

۲۰۹۱۳۲۸

توانمندسازی معماری و امنیت

اینترنت اشیاء مبتنی بر SDN

مؤلف:

محمد مهدیان

فارغ التحصیل دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

مدرسیناسی اسد رشته

مهندسی فن آوری اطلاعات گرایش شبکه‌های کامپیوتری



**NAGHOOS
PUBLICATION**

۱۳۹۸

سرشناسه	: مهدیان، محمد، ۱۳۶۴-
عنوان و نام پدیدآور	: توانمند سازی معماری و امنیت اینترنت اشیا مبتنی بر SDN/ مولف محمد مهدیان
مشخصات نشر	: تهران: ناخوس، ۱۳۹۸.
مشخصات ظاهری	: ۷۲ص. : جدول بنمودار
شابک	: 978-600-473-259-8
وضعیت فهرست نویسی	: فیا
یادداشت	: کتابنامه: ص. ۶۱.
موضوع	: اینترنت اشیا
موضوع	: Internet of things
رده بندی کنگره	: ۵۱۰۵/۸۸۵۷
رده بندی دیویی	: ۰۰۴/۶۷۸
شماره ثبت کتابخانه ملی	: ۶۰۷۴۸۰۶



**NAGHOOS
PUBLICATION**

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoos-res.ir

انتشارات ناخوس

چاپ اول

در نوبت چاپ اول از دستگاه چاپ
به کار گرفته شده است

کلیه حقوق برای ناخوس محفوظ است.
تکثیر تمامی یا قسمتی از این اثر به
صورت حروفچینی یا چاپ مجدد، چاپ
افست، پلی کپی، فتوکپی و انواع دیگر
چاپ ممنوع است و پیگرد قانونی دارد.

نام کتاب	: توانمند سازی معماری و امنیت اینترنت اشیا مبتنی بر SDN
ناشر	: انتشارات ناخوس
مولف	: محمد مهدیان
چاپ اول	: ۱۳۹۸
تیراژ	: ۵۰۰ جلد
چاپ و صحافی	: برجسته
ناظر چاپ	: یاسمن تجملی محدث
قیمت	: ۱۵۰۰۰۰ ریال
شابک	: ۹۷۸-۶۰۰-۴۷۳-۲۵۹-۸
ISBN	: 978-600-473-259-8

انتشارات ناخوس

بلوار کشاورز- خیابان ۱۶ آذر- کوچه پارسی پلاک ۱۰

تلفاکس: ۶۶۳۷۸۹۵۸-۶۶۳۷۸۹۵۷

۱- مقدمه

گسترده‌ی اینترنت اشیا یک سری نیازمندی پیچیده جدیدی را به شمای networking و internetworking در شبکه‌های امروزی و شبکه‌های آینده و مخصوصاً اینترنت تحمیل کرده است. چون هر شی (object) در اینترنت اشیا (شامل دیوایس و یا چیزها) باید طراحی یا پیکره‌بندی شوند تا خصوصیات شی گرایی (objective) را ایجاد کنند. اینترنت اشیا، اشیا چندین شبکه ناهمگون (Heterogeneous) را با اتصالات داخلی متصل و ترکیب می‌کنند.

مکان‌ها، امنیتی سنتی همانند فایروال‌ها، سیستم‌های پیشگیری و تشخیص نفوذ در لبه‌های اینترنت (Internet Edge) وجود دارند که از آن مکانیزم‌ها برای حفاظت از شبکه در برابر حمله‌های خارجی استفاده می‌شود. چنین مکانیزم‌هایی برای مدت زیادی برای امنیت نسل بعدی اینترنت کافی نخواهند بود. معماری بدون محدوده‌ی IoT نگرانی‌های بیشتری را در مورد کنترل دسترسی اینترنتی و اعتبارات شی ریم‌افزاری برانگیخت.

SDN که یک الگو و نمونه عالی از شبکه‌های هوشمند جدید است که فرصتی را فراهم آورد تا مسائل مرتبط با IoT را حل کند. با کار کردن شبکه‌های SDN مدیریت و پیکره‌بندی به صورت چشم‌گیری می‌تواند آسان گردد. از دید IoT در نظر گرفتن مشخصات SDN ما را به این سمت سوق می‌دهد که چطور SDN می‌تواند استفاده شود؟ تا ناهمگونی را در شبکه‌ها و انتقال داده حفظ کند و یک شمای cooperation به وسیله یکپارچگی در داخل شبکه ارائه کند و همچنین یک راه‌حل لایه کنترلی جدید بالاتر (کنترلر IoT) که کنترل بر SDN فعل و انفعالات انجام می‌دهند ایجاد کند. استقبال گسترده صنعتی برای SDN نشان می‌دهد که SDN می‌تواند ارتباطات انبوهی را به همراه IoT، برقرار (Establish) کند.

