وزارت ارتباطات و فناوری اطلاعات
پژوهشگاه ارتباطات و فناوری اطلاعات
(مرکز تحقیقات مخابرات ایران)
ITRC

عنوان: الزامات و رویکردهای امنیتی در حوزه اینترنت اشیاء

پروژه: تدوین نقشه راه اینترنت اشیاء

ارائه‌دهندگان: نسرین تاج – افسانه معدنی

تاریخ: بهار ۱۳۹۶

توجه

- کارگاه ارائه شده تنها بخشی از فعالیت های انجام شده در پروژه تدوین نقشه راه اینترنت اشیاء در قسمت امنیت می باشد.
- هدف نهایی کارگاه، با تاکید بر مباحث فنی، ارائه معماری امن اینترنت اشیاء و پیشنهاد راهکارهایی جهت تامین امنیت آن می‌باشد.

سوالات مطرح در زمینه تامین و حفاظت اکوسیستم اینترنت اشیاء

- ✓ دغدغه های اصلی امنیت در اینترنت اشیاء چیست؟
- ✓ معیارهای ممیزی امنیت اینترنت اشیاء چیست؟
- ✓ الزامات امنیتی متناسب با تحولات بازار و سرویس (طراحی، تولید و بکارگیری) چیست؟
- ✓ وضعیت اینترنت اشیاء از نظرتامین امنیت چگونه باید باشد؟
- ✓ اصول امنیتی ای که باید توسط توسعه‌دهندگان اینترنت اشیاء رعایت شود چیست؟
- ✓ نیازمندیهای اصلی تامین امنیت اینترنت اشیاء چیست؟

سرفصل مطالب

بخش اول

- ✓ معرفی مراکز و منابع مورد استفاده
- ✓ تشریح نمونه معماری‌های منتخب و راهکارهای پیاده سازی IoT
  - ✓ معماری های ارائه شده در استانداردها
  - ✓ معماری های ارائه شده در پروژه های معتبر
  - ✓ راهکارها و Best practice ها

بخش دوم

- ✓ بررسی و معرفی تهدیدات و حملات
- ✓ بررسی و معرفی مکانیزم‌های پیشگیری و حفاظتی الزامی
- ✓ طرح معماری امن پیشنهادی

بخش اول

- ✓ معرفی مراکز و منابع مورد استفاده
- ✓ تشریح نمونه معماری‌های منتخب و راهکارهای پیاده سازی IoT
  - ✓ معماری های ارائه شده در استانداردها
  - ✓ معماری های ارائه شده در پروژه های معتبر
  - ✓ راهکارها و Best practice ها

مقدمه

- ایده اتصال در هر زمان، در هر نقطه از جهان و توسط هر شیء توسط ITU-T جهت تعریف اینترنت اشیاء تدوین شده است.
  - (Any Thing, Any Time, Any Place)

- آنچه برای همه‌گیر شدن این اکوسیستم نیاز است تعامل بین منابع ارتباطی و سرویس‌دهی کنونی، به همراه ایجاد و گسترش منابع مورد نیاز آینده می‌باشد.

مقدمه

این شبکه ارتباطی گسترده، جهت کنترل، مدیریت و سرویس‌دهی، از منابع موجود نظیر اینترنت، سرویس‌های ارائه شده مبتنی بر ابر، دیتاسنترها، فناوری های انتقال داده نظیر 5G و بسیاری از برنامه‌ها و ابزار کاربردی استفاده می‌نماید.

تعاریف و پیشنیازها

IoT ارکان اصلی رشد برای راه‌حل‌های آینده

هر راه‌حل باید حاوی ۵ رکن اصلی زیر باشد:

۱- پلتفرم
۲- فناوری‌های دسترسی
۳- ذخیره‌سازی و پردازش داده
۴- تجزیه و تحلیل داده
۵- امنیت

معرفی مراکز و منابع مورد استفاده

معرفی مراکز معتبر پژوهشی در زمینه اینترنت اشیاء

برخی مؤسسات و مراکز تحقیقاتی

- **IERC** : مرکز تحقیقاتی بین‌المللی اتحادیه اروپا

اهداف مهم:

۱- ایجاد یک چارچوب همکاری و چشم انداز پژوهش برای فعالیت IoT
۲- تعریف یک استراتژی بین المللی برای IoT و ایجاد نوآوری

موضوعات تحقیقاتی مهم:

۱- روش ها و مدل‌های معماری IoT
۲- مسائل مربوط به حریم خصوصی و امنیت در IoT

IERC
European Research Cluster
on the Internet of Things

IERC: IoT European Research Cluster

معرفی مراکز و منابع مورد استفاده

برخی مؤسسات و مراکز تحقیقاتی

- **OWASP** : انجمن امنیت کاربرد وب

مهمترین هدف:

۱- ایجاد امنیت در تجارت، توسعه، برنامه‌های کاربردی و اهداف سازمان‌ها و ادارات

موضوعات تحقیقاتی مهم:

۱- بررسی و رفع ۱۰ مشکل امنیتی متداول در IoT

- رابط کاربری وب ناامن
- صدور مجوز و احراز هویت ناامن
- خدمات شبکه ناامن
- عدم استفاده از رمزنگاری برای انتقال داده‌ها
- نگرانی‌های حریم خصوصی
- رابط کاربری ابری ناامن
- رابط کاربری همراه ناامن
- توانایی پیکربندی امنیتی ناکافی
- نرم‌افزار / سخت‌افزار ناامن
- امنیت فیزیکی ضعیف

معرفی مراکز و منابع مورد استفاده

برخی مؤسسات و مراکز تحقیقاتی

- **Council** : گروه پیش‌بینی، شتاب و مشاوره در IoT در سطح بین‌المللی برای اتحادیه اروپا

دارای ۲۳۵ عضو از سراسر جهان

اهداف مهم:

۱- نیروی محرک IoT در اتحادیه اروپا
۲- تشکیل نیروی متخصص در زمینه IoT به همراه تعریف وظایف و ساختار

نیاز به تشکیل گروهی مشابه با این گروه در کشور ما احساس می‌شود

معرفی مراکز و منابع مورد استفاده

دانشگاه‌ها

استنفرد (آمریکا): پروژه SITP به همراه برکلی و میشیگان

جورجیا (آمریکا): توسعه و گسترش پتانسیل‌ها و توانایی‌های IoT

MIT (آمریکا): استانداردهای مربوط به RFIDها و حسگرها

برایتون (انگلیس): مخابرات ناهمگون و محاسبات ابری در IoT،
عملیات کم توان در انجام محاسبات و الکترونیک
پوشیدنی‌های هوشمند، امنیت پویا برای اینترنت اشیاء

معرفی مراکز و منابع مورد استفاده

آزمایشگاه‌ها

آزمایشگاه اشیاء مایکروسافت (IoT): یک پلتفرم قابل انعطاف برای تحقیقات تجربی

آزمایشگاه دانشگاه ویسکانسین: کار روی اکثر زمینه‌های مخابراتی و امنیتی IoT

آزمایشگاه IoT اتحادیه اروپا: تحقیقات روی پتانسیل‌های منابع جمعیتی (Crowdsourcing)

برای توسعه زیر ساخت IoT

آزمایشگاه Auto-ID در دانشگاه MIT: هویت‌یابی فرکانس - رادیویی شبکه شده

معرفی مراکز و منابع مورد استفاده

اینتل

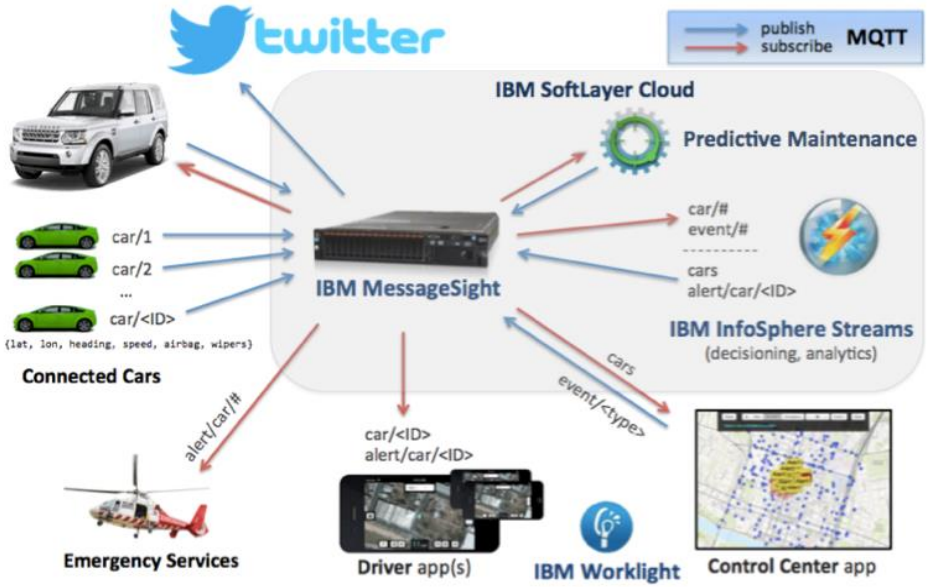
درگاه اینتل:

