بهبود امنیت اینترنت اشیا) (IoTبا شبکه سازی تعریف‌شده توسط نرم‌افزار) (SDN

مقدمه

استفاده از اینترنت اشیا) (IoTافزایش‌یافته است، که اخیرا به یک حوزه مورد علاقه تبدیل شده‌است، زیرا به طور گسترده برای برنامه‌ها و دستگاه‌های متعدد مانند سنسورهای بی‌سیم، دستگاه‌های پزشکی، سنسورهای خانگی حساس، و دیگر دستگاه‌های IoT مرتبط مورد استفاده قرار می‌گیرد.. با توجه به تقاضا برای انتشار سریع محصولات جدید IoT در بازار، جنبه‌های امنیتی اغلب نادیده گرفته می‌شوند زیرا بررسی تمام آسیب‌پذیری‌های ممکن زمان می‌برد .

تعریف مسئله و هدف اصلی مقاله

از آنجا که دستگاه‌های IoT مبتنی بر اینترنت هستند و شامل اطلاعات حساس و محرمانه هستند، نگرانی‌های امنیتی مطرح شده‌اند و چندین محقق در حال بررسی روش‌هایی برای بهبود امنیت در میان این نوع دستگاه‌ها هستند . شبکه تعریف‌شده توسط نرم‌افزارSDNیک تکنولوژی شبکه کامپیوتری امیدوار کننده است که یک برنامه مرکزی به نام SDN" کنترلر" را معرفی می‌کند که اجازه کنترل کلی شبکه را می‌دهد . بنابراین، استفاده از SDN یک راه‌حل واضح برای بهبود عملکرد شبکه IoT و غلبه بر کاستی‌های موجود است .در این مقاله، ما) (iیک مدل سیستم را برای استفاده ایمن از SDN با شبکه‌های IoT ارائه می‌دهیم؛

ضرورت تحقیق

استفاده از SDN یک راه‌حل واضح برای بهبود عملکرد شبکه IoT و غلبه بر کاستی‌های موجود است .در این مقاله، ما) (iیک مدل سیستم را برای استفاده ایمن از SDN با شبکه‌های IoT ارائه می‌دهیم؛ یک راه‌حل برای کاهش حملات انسان در میانه علیه IoT ارائه می‌دهد که تنها می‌تواند از HTTPاستفاده کند، که یک حمله حیاتی است که دفاع از آن دشوار است؛ پیاده‌سازی و ارزیابی سیستم ما نشان می‌دهد که روش پیشنهادی نسبت به حملات سایبری انعطاف‌پذیری بیشتری دارد . نگرانی‌های خاصی برای امنیت اینترنت اشیا) (IoTمطرح شده‌است [۱]، این دستگاه‌ها به طور منحصر به فرد قابل‌شناسایی هستند، در تجزیه و تحلیل داده‌ها و تصمیم‌گیری هوشمند هستند، و قابلیت‌های شبکه‌ای دارند که به آن‌ها اجازه اتصال به اینترنت را می‌دهد . با توجه به ماهیتIoT ، ارتباط ممکن است بدون محرمانه بودن و صحت انجام شود، در نتیجه آن را مستعد حملات می‌کند . روش‌های سنتی حفاظت از شبکه‌ها از فایروال ها و سیستم‌های پیش‌گیری از نفوذ در لبه شبکه برای جلوگیری از حمله خارجی استفاده می‌کنند . با این حال، به دلیل ویژگی‌های خاص آن‌ها، چنین مکانیزم‌های دفاعی به طور مستقیم با شبکه‌های IoT کار نمی‌کنند .

شاخه حل جاری

پیشرفت‌های اخیر در شبکه کامپیوتری، یک فن‌آوری جدید، شبکه سازی تعریف‌شده توسط نرم‌افزار)(SDNرا معرفی کرد، که اجازه می‌دهد یک برنامه مرکزی، به نام "کنترلر"SDN ، رفتار کلی شبکه را کنترل کند. این کنترل‌کننده، واکنش‌های سریع به تهدیدهای امنیتی، فیلترینگ گرانولار tra c و استقرار سیاست‌های امنیتی پویا را ممکن می‌سازد. محققان استفاده از SDN را برای ایمن‌سازی شبکه‌های کامپیوتری، مانند استفاده از کنترلر SDN و تغییر جهت ساخت یک فایروال بررسی کرده‌اند . و تعداد کمی از محققان، SDNرا با IoT مطالعه کرده‌اند .

مقیاسپذیری SDN و شبکه‌های IoT و همچنین نیاز به بررسی بسته عمیق‌در آن محیط دارند.

