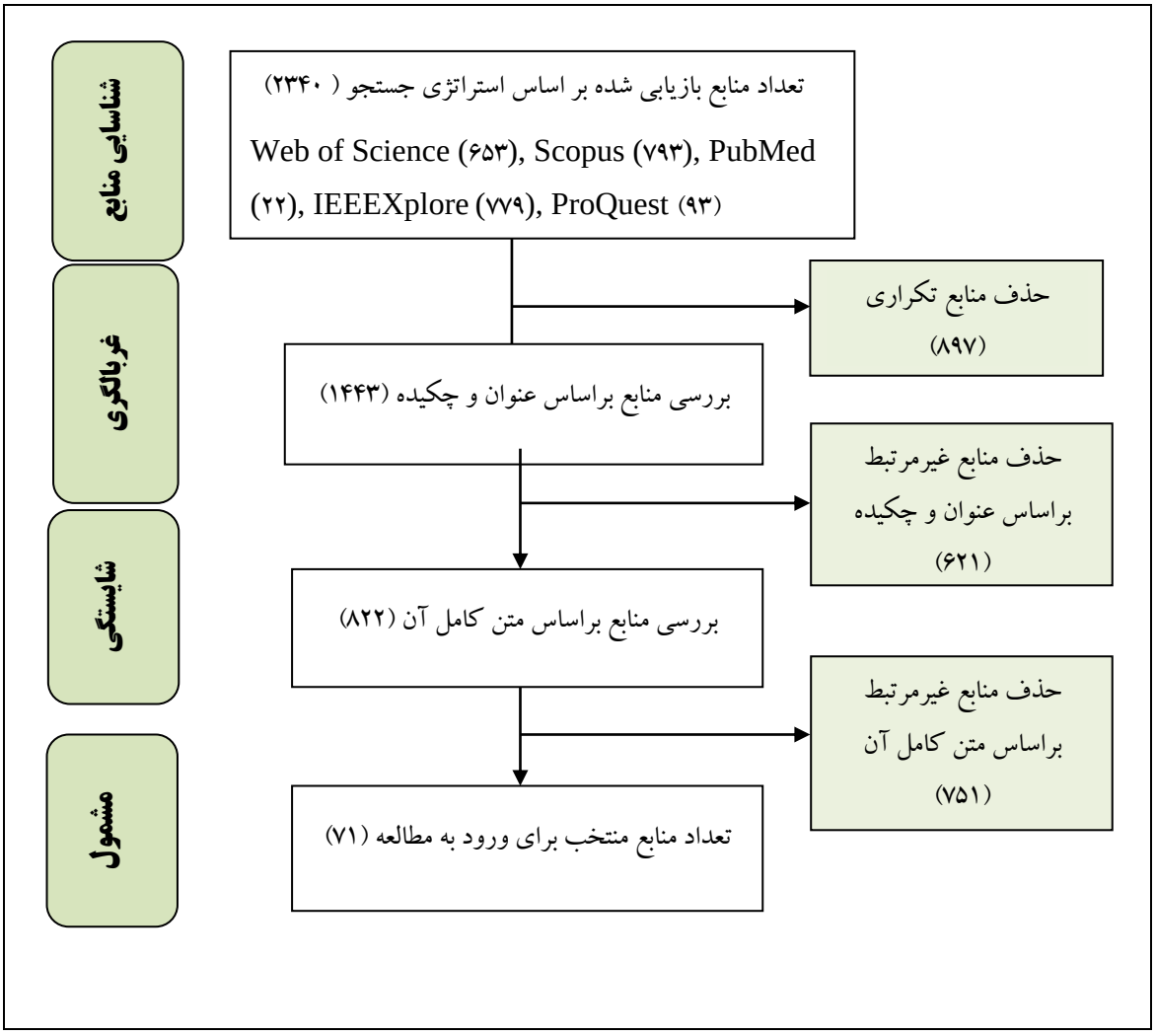
شد و در نهایت، منابعی انتخاب شد که متن کامل آن‌ها در راستای هدف پژوهش بود. تحلیل داده به شیوه تحلیل محتوای تجمعی(Summative content analysis) انجام شد. در این پژوهش بر شناسایی مؤلفه‌های مکانیسم‌های امنیتی، شمارش فراوانی آن و کمی کردن کلمات یا مضامین ویژه در متن متمرکز بوده است. همچنین، با هدف فهم، تفسیر و ارتباط این کلمات یا محتوا در متن صورت گرفت. بدین صورت که، با توجه به اهداف پژوهش محتوای مرتبط از هر مطالعه استخراج شد. واحدهای معنایی در این پژوهش کلمات، عبارات و جملاتی بودند که در منابع منتشرشده به صورت گسترده بررسی شدند. واحدهای معنایی چندین بار مطالعه شده و با استفاده از کلمات و تفسیر متون، کدگذاری اولیه انجام شد. کدها چندین بار بازخوانی شد و بر اساس تشابه و تناسب مفاهیم، در یک زیر طبقه قرار گرفتند. در مرحله بعد، طبقات نیز با یکدیگر مقایسه شدند و طبقاتی که ازنظر خصوصیات مشابه بودند در یکدیگر تلفیق و طبقه وسیع‌تری را تشکیل دادند و درنهایت طبقات اصلی نمایان گردید. [۲۰]

جدول ۲: خلاصه‌ای از استراتژی جستجو به تفکیک پایگاه داده

نام پایگاه داده	استراتژی جستجو
وب آو ساینس	TS=("internet of things" OR "internet of objects" OR "ambient intelligence" OR "ubiquitous computing" OR "pervasive computing" OR "heterogeneous sensor" OR "cyber physical system" OR "machine to machine communication") AND TS=(architecture OR framework OR taxonomy OR classification) AND TS=(security) AND TS=(mechanism OR countermeasure)
اسکوپوس	(TITLE-ABS-KEY ("internet of things" OR "internet of objects" OR "ambient intelligence" OR "ubiquitous computing" OR "pervasive computing" OR "heterogeneous sensor" OR "cyber physical system" OR "machine to machine communication")) AND (TITLE-ABS-KEY (architecture OR framework OR taxonomy OR classification)) AND ((TITLE-ABS-KEY (security)) AND (TITLE-ABS-KEY (mechanism OR countermeasure)))
پابمد	((((((((((("internet of things"[TIAB]) OR "internet of objects"[TIAB]) OR "ambient intelligence"[TIAB]) OR "ubiquitous computing"[TIAB]) OR "pervasive computing"[TIAB]) OR "heterogeneous sensor"[TIAB]) OR "cyber physical system"[TIAB]) OR "machine to machine communication"[TIAB])) AND ((((architecture[TIAB]) OR framework[TIAB]) OR taxonomy[TIAB]) OR classification[TIAB])) AND Security[TIAB]) AND (((((mechanism*[TIAB]) OR countermeasure*[TIAB]))
آی تریپل ای	("internet of things" OR "internet of objects" OR "ambient intelligence" OR "ubiquitous computing" OR "pervasive computing" OR "heterogeneous sensor" OR "cyber physical system" OR "machine to machine communication") AND (architecture OR framework OR taxonomy OR classification) AND ((security) AND (mechanism OR countermeasure))
پروکوئست	ab("internet of things" OR "internet of objects" OR "ambient intelligence" OR "ubiquitous computing" OR "pervasive computing" OR "heterogeneous sensor" OR "cyber physical system" OR "machine to machine communication") AND ab(architecture OR framework OR taxonomy OR classification) AND ab(security AND (mechanism OR countermeasure))