- اتصال بی‌درز به دستگاه‌های صنعتی
- امن سازی جریان اطلاعات بین این دستگاه‌ها و ابر

معرفی مراکز و منابع مورد استفاده

IBM

- مشارکت در پروژه‌های مختلف در زمینه اینترنت اشیاء
- نیروی تحقیق و توسعه X: شناسایی ریسک‌ها و چالش‌های امنیتی
- پروژه MessageSight برای IoT و محیط موبایل

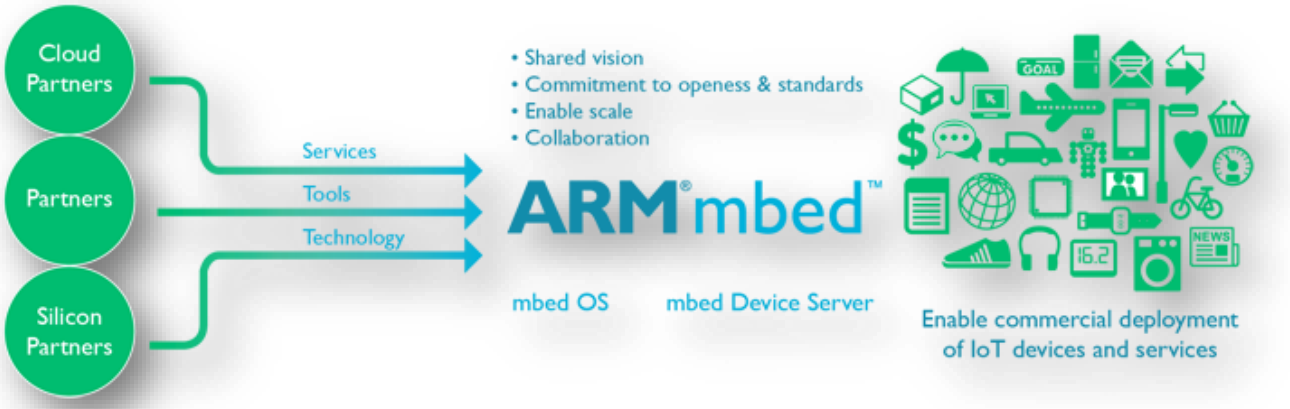


معرفی مراکز و منابع مورد استفاده

ARM (پروژه mbed)

ایجاد یک اتصال تجاری و سازگار میان دستگاه‌های IoT، با مزایای زیر :

- ارائه یک سیستم عامل مشترک برای دستگاه‌های IoT
- امکان طراحی‌ها با تضمین آینده به وسیله پشتیبانی از تمام استانداردهای کلیدی باز برای اتصال و مدیریت دستگاه
- امکان ارائه دستگاه‌های امن و قابل بروز رسانی در لبه قابلیت‌های پردازشی و تابعی
- پاسخ به مسأله دشوار مصرف توان به وسیله ایجاد مدیریت توان اتوماتیک
- ایجاد ابزار توسعه بر اساس ابر که ایجاد محصول را سرعت می‌بخشد



معرفی مراکز و منابع مورد استفاده

زمینه‌های تحقیقاتی مورد نیاز برای امنیت

۱- روش‌ها و ابزارهای آگاهی از شرایط سایبری جهت کنترل و نظارت
۲- شناسایی کلی حملات ممکن و روش‌های مقابله با آن‌ها، نظیر:

۱- Skimming: خواندن داده‌ها بدون مشخص بودن دانش Tag یا دارنده آن
۲- استراق سمع (Eavesdropping یا Sniffing؛ یا مرد در میانه نیز اتلاق می‌شود)
۳- Data Tampering: پاک کردن بدون مجوز داده‌ها برای تخریب دستگاه یا تغییر اطلاعات آن
۴- Spoofing: کپی کردن داده‌های دستگاه و انتقال آن به گیرنده برای جعل کردن آن
۵- Cloning: کپی کردن داده‌های یک دستگاه در دیگری
۶- کد بدخواه (Malicious Code): اضافه کردن یک کد اجرایی (مثل ویروس) برای تخریب سیستم
۷- رد دسترسی یا سرویس (Denial of Access/Service)
۸- کشتن (Killing): تخریب فیزیکی یا الکترونیکی یک دستگاه
۹- اختلال (Jamming): استفاده از دستگاه‌های الکترونیکی که سبب تخریب توابع گیرنده بشود.
۱۰- سپر گذاری (Shielding): استفاده از ابزارهای مکانیکی برای جلوگیری کردن از خواندن یک Tag یا دستگاه

معرفی مراکز و منابع مورد استفاده

زمینه‌های تحقیقاتی مورد نیاز برای اعتماد

۱- زیرساخت کلید عمومی (PKI) سبک
۲- سیستم‌های مدیریت کلید سبک
۳- کیفیت اطلاعات (QoI)
۴- سیستم‌های غیرمرکزی و خودپیکربند
۵- روش‌های جدید ارزیابی اعتماد در مردم
۶- کنترل دسترسی

زمینه‌های تحقیقاتی مورد نیاز برای حریم خصوصی

۱- رمزنگاری هومومورفیک و قابل جستجو
۲- کمینه‌سازی داده، شناسایی، احراز اصالت و گمنامی
۳- حفظ حریم خصوصی مکانی
۴- جلوگیری از استنتاج اطلاعات شخص
۵- نگهداری محلی اطلاعات تا حد ممکن
۶- استفاده از هویت‌های فرعی و نام مستعار



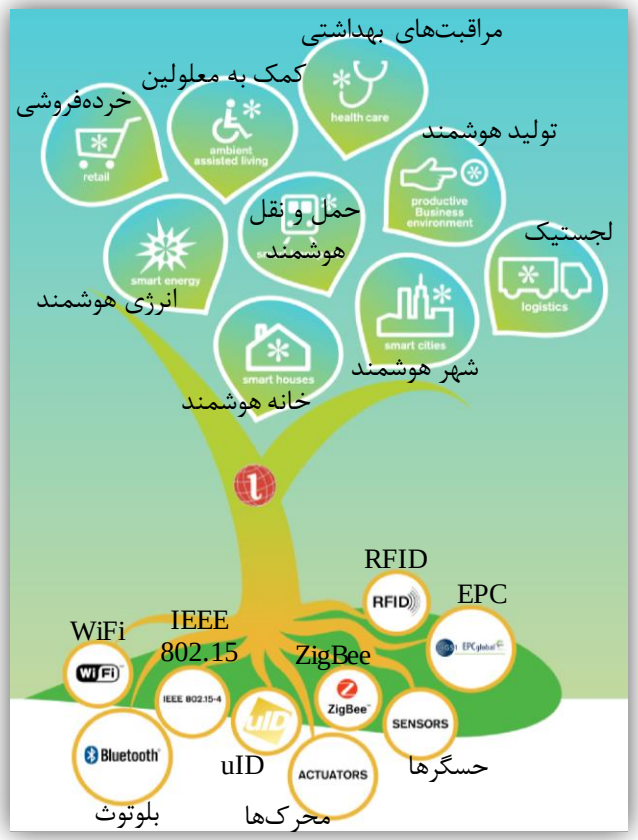

معرفی مراکز و منابع مورد استفاده

ویژگی‌های مشترک راه‌حل‌های امنیتی پیشنهادی

۱- پیشنهاد راه‌حل‌های سبک برای پشتیبانی از دستگاه‌های با محدودیت منابع
۲- مقیاس‌پذیری راه‌حل به میلیاردها دستگاه یا تراکنش
۳- پشتیبانی از ناهمگونی و چندگانگی دستگاه‌ها و پلتفرم‌ها
۴- پیشنهاد راه‌حل‌های قابل استفاده به طور بی‌درز (بدون نیاز به اطلاع کاربر از لایه‌های زیرین)