در مقایسه با کار ما، ما یک مدل سیستم با SDN را برای حفاظت از دستگاه‌های IoT که از HTTP استفاده می‌کنند، پیشنهاد کردیم Qin .و همکاران یک معماری SDN را برای IoT پیشنهاد کردند تا نیاز به SDN را نشان دهند که با یک مسیر تک کاره چندگانه و ناهمگن کار می‌کند تا شبکه را برای ماهیت IoT بهینه کند . با مقایسه این پیشنهاد با مدل سیستم خود، ما به هیچ تغییری در محیط شبکه IoTنیاز نداریم . طرح احراز هویت برای IoT با SDN که در آن هویت از پروتکل‌های ارتباطی مختلفی استفاده می‌کند که از طریق کنترلر SDN به یک هویت مشترک نگاشت می‌شوند. رمزگذاری هدر چالش‌های مسیر یابی را نشان داد که از طریق یک پروتکل مسیر یابی پخش با استفاده از کنترلر SDNنشان داده شد.

IoT and SDN

این بخش تعریف، کاربردها، معماری و مسائل امنیت عمومی اینترنت اشیا) (IoTرا ارائه می‌دهد . سپس مروری بر شبکه تعریف‌شده نرم‌افزار) (SDN.

با توجه به اتحادیه بین‌المللی مخابرات، AIoT یا دنیای اطلاعات (دنیای مجازی)است که قادر به شناسایی و ادغام در شبکه‌های ارتباطی هستند.با تکنولوژیIoT ، اشیا فیزیکی مشترک ممکن است به طور مجازی تعامل داشته باشند، و آن‌ها را قادر سازند تا از رویدادهایی که در فاصله دور اتفاق می‌افتند آگاه باشند یا به رویدادی که از نظر فیزیکی نمی‌تواند تشخیص دهد، پاسخ دهند .

در مقایسه با دستگاه‌های تلفن همراه شخصی، IoTمنابع محدودی از نظر قدرت پردازش، ذخیره‌سازی، و حافظه فرار دارد .بنابراین، ممکن است نیاز به اتصال به یک پلت فرم ابری یا پلت فرم فوگ برای پردازش بیشتر داده‌ها داشته باشد .

بنابراین، ممکن است نیاز به اتصال به یک پلت فرم ابری یا پلت فرم فوگ برای پردازش بیشتر داده‌ها داشته باشد .

سه مولفه اصلی توابع IoT را فعال می‌سازند:

(۱)سخت‌افزار - شبکه دستگاه‌های متصل، حسگرهای جاسازی‌شده اشیا؛

(۲)برنامه نرم‌افزاری مورد استفاده برای جمع‌آوری، ذخیره‌سازی، حمل و نقل، دستورالعمل دستگاه‌ها؛

(۳)ارتباط داده - پروتکل‌ها و فن‌آوری‌ها برای تبادل داده .

Applications of Internet of Things

IoTبخشی از زندگی روزمره ما است، از دستگاه‌های ساده‌ای مانند مانیتورهای کودک، دستبندهای بهداشتی، تلفن‌های هوشمند، بلندگوهای فعال شده با صدا، یخچال‌های هوشمند گرفته تا دستگاه‌های پیچیده‌تر مانند ماشین‌های خود - راننده و دستگاه‌های با منابع پایین از جمله شبکه‌های حسگر بدن بی‌سیم) (WBANو شبکه‌های حسگر بی‌سیم پزشکی) (MWSN .

به سادگی، دستگاه‌های متصل به اینترنت اشیا در اطراف ما هستند، شکل ۱، در خانه‌های ما، کسب و کارها، خیابان‌ها، محلات و شهرها، و حتی در بدن ما .

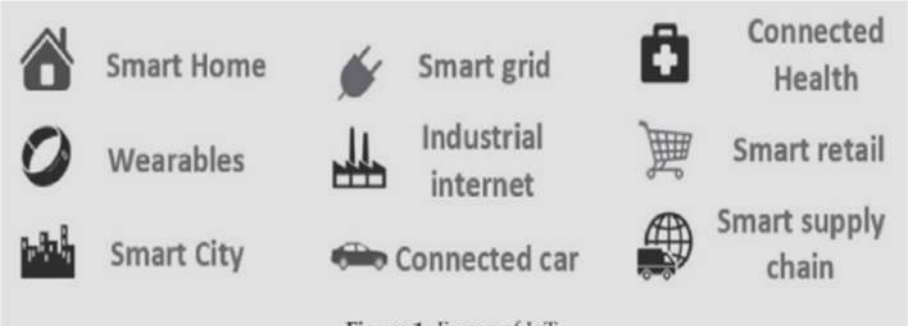

Figure 1. Forms of IoT.