یافته ها

فرایند بررسی و انتخاب مطالعات در نمودار یک نشان داده شده است. در مجموع ۲۳۴۰ مطالعه با جستجوی کلیدواژه ها در پایگاه‌های داده حاصل شد که ۸۹۷ مطالعه تکراری، ۶۲۱ منبع غیر مرتبط براساس عنوان و چکیده و ۷۵۱ منبع غیر مرتبط براساس متن کامل حذف شد. در نهایت ۷۱ مطالعه مرتبط با مکانیسم های امنیت IoT شناسایی شد. جدول سه خلاصه ای از یافته های مکانیسم امنیت و حریم خصوصی IoT در صنعت سلامت و غیر سلامت به تصویر کشیده است. براساس یافته‌های مرور نظام‌یافته، این مکانیسم ها به تفکیک در سه لایه از معماری IoT (ادراکی، شبکه و کاربردی) نشان داده شده است (جدول ۳).



نمودار ۱: فرایند بررسی و انتخاب مطالعات

جدول ۳: مکانیسم‌های امنیت و حریم خصوصی IoT

طبقه اصلی	طبقه فرعی	صنعت		لایه‌های امنیتی			منبع	فراوانی
		سلامت	غیر سلامت	ادراکی	شبکه	کاربردی		
مکانیسم رمزنگاری	رمزنگاری سبک‌وزن متقارن	✓	✓	✓	✓	✓	[۱۴, ۱۵, ۲۱-۷۶]	۵۸
	رمزنگاری سبک‌وزن نامتقارن	✓	✓	✓	✓	✓	[۱۴, ۱۵, ۲۱-۷۶]	۵۸
	توابع هش[1]	✓	✓	✓	✓	✓	[۱۴, ۲۱-۴۱, ۴۳-۴۶, ۴۸-۵۴, ۵۶-۶۱, ۶۳-۷۵, ۷۷]	۵۳

جدول ۳: (ادامه)

طبقه اصلی	طبقه فرعی		صنعت		لایه‌های امنیتی			منبع	فراوانی
			سلامت	غیر سلامت	ادراکی	شبکه	کاربردی		
مکانیسم توزیع و مدیریت کلید	تدوین و اجرای فرایند مدیریت کلید شامل: ایجاد، توزیع، نگهداری، ابطال و بروز رسانی کلیدها توافق کلید قبل از رمزنگاری داده استفاده از زیرساخت کلید عمومی		✓	✓	✓	✓	✓	[۱۵, ۲۲, ۲۶-۲۸, ۳۰-۳۲, ۳۴-۳۸, ۴۲-۴۴, ۴۷-۴۹, ۵۱, ۵۲, ۵۵-۵۷, ۶۱-۶۴, ۶۶-۷۲, ۷۸]	۳۶
مدیریت هویت دیجیتال	مکانیسم شناسایی و احراز هویت	مکانیسم‌های احراز هویت تک عاملی و چندعاملی برای موجودیت‌ها (رمز عبور، کارت‌های هوشمند یا توکن و بیومتریک)	✓	✓	✓	✓	✓	[۱۴,۱۵,۲۱ - ۵۴,۵۶,۵۷,۶۰-۷۲,-۷۷ ۷۴,۸۰-۸۳]	۵۹
	مکانیسم کنترل دسترسی	صدور مجوز دسترسی به موجودیت ها براساس نقش‌ها و مسئولیت (RBAC)[۲]	✓	✓	✓	✓	✓	[۲۳, ۲۴, ۳۳, ۵۰, ۵۱]	۵
		صدور مجوز دسترسی به موجودیت‌ها بر اساس خصوصیات (ABAC)[۳]	✓	✓	✓	✓	✓	[۲۴, ۳۳, ۳۴, ۵۴]	۴
		بکارگیری فهرست کنترل دسترسی (ACLs)[۴] به‌منظور بررسی و مجوز دسترسی به درخواست‌های کاربران در سیستم IoT	✓	✓	✓	✓	✓	[۴۱،۵۵،۶۰،۶۴،۷۵،۸۲، ۸۳]	۷
مکانیسم صرفه‌جویی در توان مصرفی	طرح برداشت انرژی[۵] از محیط خارجی (مثل انرژی خورشیدی)		-	✓	✓	–	–	[۶۷]	۱
مخفی سازی داده‌ها و تصاویر	استگانوگرافی (نهان‌نگاری)		-	✓	✓	–	–	[۷۸]	۱
	واترمارکینگ (نشان‌گذاری)		✓	✓	✓	✓	✓	[۴۰ ,۴۳ ,۴۸ ,۴۹ ,۸۴]	۵

جدول ۳: (ادامه)