معماری‌های امنیتی مطرح شده در اینترنت اشیاء

معماری ARM

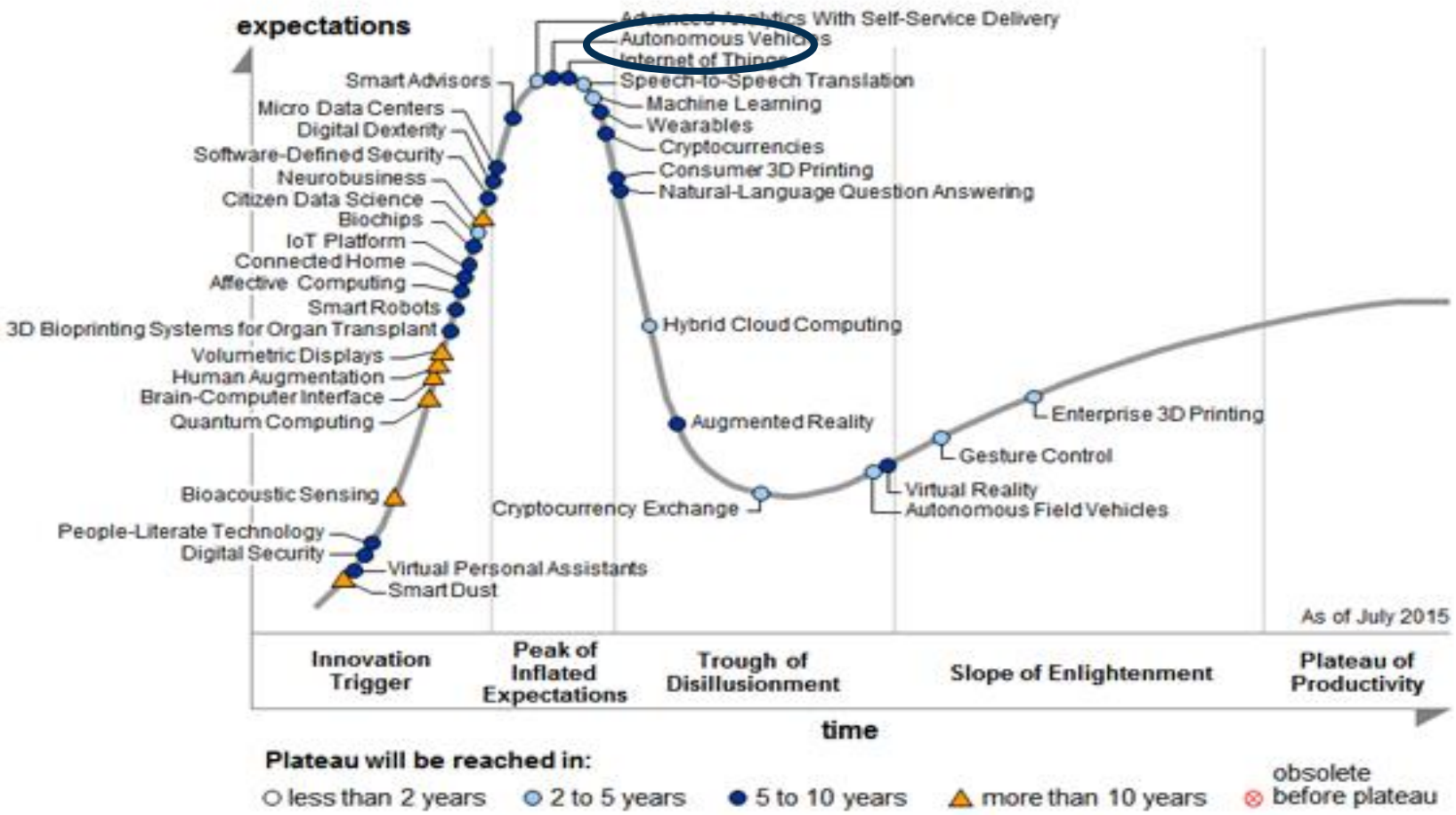


فواید استفاده از ARM:

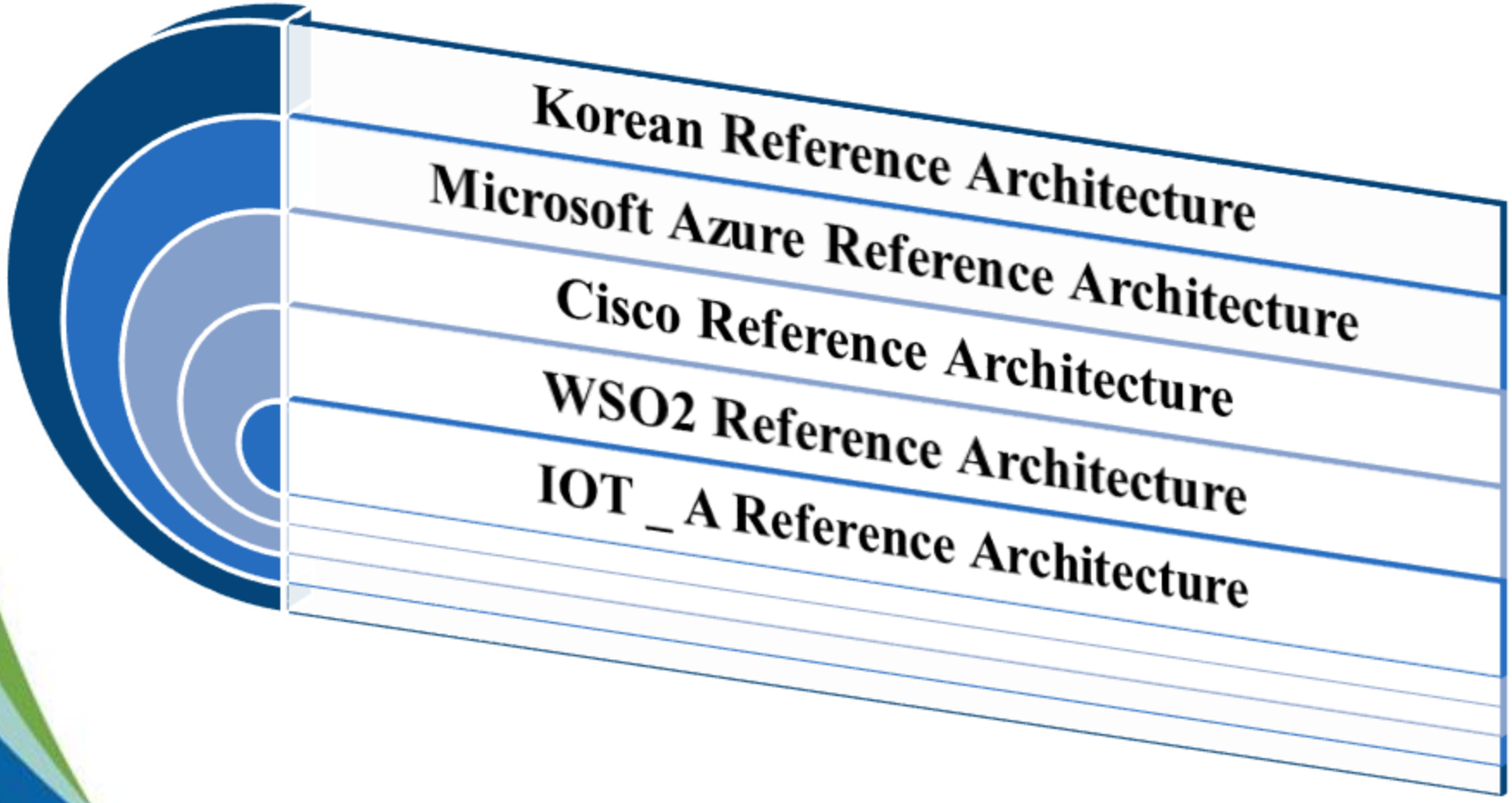
۱- کمک‌های شناختی
۲- مدل مرجع به عنوان زمین مشترک
۳- ایجاد معماری‌ها
۴- شناسایی تفاوت‌ها
۵- محک زدن