با توجه به پیش‌بینی اخیر، در سال ۲۰۲۵ تعداد کل دستگاه‌های متصل در جهان به طور تقریبی ۷۵,۴۴ میلیارد خواهد بود، شکل ۲ .در حالی که شرکت‌ها در حال رقابت برای تولید دستگاه‌های IoT جدید با برنامه‌های کاربردی خلاقانه هستند، متاسفانه، در بسیاری از موارد، امنیت به عنوان یک تفکر بعدی مطرح می‌شود .شرکت‌ها ممکن است در صورت وجود از استاندارد امنیتی تاریخ دار استفاده کنند .

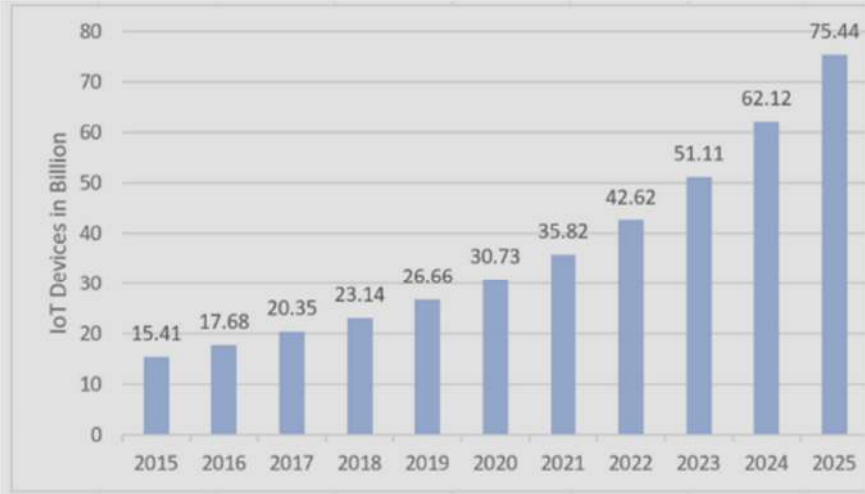

Figure 2. Internet of Things prediction from 2014 to 2025 (in billions).

Architecture of Internet of Things

هنوز هیچ معماری یا طراحی استانداردی برای یک شبکه IoT وجود ندارد .با این حال، براساس جریان داده‌ها و توابع مختلف، شبکه IoT می‌تواند به چهار لایه اصلی تقسیم شود (جدول ۱):

لایه حسگر ادراک؛

لایه حمل و نقل شبکه‌ای؛

لایه مدیریت خدمات؛

لایه واسط برنامه

Layer	Function
Application, interface layer	Presenting, user's interaction Business applications
Service, management layer	Data processing, analyzing Generating useful information
Networking, transport layer	Data transmission over wire or wireless network
Perception, sensing layer	Hardware integration Identifying, collecting data

Internet of Things Security Concerns

اکثر دستگاه‌های IoT یک طراحی ساده را به اشتراک می‌گذارند که براساس این فرض است که آن‌ها می‌توانند به سرعت و به سادگی کار کنند، یا اینکه دستگاه‌های روزمره می‌توانند با افزودن اتصال اینترنت به IoT تبدیل شوند .فشارهای انتشار سریع یک محصول گاهی اوقات می‌تواند منجر به نادیده گرفتن جنبه‌های غیرقابل‌مشاهده مانند امنیت و قابلیت اطمینان شود. دستگاه‌های IoT اخیر بر زیرساخت‌های ابری برای ارتباطات تکیه می‌کنند، که در حال حاضر مسائل امنیتی را شناخته‌اند، و ممکن است باعث شوند که دستگاه‌های IoT به اهداف آسانی تبدیل شوند .اکثر دستگاه‌های اینترنت

اشیا بر روی توسعه جدید، پلتفرم‌های نوظهوری که ممکن است آسیب‌پذیری‌های امنیتی داشته باشند، اجرا می‌شوند .از این بدتر، بسیاری از دستگاه‌های اینترنت اشیا توانایی به روز رسانی سخت‌افزار و نرم‌افزار خود را ندارند، و آن‌ها را به شدت آسیب‌پذیر کرده و در معرض اکسپلویت ها و حملات آینده قرار می‌دهند.

از این بدتر، بسیاری از دستگاه‌های اینترنت اشیا توانایی به روز رسانی سخت‌افزار و نرم‌افزار خود را ندارند، و آن‌ها را به شدت آسیب‌پذیر کرده و در معرض اکسپلویت ها و حملات آینده قرار می‌دهند .

حملات به IoT را می توان به دو دسته اصلی تقسیم کرد: حملات به لایه‌های معماری، و حملات به فازه‌ای داده.