طبقه اصلی	طبقه فرعی	صنعت		لایه‌های امنیتی			منبع	فراوانی
		سلامت	غیر سلامت	ادراکی	شبکه	کاربردی		
مکانیسم‌های مربوط به مدیریت نگهداشت چرخه حیات سیستم	بروز رسانی و وصله‌های امنیتی در نرم‌افزار و ثابت‌افزارها	✓	✓	✓	✓	✓	[۱۴, ۱۵, ۲۳, ۲۹, ۳۱, ۳۴, ۳۵, ۳۹-۴۱, ۴۶, ۵۳, ۶۰, ۷۵, ۷۷, ۷۹]	۱۶
	پیکربندی مناسب سیستم عامل‌ها و برنامه‌های کاربردی	✓	✓	–	–	✓	[۲۸, ۲۹, ۴۰, ۵۳, ۶۴, ۷۸]	۶
	ضد بدافزارها (نرم‌افزارهای ضدویروس، جاسوس‌افزار و تله عسل[۶])	-	✓	✓	✓	✓	[۲۳, ۲۸, ۳۲, ۳۶, ۳۹, ۴۱, ۴۶, ۵۲-۵۵, ۶۰, ۶۷, ۷۵, ۷۹, ۸۵]	۱۶
	بکارگیری بوت امن	✓	✓	✓	-	-	[۳۹, ۴۱, ۵۱, ۶۴, ۷۵, ۷۷, ۷۹]	۷
	پشتیبان گیری و بازیابی فاجعه	✓	✓	–	✓	✓	[۳۱, ۳۲, ۳۷, ۴۰, ۴۳, ۶۰, ۶۸]	۷
	تست نفوذ و ارزیابی امنیت نرم‌افزار IoT قبل از پیاده‌سازی کامل سیستم	-	✓	–	–	✓	[۲۳, ۲۴, ۳۵, ۵۴]	۴
	ایزوله سازی و جعبه شنی[۷] برای حفاظت از نرم‌افزارها	✓	✓	✓	–	✓	[۲۳, ۳۱, ۶۴, ۷۹]	۴
	آموزش و آگاهی کاربران در خصوص آسیب‌ها و تهدیدات امنیتی	✓	✓	–	–	✓	[۲۹, ۳۶, ۴۶, ۴۷, ۵۲, ۵۴, ۶۴, ۷۵]	۸
	ممیزی و پایش مستمر رویدادهای امنیتی	-	✓	✓	✓	✓	[۱۵,۲۳,۲۴,۲۸,۳۰,۴۳, ۵۴,۵۵,۷۷,۷۹,۸۱,۸۴]	۱۲
	ارزیابی مخاطرات و تحلیل پیامدها	✓	✓	✓	–	✓	[۱۴, ۱۵, ۲۹, ۳۹-۴۱, ۴۶, ۶۰, ۷۴]	۱۰
سیاست‌ها، استانداردها و قوانین امنیتی	تقویت قوانین و سیاست‌های امنیت اطلاعات پیرامون مدیریت رمز عبور، منابع و مالکیت معنوی فقنامه سطح خدمات (SLA)[۸] استانداردهای رمزگذاری واحد مدیریت و حاکمیت کلان داده[۹]	✓	✓	✓	✓	✓	[۲۲،۲۹-۳۱،۳۴-۳۶،۴۳،۴۴،۴۷-۴۹،۵۲،۵۳،۶۲،۶۴،۶۷، ۷۰]	۱۸

جدول ۳: (ادامه)

طبقه اصلی	طبقه فرعی	صنعت		لایه‌های امنیتی			منبع	فراوانی
		سلامت	غیر سلامت	ادراکی	شبکه	کاربردی		
مکانیسم مسیریابی امن	نظیر خوشه‌بندی، همگام‌سازی داده‌ها و مسیریاب چند گام	✓	✓	✓	✓	✓	[۲۲-۲۴,۲۸,۲۹,۳۱,۳۲,۳۷,۳۹,۴۱,۴۳,۴۴,۴۶,۴۸,۴۹,۵۶,۵۷,۶۰-۶۲,۶۴,۶۷,۶۹,۷۱,۷۲,۷۴,۷۵,۸۱-۸۳]	۳۰
سیستم تشخیص نفوذ و پیشگیری (IDPS)	سیستم تشخیص نفوذ (IDS)	-	✓	✓	✓	✓	[۲۱, ۲۳-۳۰, ۳۲, ۳۴-۳۹, ۴۱-۴۳, ۴۵-۴۹, ۵۱, ۵۲, ۵۵-۵۷, ۶۰-۶۳, ۶۶, ۶۸, ۶۹, ۷۲, ۷۴, ۷۵, ۸۴]	۴۱
	سیستم جلوگیری از نفوذ (IPS)	-	✓	✓	✓	✓	[۲۸, ۳۰, ۴۳, ۵۱, ۷۹]	۵
	تحلیل رفتار ناهنجاری	-	✓	✓	✓	✓	[۲۱, ۲۵, ۳۵, ۴۳, ۴۵, ۵۴, ۵۶, ۸۵]	۸
	دیواره آتش	–	✓	✓	✓	✓	[۱۴, ۲۱, ۲۳-۲۵, ۲۹, ۳۰, ۳۴, ۳۵, ۳۷, ۳۹, ۴۱, ۴۶, ۵۳-۵۵, ۵۸, ۶۰, ۶۱, ۶۷, ۷۵, ۷۹, ۸۲, ۸۵]	۲۴
مکانیسم مدیریت اعتماد	• ایجاد یک سیستم معتمد در کل لایه‌های IoT • برقراری ارتباط معتمد بین لایه‌های IoT • ایجاد سطح اعتماد بین سیستم IoT و موجودیت نهایی	-	✓	✓	✓	✓	[۱۴,۱۵,۳۱,۳۲,۳۵,۴۰,۱,۴۷,۵۱,۵۶,-۶۳ ۶۰,۶۷, ۸۶-۸۸]	۱۷
	بلاکچین[10] و حاکمیت غیرمتمرکز	-	✓	✓	✓	✓	[۶۰،۷۳،۸۹]	۳
طراحی امن و حفاظت فیزیکی از سخت‌افزار سیستم	خود تخریبی ضد جعل و • بسته‌های ضد جعل • تغییر مدار به‌منظور جلوگیری از تروجان سخت‌افزاری	-	✓	✓	✓	✓	[۲۳,۳۷,۳۸,۴۳,۵۴,۵۹,۶۱,۶۹,۸۲]	۹
	تحلیل سیگنال‌های کانال جانبی	-	✓	✓	–	–	[۲۳]	۱
	سنجه برآورد فاصله امن در ارتباطات بی‌سیم	-	✓	✓	–	–	[۲۳]	۱

جدول ۳: (ادامه)

طبقه اصلی	طبقه فرعی	صنعت		لایه‌های امنیتی			منبع	فراوانی
		سلامت	غیر سلامت	ادراکی	شبکه	کاربردی		
مکانیسم تشخیص و تحمل خط	بررسی افزونگی دوره‌ای[11]	-	✓	✓	✓	–	[۳۹،۴۱،۶۰،۷۵،۸۴]	۵
	ضد پارازیت[12]	-	✓	✓	✓	–	[۲۱,۲۴,۲۵,۲۸,۳۷,۳۸, ۵۴,۵۸,۶۰,۶۶,۶۸, ۶۹]	۱۲
	تقسیم بافر[13]	–	✓	✓	–	–	[۳۵]	۱
	پراکندگی افزونگی بسته‌های قطعه قطعه شده[14]	–	✓	–	–	✓	[۳۹،۷۵]	۲

[1] Hah function, [2] RBAC: Role-Based Access Control, [3] ABAC: Attribute-Based Access Control,[4] ACL: Access-Control List, [5] Energy harvest scheme, [6] Honey pot, [7] Isolation and sandbox, [8] SLA: Service Level Agreement , [9] Big data, [10] Blockchain, [11] CRC: Cyclic Redundancy Check, [12] Anti-jamming , [13] buffer split, [14] FRS: Fragmentation Redundancy Scattering