ARM: Architectural Reference Model

جایگاه IoT در نمودار hype



تشریح نمونه معماری‌های منتخب و راهکارهای پیاده سازی IoT



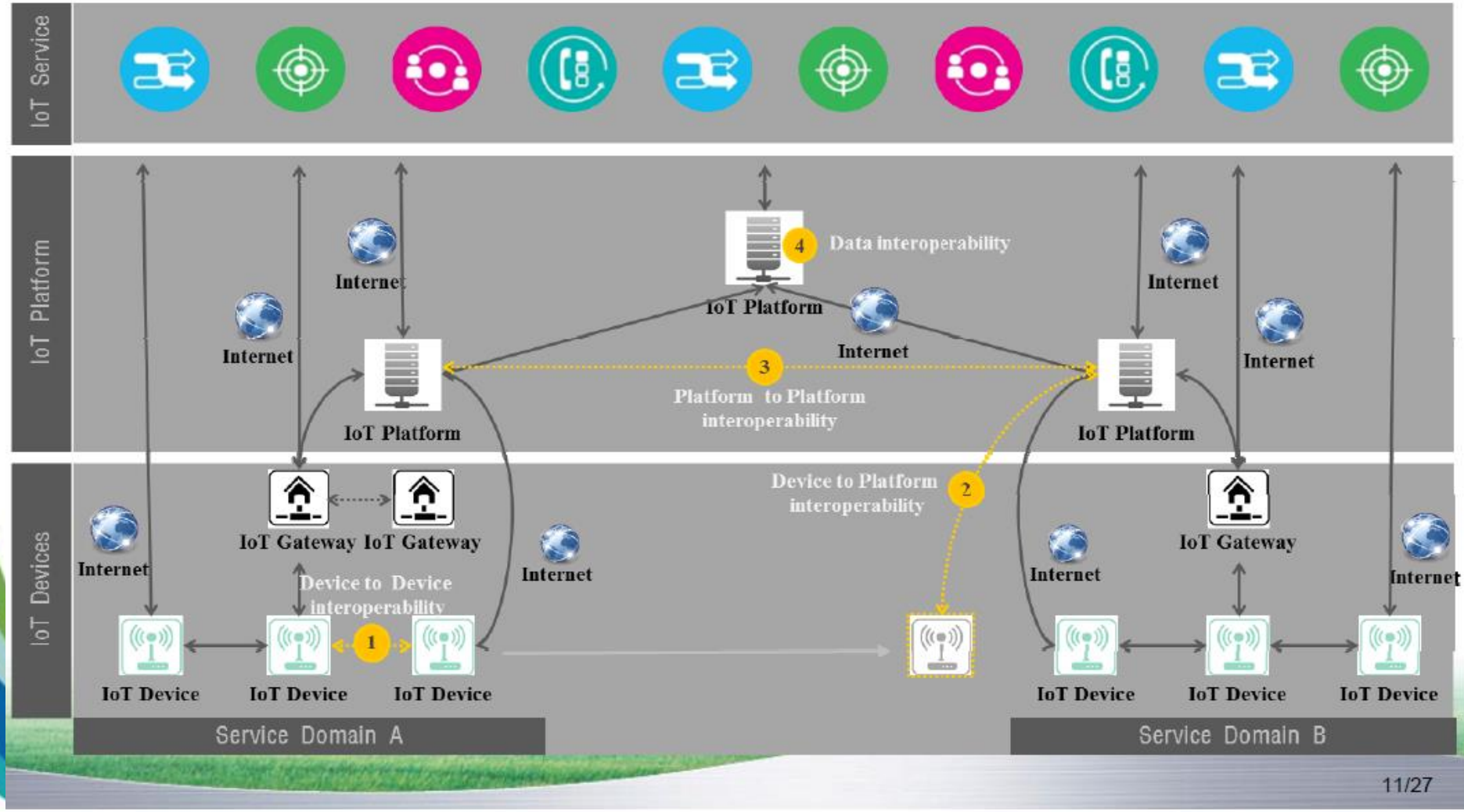
نمونه معماری‌های بررسی شده

- ✓ **معماری Korean**: ارائه معماری سه‌لایه (تجهیز، پلتفرم، سرویس) و معماری کارکردی به همراه توابع مدیریت شبکه، توابع ارتباطی، مدیریت منابع و سرویس، تحلیل داده، امنیت و حریم خصوصی با تعامل بین پلتفرم‌ها، یا تجهیز و پلتفرم،
- ✓ **معماری Azure**: تقسیم امنیت (امنیت تجهیز، امنیت ارتباطات، امنیت پلتفرم)، تاکید بر پلتفرم چند اجاره‌ای، ایزوله کردن زیرساخت کاربران در یک ابر عمومی برای حفاظت از داده‌های کاربران، احراز هویت سنسور، سیستم کسب و کاری برای تحلیل فرآیندهای B2B,B2C
- ✓ **معماری Cisco**: معماری هفت‌لایه، ارایه یک مدل امنیتی با استفاده از ارتباط cross امنیت با لایه‌های شبکه‌ای، امنیت برای هر پردازش در تمام لایه‌ها، مدیریت شناسه، احراز هویت، ذخیره سازی امن، مقابله با نفوذ و نشت داده، رمزنگاری
- ✓ **معماری WSO2**: معماری سه لایه‌ای(تجهیزات، سکو و سرویس)، تاکید بر لایه امنیت تجهیزات (سنسور) به دلیل احتمال نقض حریم خصوصی کاربران، توجه به ریسک، مدیریت شناسه مبتنی بر بلیط، احراز هویت و کنترل دسترسی

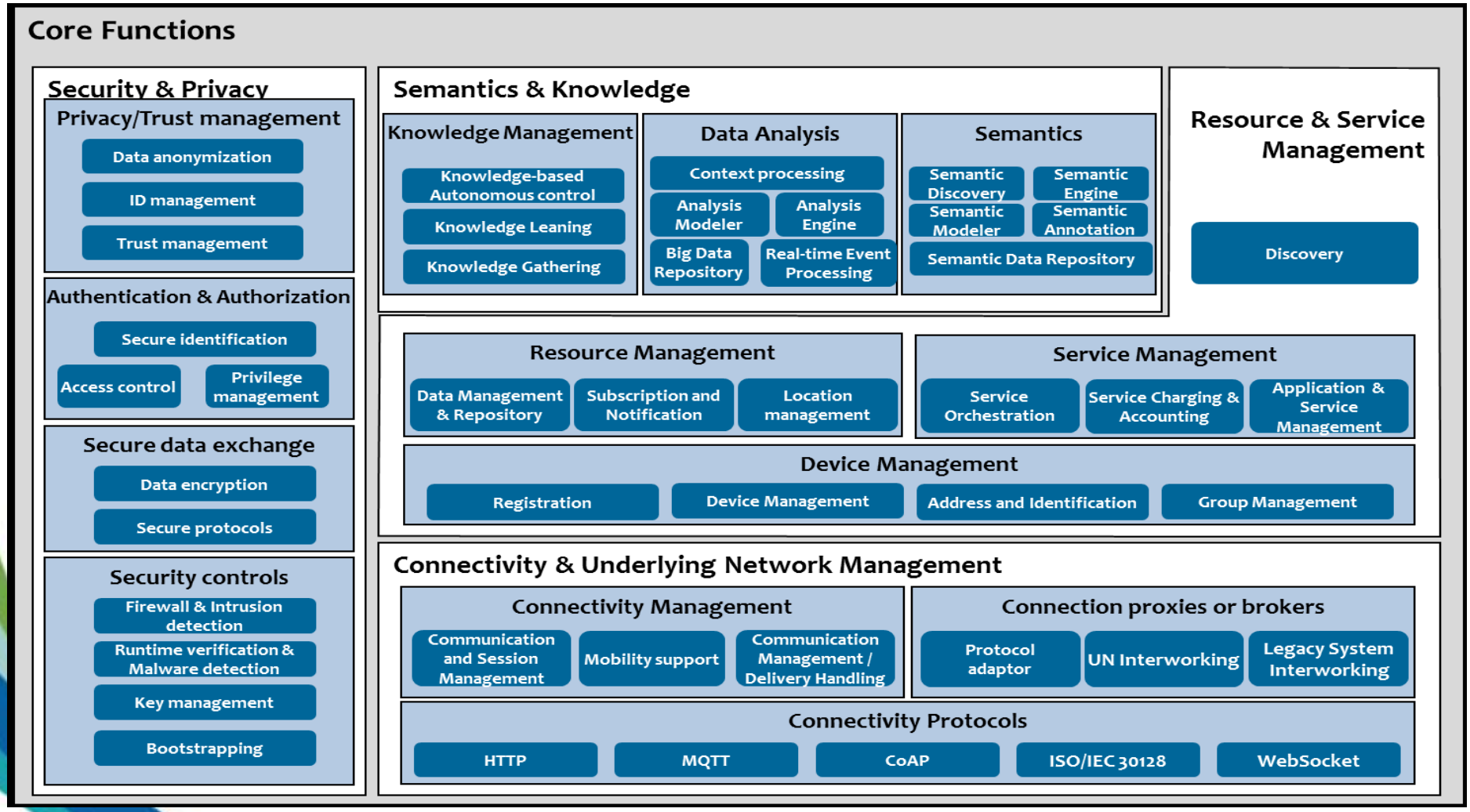
معماری Korean

- در این معماری، سه لایه تجهیزات، سکو و در انتها سرویس دیده می‌شود.
- لایه تجهیزات، تمام سنسورهای مربوط به اینترنت اشیاء می‌باشد که با این مفهوم به جمع‌آوری داده و اطلاعات از فضا پرداخته و آن را به سمت درگاه IoT ارسال می‌نماید.
- لایه سکو، تمام اطلاعات دریافتی از درگاه را در بستر اینترنت جهت محاسبه و تحلیل ارسال می‌نماید و متناسب با هر سرویس این تحلیل‌ها نهایی می‌شود.
- در لایه سرویس انواع برنامه های کاربردی و کاربردهای مختلف پیاده‌سازی می‌گردد.
- در مجموع در این معماری، تعامل بین سکوها نیز درنظر گرفته شده است تا در صورت نیاز بتوان از انتقال اطلاعات و سرویس‌ها بین دو سکو استفاده نمود.