System Model

زمینه IoT امروزه یکی از سریع‌ترین تکنولوژی‌های در حال رشد است و دستگاه‌های IoT جدید هر روز معرفی می‌شوند .این دستگاه‌ها هوشمند هستند و به اینترنت متصل هستند .با توجه به این نوع محیط پویا، شبکه‌های سنتی بهترین گزینه برای برآورده کردن الزامات IoT نیستند .نیاز به یک زیرساخت شبکه پویاتر و امن برای پشتیبانی از عملیات IoT وجود دارد .همانطور که قبلا توضیح داده شد، SDNیک فن‌آوری جدید است که اجازه کنترل کامل رفتار کلی شبکه و جلوگیری از اضافه‌بار شبکه را می‌دهد .علاوه بر این، کنترلر SDN ابزارهای اشکال‌زدایی مفیدی فراهم می‌کند که می‌تواند توسط محیط IoT برای افزایش امنیت مورد استفاده قرار گیرد.

شکل ۳ IoT را با ساختار SDN نشان می‌دهد، کنترلر SDN امکان تفکیک شبکه به زیرشبکه های مجزا را فراهم می‌کند [۳۰] .علاوه بر این، کنترلر SDN با برنامه IoT تعامل دارد .

با استفاده از یک رابط برنامه‌نویسی برنامه کاربردی خاصAPI ، که به عنوان "شمال "API شناخته می‌شود .سپس شبکه tra c را تجزیه و تحلیل کرده و اقداماتی را براساس قوانین پیکربندی شده انجام می‌دهد .از سوی دیگر، کنترلر از API دیگری) که با عنوان API" جنوب متصل" شناخته می‌شود(برای ارتباط با سوئیچ‌های شبکه براساس قوانین پیکربندی شده استفاده می‌کند [۳۰] .به طور کلی، ادغامSDN - IoT ، عملیات IoT و امنیت را افزایش می‌دهد زیرا امکان کنترل کامل و از راه دور پیکربندی شبکه را بدون تعامل مستقیم با دستگاه‌های IoT فراهم می‌کند .

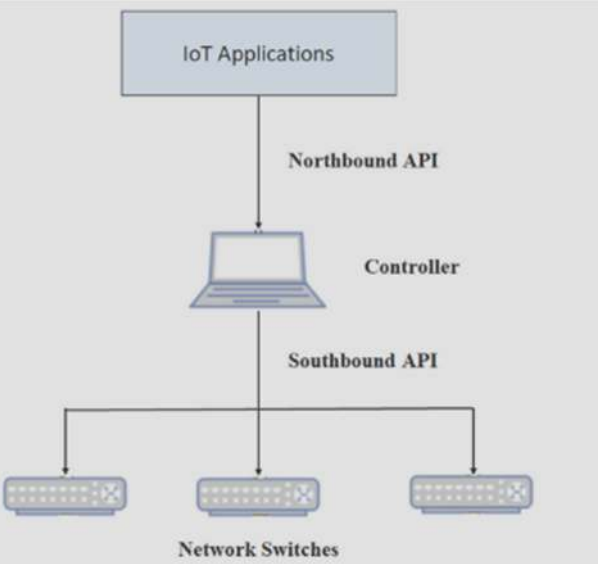

Figure 3. SDN and IoT Structure.

ارزیابی و بررسی

در این مقاله ما به مطالعه ی **بهبود امنیت اینترنت اشیا پرداختیم البته با توجه به SDNو نگرانی هایی که بابت دستگاههای هوشمند بود را مورد بحث قرار دادیم.**

و همچنین ه این نتیجه رسیدیم که ستفاده از SDN یک راه‌حل واضح برای بهبود عملکرد شبکه IoT و غلبه بر کاستی‌های موجود است.و همچنین به این نتیجه رسیدیم که با توجه به ماهیتIoT ، ارتباط ممکن است بدون محرمانه بودن و صحت انجام شود، در نتیجه آن را مستعد حملات می‌کند.

جمع بندی

در چند سال گذشته، اینترنت اشیا) (IoTبه بخشی جدایی‌ناپذیر از زندگی روزمره ما تبدیل شده‌است . تقاضای قابل‌توجهی برای عرضه دستگاه‌های هوشمندتر به جهان وجود دارد .همانطور که دستگاه‌های بیشتری به اینترنت متصل می‌شوند، تقاضای فزاینده‌ای برای امنیت اطلاعات وجود خواهد داشت زیرا اطلاعات حساس را می توان متوقف کرد .ما ادغام SDN با IoT را به منظور افزایش امنیت سیستم مورد بررسی قرار دادیم .سپس SDN را به عنوان یک تکنولوژی شبکه جدید و ترکیب ساختار IoT با SDN بررسی می‌کنیم .با پیاده‌سازی و آزمایش، ما نشان دادیم که حفاظت از دستگاه‌های IoT که تنها به دلیل محدودیت‌های منابع بدون اصلاح دستگاه می‌توانند از HTTP استفاده کنند، امکان پذیر است .

در