بحث

از ۷۱ مطالعه که مکانیسم‌های امنیت IoT را در حوزه‌های مختلف بررسی کرده‌اند ۶۷ مطالعه مربوط به صنعت غیر سلامت بود و تنها چهار مطالعه اختصاص به صنعت سلامت داشت. این بدان معناست که موضوع IoT در صنعت مراقبت سلامت هنوز به بلوغ نرسیده و در مرحله ابتدایی قرار دارد. با توجه به نقش IoT در ارتقای مدیریت اطلاعات، تمامی اشیا در دستگاه‌های مراقبت بهداشتی (افراد و تجهیزات) می‌توانند به‌طور مداوم ردیابی و پایش شوند. [۹۰] بنابراین، IoT باید قابلیت امکان دستیابی افراد مجاز (پزشک، پرستار، رادیوژیست و فیزیوتراپ) را به تمامی اطلاعات پزشکی یک بیمار در محل‌های مختلف (بیمارستان‌ها و مطب پزشکان) فراهم نماید. [۹۱،۹۲] ضمن اینکه حفاظت از IoT در صنعت سلامت به دلیل محرمانگی و حساس بودن اطلاعات بیمار و دسترسی به موقع اطلاعات برای متخصصان مراقبت سلامت به مراتب دشوارتر است. [۵]

براساس یافته‌های پژوهش حاضر مکانیسم‌های امنیت IoT در ۱۱ طبقه اصلی سازماندهی شده‌اند که اکثر مطالعات به مکانیسم‌های رمزنگاری (Cryptography)، توزیع و مدیریت کلید (Key distribution and management)، مدیریت هویت دیجیتال (Digital identity management)، مدیریت نگهداشت چرخه حیات سیستم (System life-cycle maintenance management) و مسیریابی امن (Secure routing) در هر دو صنعت سلامت و غیر سلامت توجه کرده‌اند. یافته‌های مطالعه حاضر نشان داد که پنج مورد از مکانیسم‌های امنیتی باوجود اهمیتی که دارند در صنعت سلامت پرداخته نشده است، این مکانیسم‌ها در ارتباط با صرفه‌جویی توان مصرفی (Power saving)، طراحی امن و حفاظت فیزیکی از سخت‌افزار سیستم (Secure design and physical protection) ، سیستم تشخیص نفوذ و پیشگیری (Intrusion Detection and Prevention System (IDPS))، مدیریت اعتماد(Trust management) و تشخیص و تحمل خطا (Fault detection and tolerance) بودند.

یافته‌های حاصل از این پژوهش نشان داد که در صنعت مراقبت سلامت به مکانیسم‌های تشخیص و تحمل خطا توجه نشده است در حالی که یک طرح امنیتی مناسب باید تضمین نماید که خدمات IoT حتی در صورت وجود خرابی دستگاه‌ها، بلایای طبیعی در مقابل حملات و تهدیدات بتوانند کار کنند و از فعالیت بازنمانند. [۹۳] بسیاری از تهدیدات امنیتی مرتبط با لایه ادراکی و طراحی بخش سخت‌افزار سیستم IoT است. بنابراین، دستگاه‌ها باید از لحاظ فیزیکی امن بوده و اجزای مدارهای

فرکانس رادیویی نباید قابل تغییر و دستکاری باشد. [۳۹] از آنجا که داده‌ها از طریق حسگرها و دستگاه‌های مختلف IoT جمع‌آوری می‌شود، حفاظت و امنیت فیزیکی آن‌ها در همان ابتدا مهم است. بنابراین، امنیت فیزیکی دستگاه در قالب پوشش یا عایقی برای طراحی آنتن، گره‌های حسگر، ساختار سخت‌افزار و مدار مورد نیاز است تا از هرگونه دستکاری سخت‌افزار و جعل هویت جلوگیری شود. [۷۹] برای نمونه، استفاده از مکانیسم خود تخریبی می‌تواند مانع از جعل و دستکاری گره‌های حسگر شود بدین صورت که به محض باز شدن گره حسگر توسط مهاجم تمام اطلاعات مهم و حساس از بین می‌رود. [۲۳]

یافته‌های این پژوهش نشان داد تعداد کمی از مطالعات به آموزش و آگاهی کاربران توجه کرده‌اند. با توجه به اینکه اکثر کاربران پیرامون مسائل امنیتی در فضای مجازی و محافظت از اعتبارنامه‌ها آگاهی کافی و دانش لازم را ندارند. این عوامل زمینه را برای بسیاری از حملات مانند جستجوی فراگیر (Brute force)، حمله دیکشنری (Dictionary)، مهندسی اجتماعی (Social engineering) و فیشینگ (Phishing) فراهم می‌کند که کاربران ناخواسته کدهای مخرب را با کلیک روی لینک‌های آلوده در ایمیل‌ها دانلود کرده و مهاجم رمز عبور کاربر را حدس می‌زند. [۹۴] از اینرو، آموزش و آگاهی کاربران در خصوص آسیب‌ها و تهدیدات امنیت IoT به ویژه مدیریت رمز عبور و نحوه استفاده صحیح از خدمات این فناوری حائز اهمیت است. [۳۶،۵۲]

نتایج حاصل از مرور نظام‌یافته نشان داد بیشتر مطالعات مکانیسم‌های مرتبط با مدیریت هویت دیجیتال، رمزنگاری و مدیریت کلید را برای حفاظت از دستگاه‌های IoT مهم شناخته‌اند. زیرا مکانیسم‌های رمزنگاری از حمله استراق سمع و تداخل فرکانس های رادیویی جلوگیری می‌کند و می‌توان اطمینان حاصل کرد که اطلاعات حساس در فرایند انتقال داده به دست فرد غیرمجاز نمی‌رسد. این در حالی است که برای رمزگذاری داده‌ها نیاز به مبادله کلید معتبر و طرح‌های مدیریت کلید است. [۳۲] در دنیای واقعی مدیریت کلید سخت‌ترین قسمت رمزنگاری محسوب می‌شود و حفاظت از کلیدهای سری کار بسیار دشواری است. از آنجا که احتمال حمله به دستگاه‌های رمز کلید عمومی و الگوریتم‌های رمزنگاری وجود دارد. از اینرو طراحی مطمئن و قدرتمند مدیریت کلید نقش بسزائی در امنیت تبادل داده دارد. در این رابطه وجود زیرساخت کلید عمومی (Public Key Infrastructure (PKI)) جهت تولید، نگهداری، عملیات صدور و توزیع گواهینامه برای کلید عمومی، نگهداری و انتشار لیست گواهی‌های لغو شده امری حیاتی است. [۶۲،۹۵]