معماری Korean

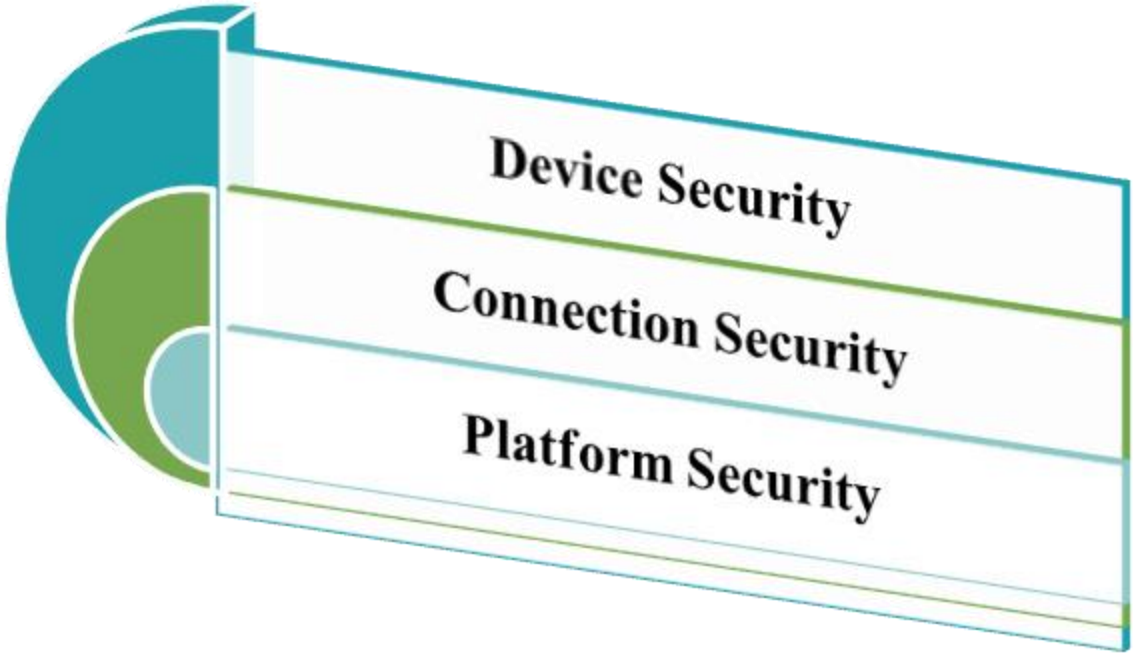


معماری Korean



معماری Microsoft Azure

- معماری Azure: تقسیم امنیت (امنیت تجهیز، امنیت ارتباطات، امنیت پلتفرم)، تاکید بر پلتفرم چند اجاره‌ای، ایزوله کردن زیرساخت کاربران در یک ابر عمومی برای حفاظت از داده‌های کاربران، احراز هویت سنسور، سیستم کسب و کاری برای تحلیل فرآیندهای B2B,B2C

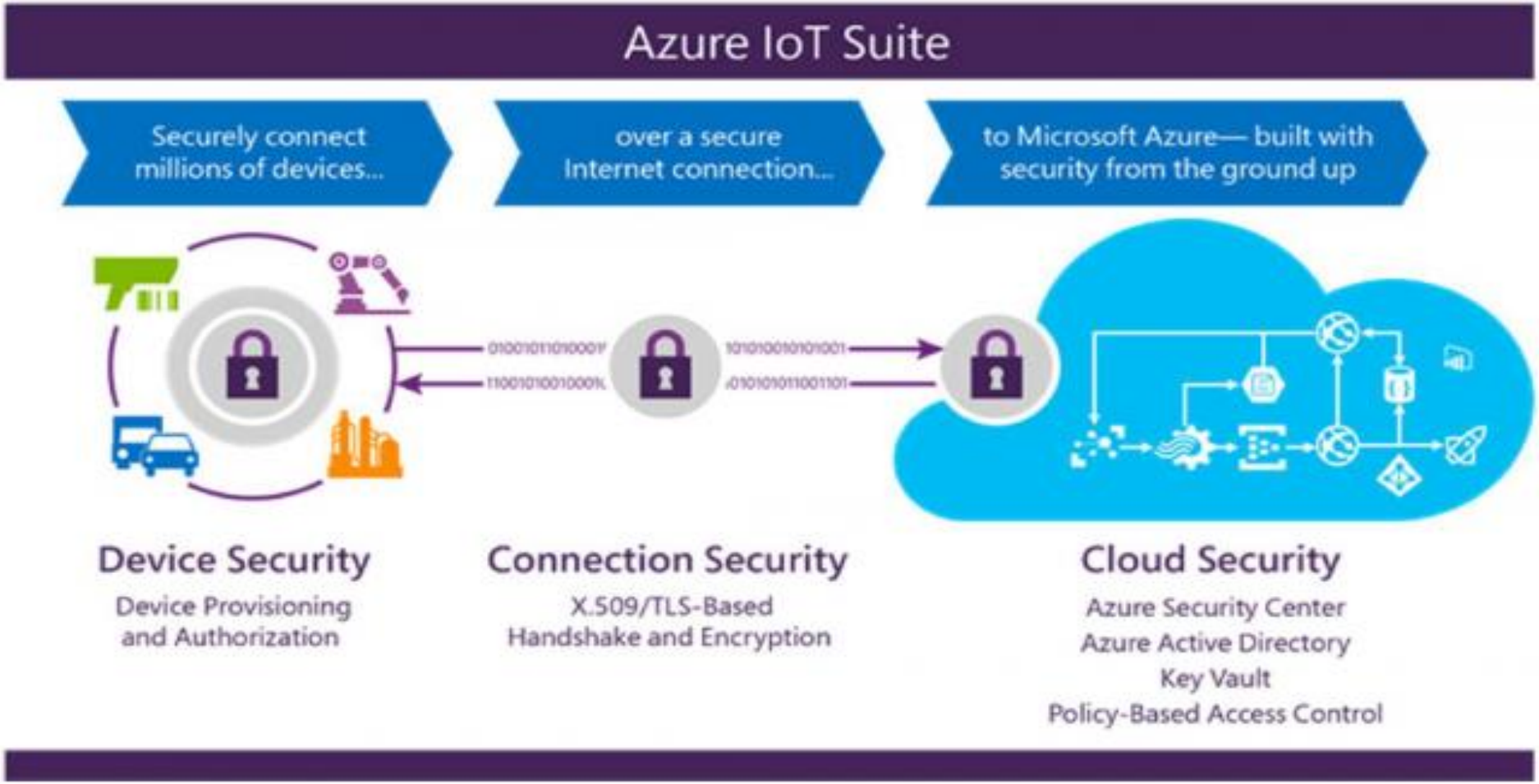


معماری Microsoft Azure

- پلتفرم Azure ماکروسافت بستر ارتباطی امن ماشینهای مجازی، و ابر با پایگاه داده را ایجاد می‌کند. خدمات شبکه، انعطاف‌پذیری، دسترس‌پذیری، امنیت و یکپارچگی را در انتقال اطلاعات فراهم می‌کند.
- پلتفرم چند اجاره‌ای از زیرساختهای مشترک برای پشتیبانی همزمان میلیونها کاربر، در قالب ۸۰ پایگاه داده استفاده میکند.
- برای حفاظت از داده های کاربران، از ایزوله کردن منطقی، فایروال، کنترل دسترسی، احراز اصالت و رمزنگاری استفاده میکند.
- پایگاه داده Azure از استانداردهای امنیتی متنوعی، از جمله SOC، ISO 27001 و SOC 2.1، استفاده میکند.