در این گزارش فعالیت‌های اصلی ما به شرح زیر است:

- معماری IoT و سپس معماری شبکه‌های SDN و معماری SDN برای شبکه‌های Ad-hoc بررسی می‌کنیم. در این موقع یک مدل مفهومی برای معماری IoT مبتنی بر SDN بررسی می‌کنیم.
- شبکه‌های امروزی باید هوشمندی، قدرت، امنیت، بازدهی، قابلیت اطمینان و قابلیت گسترش بیشتری در مواجهه با نیازمندی‌های متنوع و دینامیکی داشته باشند. SDN و NFV دو فن‌آوری امیدوارکننده برای برطرف کردن چالش‌های آدرس دهی و وسیله‌ای برای معماری IoT در era ابری است.

- در اینجا یک معماری IoT مبنی بر SDN برای سرویس‌های IoT افقی پیشنهاد شده است و بر اساس معماری SDN مدلی امنیتی را برای IoT ارائه می‌کنیم.

- یک شبکه Black را معرفی می‌کنیم تا حمله آنالیز ترافیک شبکه و حمله جمع‌آوری داده‌ها را تقلیل دهیم. ما Black SDN را برای IoT در توپولوژی ستاره و مش در نظر می‌گیریم و نتایج آن را ارزیابی می‌کنیم.

در پایان، دست شما خواننده گرامی را به عنوان دوستی جدید می‌فشارم و به این دوستی افتخار خواهد کرد و مایلیم نظرات همه بزرگواران را که در این زمینه صاحب اندیشه و رأی هستند، بدانم:

اصفهان، زمستان ۱۳۹۸، محمد مهدیان

(mahdian260@gmail.com)

(mmahdian@aut.ac.ir)

فهرست مطالب

۱- اینترنت اشیاء.....	۱
۱-۲- ساختار سه لایه‌ای IoT.....	۲
۲-۲- وضعیت کنونی اینترنت اشیاء.....	۴
۲- معماری شبکه‌های SDN.....	۵
۱-۳- مدل سه لایه‌ای معماری SDN.....	۸
۲-۳- چهار کامپوننت در SDN در مقایسه با شبکه سنتی.....	۹
۳-۳- وجود نقطه تکیه (Single point of failure).....	۱۰
۴-۳- همگام‌سازی پدین کنترل.....	۱۱
۴- معماری SDN برای شبکه‌های Ad-hoc.....	۱۲
۱-۴- محتویات معماری Ad-hoc مبتنی بر SDN.....	۱۲
۲-۴- Control Plane در Ad-hoc توزیع شده.....	۱۴
۵- معماری IoT مبتنی بر SDN.....	۱۵
۱-۵- معماری پیشنهادی برای IoT مبتنی بر SDN.....	۱۶
۲-۵- دامنه‌ی SDN.....	۱۷
۳-۵- تعاملات دامنه‌ی SDN.....	۱۸
۶- یک معماری مبتنی بر SDN برای سرویس‌های IoT افقی.....	۱۹
۱-۶- انگیزه طراحی پلتفرم‌های IoT افقی.....	۱۹
۲-۶- اصول طراحی برای توسعه معماری IoT افقی.....	۲۱
۳-۶- پیاده‌سازی معماری IoT افقی مبتنی بر SDN.....	۲۲
۴-۶- پیاده‌سازی.....	۲۶
۵-۶- ارزیابی معماری IoT افقی مبتنی بر SDN.....	۲۷
۷- چارچوب IoT مبتنی بر SDN با پیاده‌سازی NFV.....	۳۳
۸- معماری امنیتی برای IoT مبتنی بر SDN.....	۳۵
۱-۸- مرور کلی امنیت شبکه‌های IoT.....	۳۶
۱-۱-۸- بعضی از چالش‌های امنیتی IoT.....	۳۷

۳۸	۲-۱-۸- معرفی و مقدمه امنیتی IoT
۳۹	۲-۱-۸- امنیت IEEE 802.15.4
۴۰	۲-۸- بررسی امنیت در SDN
۴۱	۱-۲-۸- وجود نقطه‌ی تکی شکست (Single point of failure)
۴۲	۲-۲-۸- همگام‌سازی چندین کنترلر
۴۲	۳-۸- پیشنهاد چارچوب و راه‌حل امنیتی برای IoT مبتنی بر SDN
۴۳	۴-۸- مکانیسم‌های امنیتی برای IoT مبتنی بر SDN
۴۵	۵-۸- تعریف Black SDN برای اینترنت اشیاء
۴۶	۱-۵-۸- شبکه Black برای IoT
۴۶	۱-۱-۵-۸- Black IEEE 802.15.4
۴۸	۲-۱-۵-۸- شبیه‌سازی رزینک Broadcast شبکه Black
۵۰	۳-۱-۵-۸- شبیه‌سازی نتایج و "آز"رها
۵۱	۴-۱-۵-۸- کنترلر SDN برای Trustworthy Party
۵۲	۲-۵-۸- Black SDN برای اینترنت اشیاء
۵۷	۳-۵-۸- ارزیابی و آنالیز
۶۱	۹-مراجع