قابل ذکر است که دومین عامل مهم امنیت IoT توافق کلید است که قبل از رمزنگاری داده به عنوان فرآیند مهم شناخته می‌شود. از اینرو حصول اطمینان از احراز هویت و توافق کلید در شبکه‌های ناهمگون و نامتجانس حائز اهمیت است. ایجاد یک کلید نشست امن بین اشیا در محیط IoT می‌تواند ارتباط ایمن بین کاربر و گره‌های حسگر را تضمین نماید. [۳۵،۶۲]

نکته مهم دیگر آن است که امنیت IoT فقط با تکیه بر مکانیسم رمز عبور و الگوریتم‌های رمزنگاری تأمین نمی‌شود برای حفاظت از احراز هویت موجودیت‌ها و تمامیت (Integrity) داده نیاز است که گره‌های حسگر قانونی باشد. بنابراین، مکانیسم مدیریت اعتماد برای اطمینان از اعتماد در روابط بین دستگاه‌های IoT و کاربران ضروری است. درحالی‌که حسگرهای و دستگاه‌های پزشکی IoT در محیط‌های باز و کنترل نشده تعبیه‌شده‌اند. وجود مکانیسم‌های اعتماد برای غلبه بر محیط‌های ناامن و پرخطر در استفاده از خدمات و برنامه‌های IoT اساسی است. [۳۲،۴۱،۸۶] اخیراً بسیاری از دستگاه‌های سلامت الکترونیک از طریق مکانیسم‌های امنیتی ایستا نظیر دیواره آتش (Firewall) و دستگاه‌های تشخیص نفوذ) حفاظت می‌شود. [۱۲،۹۶] درحالی‌که این مکانیسم‌ها به‌تنهایی نمی‌توانند اهداف و الزامات امنیتی را در محیط پویای IoT تأمین نمایند. اگرمعماری IoT بتواند مسئله امنیت سایبری (Cyber security) و تاب‌آوری سایبری (Cyber resilience) را تامین کند. این دستگاه‌ها به بالاترین سطح اعتمادپذیری خواهند

رسید. [۵] سیستم مدیریت اعتماد باید برای تضمین اهداف و مکانیسم‌های امنیتی به طور موفقیت‌آمیزی اعمال شود.

یکی از چالش‌های IoT در صنعت مراقبت سلامت عدم مکانیسم‌های نظارتی در شرایط اورژانسی و نبود قوانین و مقررات، استانداردها و سیاست‌های مدون است. علاوه بر این، هیچ راهکاری برای نظارت بر قابلیت دسترسی، پایش منابع موجود و پیش‌بینی حملات احتمالی امنیتی و خرابی‌های تجهیزات پزشکی از راه دور ارائه نشده است. به‌عنوان‌مثال محصولات کاشتنی در بدن با سیستم فعلی قادر به برقراری ارتباط امن از راه دور نیستند. همچنین، حسگرها در مواقع اورژانسی قادر به تولید هشدار و ارسال داده‌ها به پزشکان از راه دور و درمان فوری نیستند. در موقعیت اورژانسی کارکنان پزشکی نیاز به تنظیم عملکرد یا حتی غیرفعال کردن دستگاه‌های کاشتنی در بدن برای اهداف درمان دارند. تصور کنید که یک بیمار ناگهان در وضعیت اضطراری قرار گیرد تأخیر طولانی در به دست آوردن این اعتبارنامه، می‌تواند موجب از دست رفتن جان بیمار شود. [۹۷] بنابراین، تمام دستگاه‌های IoT باید مطابق با استانداردها و خط‌مشی‌های امنیتی باشد. علاوه براین، داده‌های موجود در برچسب RFID برای تبادل داده باید از یک استاندارد رمزگذاری واحد تبعیت کند. [۳۱،۶۲]

تحلیل یافته ها نشان داد اگر چه محدودیت توان مصرفی یکی از موانع مهم در شبکه IoT است اما تدابیر و راهکار امنیتی چندانی برای آن ذکر نشده است. این فناوری از دستگاه‌های کوچک با باتری محدود تشکیل‌شده است و دارای قدرت کم و ذخیره‌سازی پائین هستند. بنابراین، الگوریتم‌های رمزنگاری سنتی نمی‌توانند مستقیماً روی چنین دستگاه‌هایی با توان پایین قرار گیرد. این دستگاه‌ها در زمانی که نیازی به پردازش و ارسال داده نیست باید در حالت ذخیره مصرف انرژی قرار گیرند. دستگاه‌هایی که انرژی کافی ندارند، اساساً نمی‌توانند به‌طور عادی کار کنند. [۹۸] بنابراین، محدودیت انرژی، یافتن راه‌حل امنیتی را به چالش می‌کشد. دستگاه‌های تعبیه‌شده IoT متشکل از دستگاه‌ها و پشته‌های پروتکل شبکه ضعیف و فاقد ماژول‌های امنیتی کافی هستند. [۴۰،۹۹] در همین راستا براساس یافته‌های پژوهش تنها یک مطالعه طرح برداشت انرژی از محیط خارجی (مثل انرژی خورشیدی) را به عنوان راه‌حل امنیتی برای صرفه‌جویی در توان مصرفی مطرح کرده است.

از محدودیت‌های پژوهش حاضر می‌توان به تعداد اندک مطالعات در خصوص امنیت IoT در صنعت مراقبت سلامت اشاره نمود. پیشنهاد می‌شود برای طراحی و پیاده‌سازی معماری امن IoT به تهدیدات و مکانیسم‌های امنیتی این حوزه توجه شود. از نقاط قوت این پژوهش مرور جامع و طبقه‌بندی مفهومی از مکانیسم‌های امنیت IoT بود که بینش وسیعی را برای محققان، مدیران و متخصصان امنیت اطلاعات در جهت مقابله با تهدیدات و حملات امنیتی IoT فراهم می‌کند.

ملاحظات اخلاقی

ملاحظات اخلاقی: این پژوهش با کد اخلاق شماره IR.IUMS.REC.1396.9321563003 انجام شده است.

حمایت مالی: این پژوهش با حمایت مالی دانشگاه علوم پزشکی ایران، تهران انجام شده است.

تضاد منافع: نویسندگان اظهار داشتند که تضاد منافعی وجود ندارد.

تشکر و قدردانی: این پژوهش بخشی از پایان نامه با عنوان ارائه چارچوب امنیت اینترنت اشیا مراقبت سلامت برای ایران، در مقطع دکترای تخصصی، مصوب دانشگاه عوم پزشکی ایران در سال ۱۳۹۶ می‌باشد.