معماری Microsoft Azure

در پروژه Azure امنیت به سه بخش کلی (شکل زیر) تقسیم بندی می شود: امنیت دستگاه، امنیت ارتباطات و امنیت سکو



معماری Cisco

شرکت Cisco محصولات متنوعی را برای پاسخ به نیازمندی های امنیتی در قالب پروژه ارائه داده است که از جمله آنها موارد زیر بوده است:

- ✓ حفاظت پیشرفته در برابر بدافزارها (Advanced Malware Protection)
- ✓ نسل بعدی امنیت شبکه
- ✓ امنیت وب و ایمیل
- ✓ تحرک پذیری و دسترسی امن
- ✓ مرکز داده امن
- ✓ امن‌سازی هر تجهیز و هر سیستم
- ✓ مهیا نمودن امنیت برای تمام پردازش‌ها در تمام لایه‌ها
- ✓ انتقال و اتصالات امن بین هر لایه حتی بین دورترین گره‌ها

معماری Cisco

Levels

7 **Collaboration & Processes**
(Involving People & Business Processes)

6 **Application**
(Reporting, Analytics, Control)

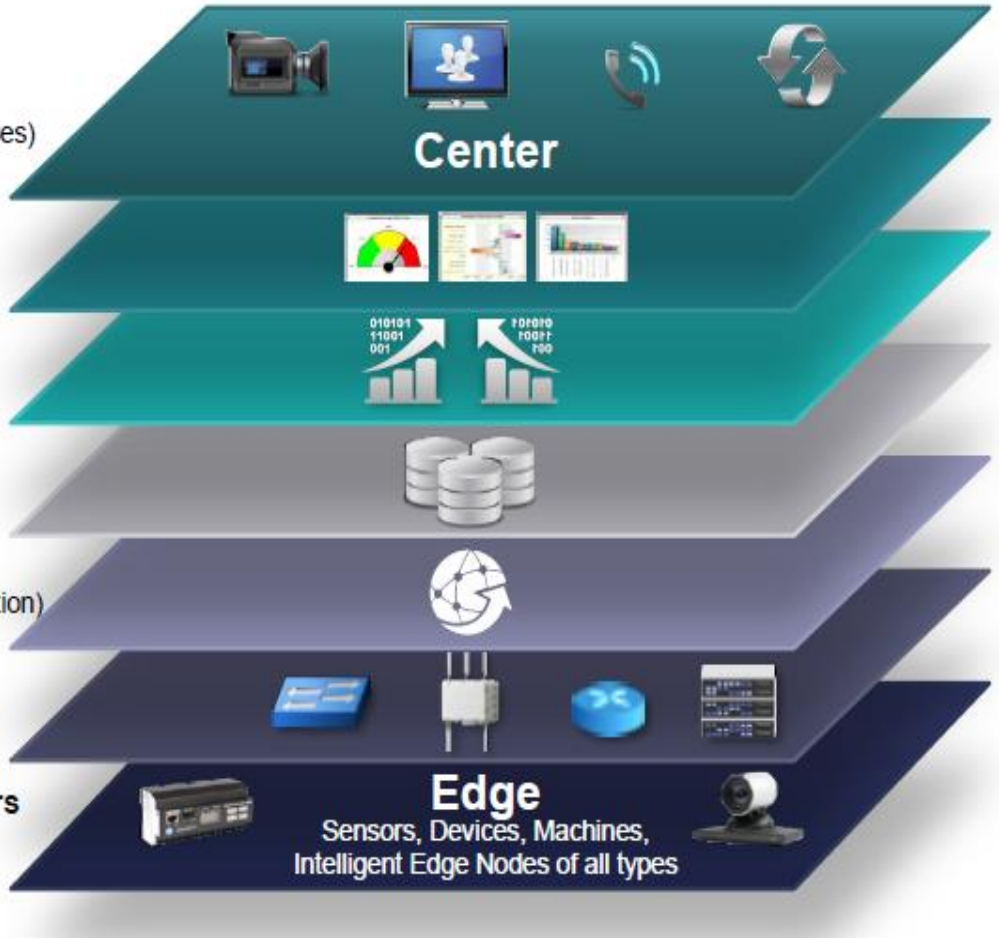
5 **Data Abstraction**
(Aggregation & Access)

4 **Data Accumulation**
(Storage)

3 **Edge (Fog) Computing**
(Data Element Analysis & Transformation)

2 **Connectivity**
(Communication & Processing Units)

1 **Physical Devices & Controllers**
(The "Things" in IoT)



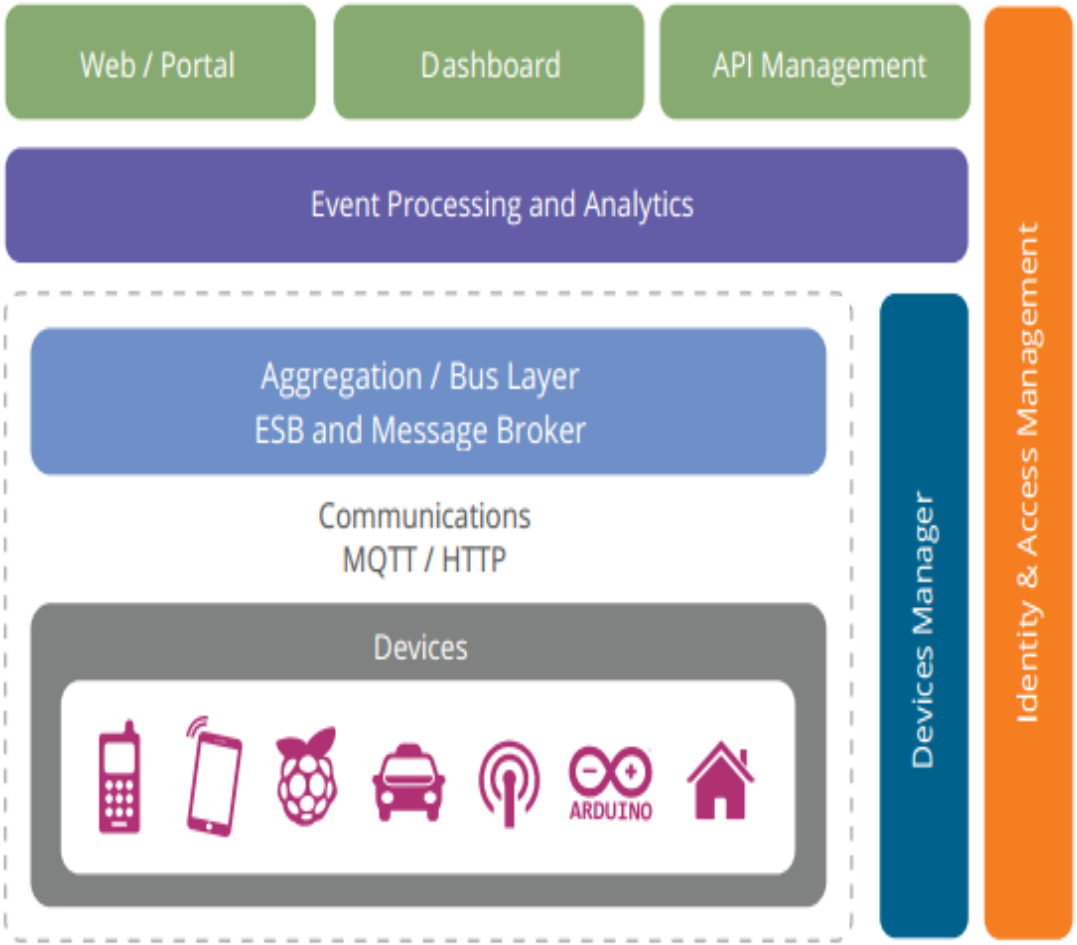
معماری WSO2

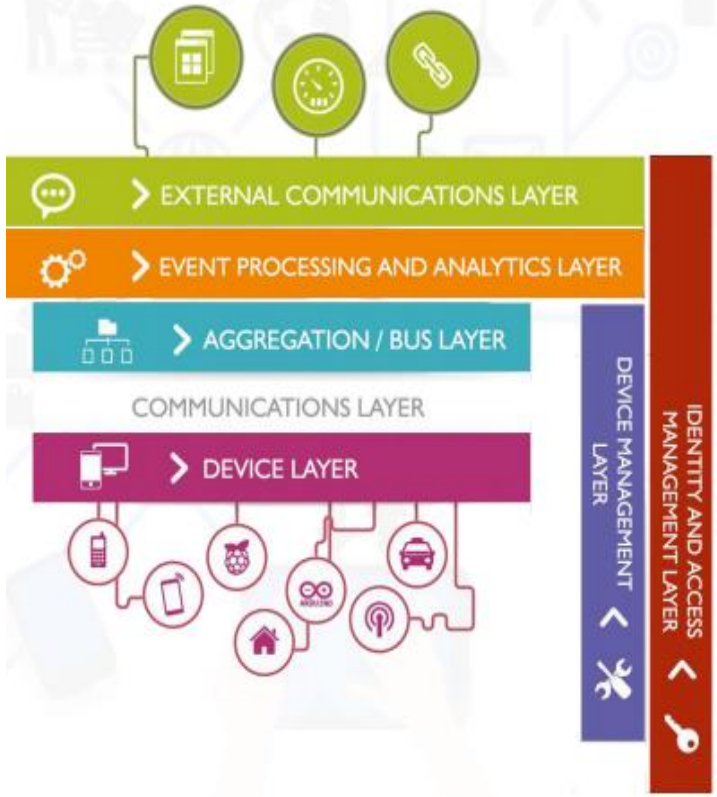
در مدل مرجع WSO2، امنیت از مهمترین لایه‌های مطرح در معماری می‌باشد. به این دلیل که سنسورهای IoT، اغلب اطلاعات بسیار خصوصی را جمع‌آوری نموده و به نوعی دنیای واقعیت را به دنیای مجازی منتقل می نمایند.

در بخش امنیت، مدیریت شناسه و مدیریت سطح دسترسی جزو موارد مهم از شاخص‌های امنیتی به شمار می‌روندکه از روش احراز اصالت از طریق بلیط‌های مدیریت شده استفاده می گردد.

- مدیریت شناسه و بلیط به صورت دسترسی از راه دور امکان‌پذیر خواهد شد.
- کنترل دسترسی مبتنی بر مدیریت کاربر و مبتنی بر سیاست‌ها برقرار خواهد شد.

معماری WSO2

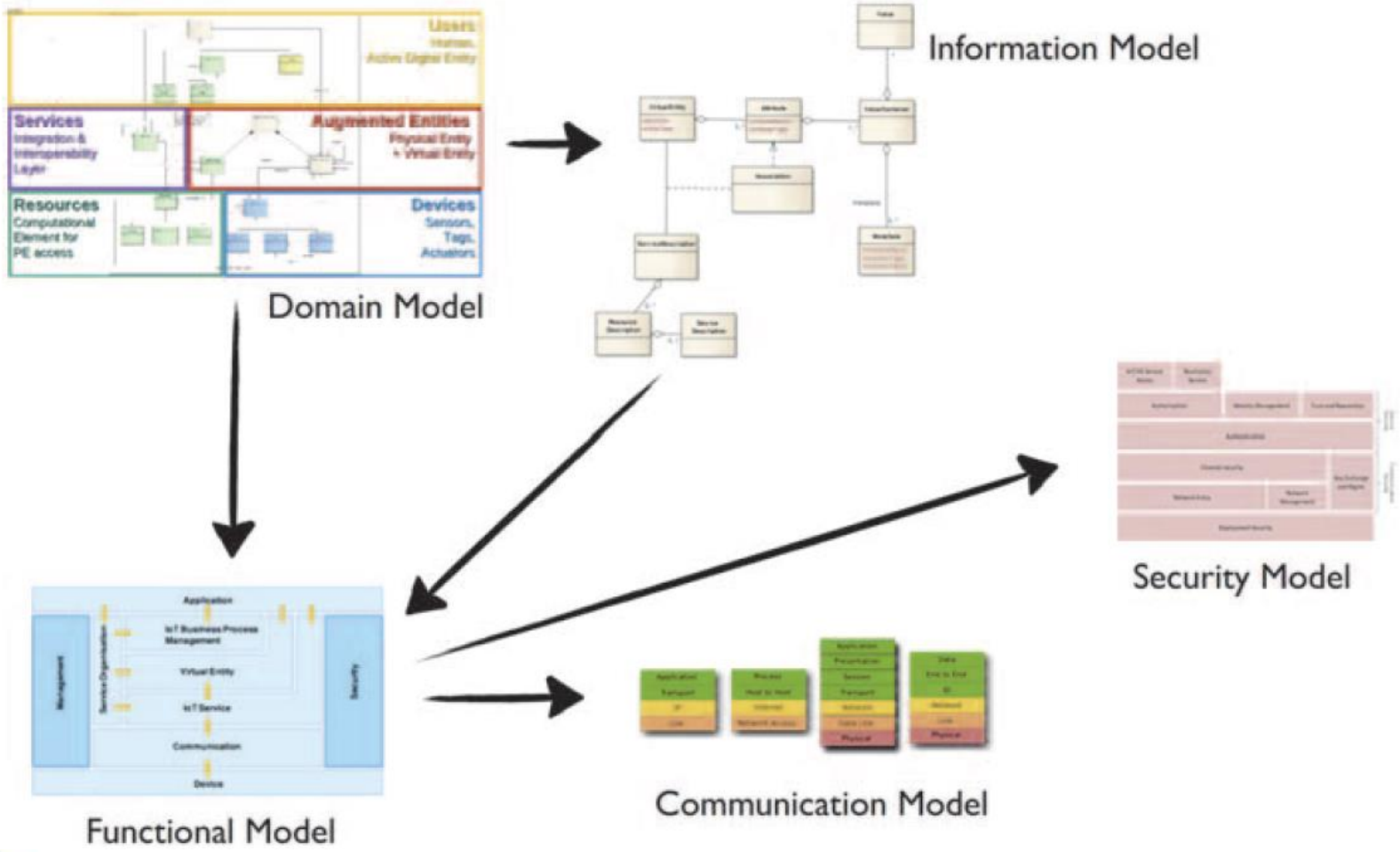

Web / Portal
Dashboard
API Management
Event Processing and Analytics
Aggregation / Bus Layer
ESB and Message Broker
Communications
MQTT / HTTP
Devices
ARDUINO
Devices Manager
Identity & Access Management


EXTERNAL COMMUNICATIONS LAYER
EVENT PROCESSING AND ANALYTICS LAYER
AGGREGATION / BUS LAYER
COMMUNICATIONS LAYER
DEVICE LAYER
DEVICE MANAGEMENT LAYER
IDENTITY AND ACCESS MANAGEMENT LAYER

معماری IoT-A

- ✓ ارائه یک مدل مرجع معماری برای سیستم های IoT با بیان اصول و راهنماها برای طراحی فنی پروتکل ها، رابط های کاربری و الگوریتم های آن برای رسیدن به سازگاری ارتباط پایان به پایان برای ارتباطات بی درز میان دستگاه های IoT
- ✓ ایجاد و توسعه ابزارهای مدلسازی و زبان توصیف برای تراکنش های IoT که امکان بیان وابستگی های آنها را برای مجموعه ای از مدل های گسترش گوناگون فراهم سازد.
- ✓ ایجاد مکانیزم حریم خصوصی و امنیت کارا و کل نگرانه در دستگاه های IoT و پروتکل ها و سرویس های مورد استفاده آنها مشارکت در پخش و بهره برداری از پایه های معماری ایجاد شده

معماری IoT-A


Users
Services
Integration & Interoperability Layer
Augmented Entities
Physical Entity + Virtual Entity
Resources
Computational Element for PE access
Devices
Sensors, Tags, Actuators
Domain Model
Information Model
Security Model
Application
IoT Business Process Management
Virtual Entity
IoT Service
Communication
Device
Functional Model
Communication Model

بخش دوم

- ✓ بررسی و معرفی تهدیدات و حملات
- ✓ بررسی و معرفی مکانیزم‌های پیشگیری و حفاظتی الزامی
- ✓ طرح معماری امن پیشنهادی

Attributes	indexes		IoT_A ARM	Wso2	Korean ARM	Azure ARM
Non-functional	Interoperability		√	√	√	√
	Scalability		√	√	√	√
	Reliability		√	√	√	√
	Availability		√	√	√	√
	Adaptability		√	√	√	√
	Manageability		√	√	√	√
Functional	**Application & Network Support Requirements**	Programmable Interfaces	√	√	√	√
		Collaboration	√	√	√	√
		Real-time	√	√	√	√
		Mobility Services	√	√	√	√
		Reliable And Secure Human Body Connectivity Services	√	-	-	√
		Autonomic Services	√	√	√	√
		Service Management	√	√	√	√
		Discovery Services	-	√	-	-
		Virtual Storage And Processing	√	-	√	-
		Context Awareness	-	√	-	-
		Communication Control	√	√	√	√
		Intelligent Communication	√	-	-	√
		Heterogeneous Communication Support	√	√	√	√
		Dynamic Adaption	-	-	-	-
	Device Requirements	Connectivity Of Things	√	√	√	√
		Device Control And Configuration	√	√	√	√
		Monitoring Of Things	√	√	√	√
		Device Mobility	√	√	√	√
		Device Integrity Checking	√	√	√	√
		Data Access Control	√	√	√	√