References

1. Lei y, Ma P, Zhao L. The internet of things brings new wave of the information industry. IJCSNS. 2011;11(5):15-21.
2. KIM JT. Privacy and security issues for healthcare system with embedded RFID system on internet of things.Adv. Sci. Technol. Lett. 2014;72:109-12.
3. Bandyopadhyay D, Sen J. Internet of things: Applications and challenges in technology and standardization. Wireless Pers Comm. 2011;58(1):49-69.
4. Chandrakanth S, Venkatesh K, Mahesh Ju, Naganjaneyulu K. Internet of thing. Int J Innov Res Sci Eng Technol. 2014;3(8):16-20.
5. Nasiri S, Sadoughi F, Tadayon MH, Dehnad A. Security requirements of internet of things-based healthcare system: A survey study. Acta Inform Med. 2019;27(4):253-8.
6. Ray PP. Home health hub internet of things (h 3 iot): An architectural framework for monitoring health of elderly people. Proceedings of the 2014 International Conference On Science Engineering And Management Rresearch (ICSEMR); 2014 nov 27-29; Chennai, India. Piscataway, New Jersey: IEEE; 2014.P. 1-3.
7. Islam S, Kwak D, Kabir M, Hossain M, Kwak K. The internet of things for health care: A comprehensive survey. IEEE Access. 2015;3:678-708.
8. Diogo P, Reis LP, Vasco Lopes N. Internet of things: A system's architecture proposal. In: Rocha A, Fonseca D, Redondo E, Reis LP, Cota MP, editors. Proceedings of the 9th Iberian Conference On Information Systems And Technologies (CISTI); 2014 Jun 18-21; Barcelona, Spain. New York: IEEE; 2014. P.1-6 .
9. Basu SS, Tripathy S, Chowdhury AR. Design challenges and security issues in the internet of things. In: Vig j, roy ak, wang c, das ml,editors. Proceedings of the IEEE Region 10 Symposium; 2015 May 13-15; Ahmedabad, India. New York: IEEE; 2015. P.90-93.
10. Wong K-S, Kim MH. Towards self-awareness privacy protection for internet of things data collection. J Appl Math. 2014;2014:1-9.
11. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IoT). In: Meghanathan N, Boumerdassi S, Chaki N, Nagamalai D, editors. Recent ttrends in network security and applications: Proceedings Of The Third Conference on Network Security And Applications, CNSA; 2010 Jul 23-25; Chennai, India. Berlin, Heidelberg: Springer; 2010.P. 420-9 .
12. Habib K, Leister W. Threats identification for the smart internet of things in ehealth and adaptive security countermeasures. In: Badra M, Boukerche A, Urien P, Editors. Proceedings of The 7th International Conference on New Technologies, Mobility And Security (NTMS); 2015 July 27-29; Paris, France. New York: IEEE; 2015. P. 1-5.

13. Namazii Z, Kalantari N, Nezamolhosseini AS. Internet of things and smart health: Benefits and challenges ahead. Proceedings of the 3rd International Conference On Applied Research In Computer & Information; 2016 Feb 4; Malek Ashtar University Of Technology.Tehran: Civilica. P.1-19. [In Persian]

14. Abdul Rahman AF, Daud M, Mohamad MZ. Securing sensor to cloud ecosystem using internet of things (IoT) security framework. In: Guezouli L, Cruz HT, Hidoussi F, Boubiche DE, Bounceur A, editors. Proceedings of the International Conference on Internet of Things and Cloud Computing; 2016 Mar 22-23; Cambridge, United Kingdom; 2016. p. 1-5.

15. Kumar SA, Vealey T, Srivastava H. Security in internet of things: Challenges, solutions and future directions. In: Bui TX, Sprague RH, editors. Proceedings of the 49th Annual Hawaii International Conference on System Sciences; 2016 Jan 5-8; Koloa, HI , USA; 2016. p. 5772-81.

16. Ahmed Sms, Zulhuda S. The concept of internet of things and its challenges to privacy. South East Asian Journal Of Contemporary Business, Economics And Law.2015;8(4):1-6.

17. Jose S. IOT, AoT, AI, machine learning, cloud, big data and predictive analytics to dominate in 2017: Teradata India [Internet]. India: Tech And Startups; 2017 [cited 2017 Mar 4] ; Available from: https://se.Linkedin.Com/pulse/iot-aot-ai-machine-learning-cloud-big-data-predictive-sunil-jose.

18. Zhang B, Ma X-X, Qin Z-G. Security architecture on the trusting internet of things. J Electron Sci Tech China. 2011;9(4):364-7.

19. Babar S, Stango A, Prasad N, Sen J, Prasad R. Proposed embedded security framework for internet of things (iot). Proceedings Of The 2nd International Conference On Wireless Communication, Vehicular Technology, Information Theory And Aerospace & Electronic Systems Technology; 2011 Feb 28 - Mar 3; Chennai, Iindia. New York: IEEE; 2011. P.1-5.

20. Parvizy S, Adib-Hajbaghery M, Salsali M. Principles and methods in qualitative research. Tehran: Jameengar; 2014. [In Persian]

21. Pacheco J, Ibarra D, Vijay A, Hariri S. IoT security framework for smart water system. Proceedings of the IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA); 2017Oct 30 -Nov 3; Hammamet, Tunisia 2017. p. 1285-92.

22. Gao Y, Peng Y, Xie F, Zhao W, Wang D, Han X, et al. Analysis of security threats and vulnerability for cyber-physical systems. Proceedings of the 3rd International Conference on Computer Science and Network Technology; 2013 Oct 12-13 Dalian, China; 2014. p. 50-5.

23. Mosenia A, Jha NK. A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput. 2017;5(4):586-602.

24. Wang XF. Research on security issues of the internet of things. Adv Mater Res. 2014;989-994:4261-4.

25. Pacheco J, Hariri S. IoT security framework for smart cyber infrastructures. In: Lewis PR, Muller-Schloer C, Elnikety S, editors. Proceedings of the IEEE 1st International Workshops on Foundations and Applications of Self- Systems (FAS-W); 2016 Sept 12-16 Augsburg, Germany; 2016. p. 242-7.

26. Saadeh M, Sleit A, Qatawneh M, Almobaideen W. Authentication techniques for the internet of things: A survey. Cybersecurity and Cyberforensics Conference; 2016 Aug 2-4; Amman, Jordan 2016. p. 28-34.

27. Saadeh M, Sleit A, Sabri KE, Almobaideen W. Hierarchical architecture and protocol for mobile object authentication in the context of IoT smart cities. J Network Comput Appl. 2018;121:1-19.

28. ur Rehman S, Iannella A, Gruhn V. A security based reference architecture for cyber-physical systems. International Conference on Applied Informatics; 2018 Oct 25 Bogotá, Colombia; 2018. p. 157-69.

29. Samaila MG, Sequeiros JBF, Freire MM, Inácio PRM. Security threats and possible countermeasures in IoT applications covering different industry domains. Proceedings of the 13th International Conference on Availability, Reliability and Security; 2018 Aug; Hamburg, Germany; 2018. p. 1-9.

30. Zhang Y, Zou W, Chen X, Yang C, Cao J. The security for power internet of things: Framework, policies, and countermeasures. 2014 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery; 2014 Oct 13-15; Shanghai, China 2014. p. 139-42.

31. Jing Q, Vasilakos AV, Wan JF, Lu JW, Qiu DC. Security of the internet of things: Perspectives and challenges. Wirel Netw. 2014;20(8):2481-501.

32. Wu Q, Jiang L. A flexible security architecture for the internet of things. Appl Mech Mater. 2013;241-244:3255-9.

33. Lee JD, Yoon TS, Chung SH, Cha HS. Service-oriented security framework for remote medical services in the internet of things environment. Healthc Inform Res. 2015;21(4):271-82.

34. Ghadeer H. Cybersecurity issues in internet of things and countermeasures. Proceedings of the IEEE International Conference on Industrial Internet (ICII); 2018 Oct 21-23; Seattle, Washington, United States; 2018. p. 195-201.

35. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82:395-411.

36. Adat V, Gupta BB. Security in internet of things: Issues, challenges, taxonomy, and architecture. Telecommun Syst. 2018;67(3):423-41.

37. Matharu GS, Upadhyay P, Chaudhary L. The internet of things: Challenges & security issues. Proceedings of the International Conference on Emerging Technologies (ICET); 2014 Dec 8-9; Islamabad, Pakistan; 2014. p. 54-9.

38. Krishna BVS, Gnanasekaran T. A systematic study of security issues in internet-of-things (IoT). Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2017 Feb 10-11 Palladam, India; 2017. p. 107-11.

39. Ahmed AW, Ahmed MM, Khan OA, Shah MA. A comprehensive analysis on the security threats and their countermeasures of IoT. Int J Adv Comput Sci Appl. 2017;8(7):489-501.

40. Ben Ida I, Jemai A, Loukil A. A survey on security of IoT in the context of ehealth and clouds. Proceedings of the 11th International Design & Test Symposium; 2016 Dec 18-20; Hammamet, Tunisia; 2017. p. 25-30.

41. Andrea I, Chrysostomou C, Hadjichristofi G. Internet of things: Security vulnerabilities and challenges. Proceedings of the 3rd IEEE ISCC 2015 International Workshop on Smart City and Ubiquitous Computing Applications; 2015 Jul 6-9; Larnaca, Cyprus; 2016. p. 180-7.

42. Erfani S, Ahmadi M, Chen L. The internet of things for smart homes: An example. In: Saha HN, Chakrabarti S, editors. Proceedings of the 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON); 2017 Aug 16-18; Bangkok, Thailand; 2017. p. 153-7.

43. Sun H, Li Y, Yang Y, Feng L, Zhang H. A security scheme research of the internet of things based on the SA/NIA architecture. Adv Mater Res. 2011;320:291-6.

44. Zhang L, Wang Q, Tian B. Security threats and measures for the cyber-physical systems. J China Univ Post Telecom. 2013;20(1):25-9.

45. Abbou AN, Baddi Y, Hasbi A. Software defined networks in internet of things integration security: Challenges and solutions. Proceedings of the 6th International Conference on Wireless Networks and Mobile Communications (WINCOM); 2018 Oct 16-19; Marrakesh, Morocco; 2018. p. 1-6.

46. Dazine J, Maizate A, Hassouni L. Internet of things security. Proceedings of the IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD); 2018 Nov 21-23; Marrakech, Morocco; 2018. p. 137-41.

47. Rahimi H, Zibaeenejad A, Rajabzadeh P, Safavi AA. On the security of the 5g-IoT architecture. Proceedings of the International Conference on Smart Cities and Internet of Things; 2018 Sep 26-27; Mashhad, Iran; 2018. p. 1-8.

48. Verma H, Chahal K. A review on security problems and measures of internet of things. Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS); 2017 June 15-16; Madurai, India 2018. p. 71-6.

49. Zhao K, Ge L. A survey on the internet of things security. 2013 Ninth International Conference on Computational Intelligence and Security; 14-15 Dec. 2013; Leshan, China; 2013. p. 663-7.

50. Chen W, Song X, Liu W. Research of information security framework in ubiquitous environment. Adv Mater Res. 2012;433-440:1397-9.

51. Burhan M, Rehman RA, Khan B, Kim BS. IoT elements, layered architectures and security issues: A comprehensive survey. Sensors (Basel). 2018;18(9):2796.

52. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: A review. International Conference on Computer Science and Electronics Engineering; 2012 Mar 23-25; Hangzhou, China; 2012. p. 648-51.

53. Li S, Tryfonas T, Li H. The internet of things: A security point of view. Internet Res. 2016;26(2):337-59.

54. Varga P, Plosz S, Soos G, Hegedus C. Security threats and issues in automation IoT. Proceedings of the IEEE 13th International Workshop on Factory Communication Systems (WFCS); 2017 May 31-June 2 Trondheim, Norway; 2017. p. 1-6.

55. Chen L. Security management for the internet of things [M.Sc. thesis]. Ontario, Canada: Windsor Univ; 2017.

56. Chen D, Chang G, Jin L, Ren X, Li J, Li F. A novel secure architecture for the internet of things. Proceedings of the Fifth International Conference on Genetic and Evolutionary Computing; 2011 Aug 29 -Sept1; Xiamen, China; 2011. p. 311-4.

57. Li XR, Zheng S, Liu YL. Analysis and research on secure architecture in the internet of things. Appl Mech Mater. 2014;687-691:2205-9.

58. Lu T, Lin J, Zhao, Li Y, Peng Y. A security architecture in cyber-physical systems: Security theories, analysis, simulation and application fields. Int J Secur Appl. 2015;9(7):1-16.

59. Kim NY, Rathore S, Ryu JH, Park JH, Park JH. A survey on cyber physical system security for IoT: Issues, challenges, threats, solutions. Journal of Information Processing Systems. 2018;14(6):1361-84.

60. Yousuf O, Mir RN. A survey on the internet of things security: State-of-art, architecture, issues and countermeasures. Inf Comput Security. 2019;27(2):292-323.

61. Jain A, Singh T, Sharma SK. Threats paradigmin IoT ecosystem. Proceedings of the 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); 2018 Aug 29-31; Noida, India 2018. p. 664-70.

62. Ashibani Y, Mahmoud QH. Cyber physical systems security: Analysis, challenges and solutions. Comput Secur. 2017;68:81-97.

63. Dong P, Han Y, Guo X, Xie F. A systematic review of studies on cyber physical system security. Int J Secur Appl. 2015;9(1):155-64.

64. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT ehealth: Promises and challenges of IoT in medicine and healthcare. Future Gener Comput Syst. 2018;78:659-76.

65. Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status, challenges and prospective measures. Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015); 2015 Dec 14-16 London, UK; 2016. p. 336-41.

66. Mendez Mena D, Papapanagiotou I, Yang B. Internet of things: Survey on security. Inf Secur J. 2018;27(3):162-82.

67. Lin J, Yu W, Zhang N, Yang XY, Zhang HL, Zhao W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J. 2017;4(5):1125-42.

68. Harita U, Daya Sagar KV. A survey on secured internet of things architecture. Int J Eng Technol. 2018;7(2.7):274-6.

69. Kamble A, Bhutad S. Survey on internet of things (IoT) security issues & solutions. Proceedings of the 2nd International Conference on Inventive Systems and Control (ICISC); 2018 Jan 19-20; Coimbatore, India; 2018. p. 307-12.

70. Cvitić I, Vujić M, Husnjak S. Classification of security risks in the IoT environment. In: Katalinic B, editor. Proceedings of the 26th DAAAM International Symposium on Intelligent Manufacturing and Automation; 2015 Oct; Vienna, Austria; 2015. p. 731-40.

71. Lu Y, Da Xu L. Internet of things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things J. 2018;6(2): 2103 - 15.

72. El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. A survey of internet of things (IoT) authentication schemes. Sensors. 2019;19(5): E1141.

73. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, Sikdar B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access. 2019;7:82721-43.

74. U Farooq M, Waseem M, Khairi A, Sadia Mazhar P. A critical analysis on the security concerns of internet of things (IoT). Int J Comput Appl. 2015;111(7):1-6.

75. Ahemd MM, Shah MA, Wahid A. IoT security: A layered approach for attacks & defenses. Proceedings of the International Conference on Communication Technologies (ComTech); 2017 April 19-21; Rawalpindi, Pakistan; 2017. p. 104-10.

76. Jaigirdar FT, Rudolph C, Bain C. "Can i trust the data i see?" A physician's concern on medical data in IoT health architectures. Proceedings of the Australasian Computer Science Week Multiconference; 2019 Jan; Sydney, NSW, Australia; 2019.

77. Yaqoob I, Ahmed E, Rehman MHU, Ahmed AIA, Al-garadi MA, Imran M, et al. The rise of ransomware and emerging security challenges in the internet of things. Comput Networks. 2017;129:444-58.

78. Assiri A, Almagwashi H. IoT security and privacy issues. Proceedings of the 1st International Conference on Computer Applications and Information Security (ICCAIS); 2018 Apr 4-6; Riyadh, Saudi Arabia; 2018. p. 1-5.

79. Han ZB, Li XH, Huang KM, Feng ZY. A software defined network-based security assessment framework for cloudIoT. IEEE Internet Things J. 2018;5(3):1424-34.

80. Tabassum K, Ibrahim A, El Rahman SA. Security issues and challenges in IoT. 2019 International Conference on Computer and Information Sciences (ICCIS); 2019 Apr 3-4; Sakaka, Saudi Arabia; 2019. p. 1-5.

81. Virat MS, Bindu SM, Aishwarya B, Dhanush BN, Kounte MR. Security and privacy challenges in internet of things. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI); 11-12 May 2018; Tirunelveli, India; 2018. p. 454-60.

82. Daud M, Khan Q, Saleem Y. A study of key technologies for IoT and associated security challenges. Proceedings of the International Symposium on Wireless Systems and Networks (ISWSN); 2017 Nov 19-22; Lahore, Pakistan; 2018. p. 1-6.

83. Simha CY, Harshini VM, Raghuvamsi LVS, Kounte MR. Enabling technologies for internet of things & it's security issues. Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems; 2018 Jun 14-15; Madurai, India; 2018. p. 1849-52.

84. Ashraf QM, Habaebi MH. Autonomic schemes for threat mitigation in internet of things. J Network Comput Appl. 2015;49:112-27.

85. Deogirikar J, Vidhate A. Security attacks in IoT: A survey. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC); 2017 Feb 10-11; Palladam, India; 2017. p. 32-7.

86. Frustaci M, Pace P, Aloi G, Fortino G. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things J. 2018;5(4):2483-95.

87. Rauf A, Shaikh RA, Shah A. Security and privacy for IoT and fog computing paradigm. Proceedings of the 15th Learning and Technology Conference (L&T); 2018 Feb 25-26; Jeddah, Saudi Arabia; 2018. p. 96-101.

88. Sedrati A, Mezrioui A. A survey of security challenges in internet of things. Adv Sci, Technol Eng Syst. 2018;3(1):274-80.

89. Yu Y, Li Y, Tian J, Liu J. Blockchain-based solutions to security and privacy issues in the internet of things. IEEE Wirel Commun. 2018;25(6):12-8.

90. Da Xu L, Hhe W, Li S. Internet of things in industries: A survey. IEEE Trans Industr Inform. 2014;10(4):2233-43.

91. Vermesan O, Friess P. Internet of things: Converging technologies for smart environments and integrated ecosystems. Aalborg: River Publishers; 2013. .

92. Pang Z. Technologies and architectures of the internet-of-things (IoT) for health and well-being [PhD thesis]. Stockholm, Sweden: Kth Royal Institute of Technology; 2013. .

93. Zieglmeier V. Resilience metrics. Network. 2016;9:1-15.

94. Makhdoom I, Abolhasan M, Lipman J, Liu RP, Ni W. Anatomy of threats to the internet of things. IEEE Commun Surv Tut. 2018;21(2): 1636 – 1675.

95. Kheyrkhah A, Hajirezaei G, Pourkhanlar M, Matani M. Launch operational digital signature: 10 PKI major threats. Proceedings Of The 2nd Conference On Electronic Banking And Payment System; 2013 Feb 17; IRIB International Conference Center; 2013. p. 1-14.

96. Olivier F, Carlos G, Florent N. New security architecture for IoT network. Procedia Comput Sci. 2015;52:1028-33.

97. Rekhis S, Boudriga N, Ellouze N. Securing implantable medical devices against cyberspace attacks. Proceedings of the 2nd International Conference on Anti-Cyber Crimes (ICACC); 2017 Mar 26-27 Abha, Saudi Arabia; 2017. p. 187-92.

98. Jaiswal S, Gupta D. Security requirements for internet of things (IoT). In: Modi N, Verma P, Trivedi B, editors. Proceedings of the International Conference on Communication and Networks; 2016 Feb; Ahmedabad, India; 2017. p. 419-27.

99. Hossain MM, Fotouhi M, Hasan R. Towards an analysis of security issues, challenges, and open problems in the internet of things. Proceedings of the 2015 IEEE World Congress on Services; 2015 June 27-July2; New York, USA; 2015. p. 21-8.