توابع معماری مرجع

Attributes	indexes	IoT_A ARM	Wso2	Korean ARM	Azure ARM
Non-functional	Interoperability	√	√	√	√
	Scalability	√	√	√	√
	Reliability	√	√	√	√
	Availability	√	√	√	√
	Adaptability	√	√	√	√
	Manageability	√	√	√	√

Attributes	indexes		Iot_a ARM	Wso2	Korean ARM	Azure ARM
Functional	Application & Network Support Requirements	Programmable Interfaces	√	√	√	√
		Collaboration	√	√	√	√
		Real-time	√	√	√	√
		Mobility Services	√	√	√	√
		Reliable And Secure Human Body Connectivity Services	√	-	-	√
		Autonomic Services	√	√	√	√
		Service Management	√	√	√	√
		Discovery Services	-	√	-	-
		Virtual Storage And Processing	√	-	√	-
		Context Awareness	-	√	-	-
		Communication Control	√	√	√	√
		Intelligent Communication	√	-	-	√
		Hetrognous. Cmmuncton. Suprt.	√	√	√	√
		Dynamic Adaption	-	-	-	-
	Device Requirements	Connectivity Of Things	√	√	√	√
		Device Control/ Configuration	√	√	√	√
		Monitoring Of Things	√	√	√	√
		Device Mobility	√	√	√	√
		Device Integrity Checking	√	√	√	√
	Data Management Requirements	Data Access Control	√	√	√	√
		Data Validation	√	√	√	√
		Mngmnt Of Large Volumes Data	√	√	√	-
	Security And Privacy Protection Requirements	Secure Control	√	√	√	√
		Secure Device	√	√	√	√
		Secure data exchange	√	√	√	√
		Trust & Privacy	√	√	√	√
		security management	√	√	√	√

Attributes	indexes		Iot_a ARM	Wso2	Korean ARM	Azure ARM
Functional	Application & Network Support Requirements	Programmable Interfaces	√	√	√	√
		Collaboration	√	√	√	√
		Real-time	√	√	√	√
		Mobility Services	√	√	√	√
		Reliable And Secure Human Body Connectivity Services	√	-	-	√
		Autonomic Services	√	√	√	√
		Service Management	√	√	√	√
		Discovery Services	-	√	-	-
		Virtual Storage And Processing	√	-	√	-
		Context Awareness	-	√	-	-
		Communication Control	√	√	√	√
		Intelligent Communication	√	-	-	√
		Hetrognous. Cmmuncton. Suprt.	√	√	√	√
		Dynamic Adaption	-	-	-	-
	Device Requirements	Connectivity Of Things	√	√	√	√
		Device Control/ Configuration	√	√	√	√
		Monitoring Of Things	√	√	√	√
		Device Mobility	√	√	√	√
		Device Integrity Checking	√	√	√	√
	Data Management Requirements	Data Access Control	√	√	√	√
		Data Validation	√	√	√	√
		Mngmnt Of Large Volumes Data	√	√	√	-
	Security And Privacy Protection Requirements	Secure Control	√	√	√	√
		Secure Device	√	√	√	√
		Secure data exchange	√	√	√	√
		Trust & Privacy	√	√	√	√
		security management	√	√	√	√

بررسی و معرفی آسیب‌پذیری‌ها، تهدیدات و حملات

فناوری‌ها	آسیب‌پذیری‌ها
شبکه	✓ احراز هویت و مجوز دهی و اعتبارسنجی داده‌ها انجام نمی‌شود. ✓ API های نا امن و رمزنشده موجود است. ✓ بیش از ۸۰٪ از اطلاعات شخصی کاربران در شبکه در حال جمع آوری است. ✓ آسیب‌پذیری Xss/SQLi در اغلب واسط‌های وب وجود دارد. ✓ در ۹۰٪ موارد احراز هویت دوفاکتوری وجود ندارد. ✓ ۷۰٪ تجهیزات از رمزنگاری استفاده نمیکنند. ✓ بروزرسانی‌ها اغلب مغفول می‌ماند. ✓ اغلب سیستم‌ها کلمه عبور ۱۲۳۴۵۶ را می پذیرند. ✓ تعداد شناسه‌های کاربردی متعددی وجود دارد. ✓ Lockout شدن شناسه های کاربری انجام نمی شود.
برنامه‌های کاربردی	
موبایل و تجهیزات سیار	
فناوری cloud	

آسیب‌پذیری‌های IOT (OWASP IOT TOP 10)

آسیب‌پذیری‌های IoT (OWASP)	الزامات امنیتی IoT
1. Insecure web interface	• هیچ واسط وبی مجاز به انتخاب کلمه عبور ضعیف نمی باشد. • تمام واسطهای وب مقابل حملات XSS, SQLi and CSRF تست شده اند. • تمام واسطهای وب ارتباط HTTPS را پشتیبانی می کنند • یک دیوار آتش لایه کاربردی برای حفاظت از واسط وب تعبیه شده است. • در هر زمان امکان ویرایش credentialها توسط مالک وجود دارد.
2. Insufficient Authentication/Authorization	• هر دسترسی که با احراز هویت انجام می شود کلمه عبوهای قوی خواهد داشت. • هرجا که ممکن است احراز هویت دو فاکتوری انجام شود. • امکان بازیابی کلمه عبور به صورت امن وجود داشته باشد. • همه کاربران امکان انتخاب کلمه عبور سخت را داشته باشند • هر کلمه عبوری دوره انقضایی داشته باشد. • کابران امکان تغییر credential پیش تعریف شده را داشته باشند.
3. Insecure Network Services	• مطمین باشیم که هر تجهیزی تنها با پورت‌های فعال شبکه کار کند. پورتهای بلااستفاده بسته باشند. • تمام سرویسهای شبکه از آسیب‌پذیری‌هایی نظیر buffer overflows و DOS اسکن شده باشند.

آسیب‌پذیری‌های IOT (OWASP IOT TOP10)

آسیب‌پذیری‌های (OWASP) IoT	الزامات امنیتی IoT
4. Lack of Transport Encryption	• از رمزنگاری ارتباطات بین نهادهای سیستمی، تجهیزات مطمئن باشیم. • از استانداردهای رمزنگاری معتبر استفاده شود و از مکانیزم های پیش تعریف تجهیزات اجتناب شود. • پروتکل‌های TLS/SSL به صورت درست و بروز پیاده سازی شده باشد و درست پیکربندی شده باشند. • دیوار آتش لحاظ شده باشد.
5. Privacy Concerns	• کمترین و تنها مورد نیازترین اطلاعات شخصی کاربران جمع آوری شود. • جمع‌آوری داده محافظت شده انجام شود و رمزنگاری در زمان ذخیره و انتقال انجام گیرد. • تنها افراد مجاز خاصی به اطلاعات شخصی دسترسی داشته باشند. • تنها اطلاعات حساسیت کم جمع آوری شود. اطلاعات حساس مکانیزم اختصاصی دارد. • داده‌ها نهان نگاری شوند. • مدیریت Log و سیاست‌های مربوطه در محل اعمال گردد. • کاربران مجاز به اعمال مدیریت بر سطح / نحوه ذخیره داده خود باشند.
6. Insecure Cloud Interface	• تمام واسطهای ابر اسکن آسیب‌پذیری شده باشند. • انتخاب کلمه عبور ضعیف مجاز نباشد. • واسط وبی دارای انتخاب کلمه عبور دو فاکتوری باشند. • تمام واسط های وبی از رمزنگاری در زمان انتقال استفاده نمایند. • تمام واسط های وبی در مقابل آسیب پذیری‌های XSS, SQLi , CSRF تست شده باشند. • کاربران کلمه عبور قوی داشته باشند. • کلمات عبور دوره اعتبار داشته باشند.

آسیب‌پذیری‌های IOT (OWASP IOT TOP10)

آسیب‌پذیری‌های (OWASP) IoT	الزامات امنیتی IoT
7. Insecure Mobile Interface	• هیچ برنامه کاربردی موبایل کلمه عبور ضعیف نداشته باشد. • امکان lockout در تمام برنامه های کاربردی موبایل وجود داشته باشد. • امکان احراز هویت دو فاکتوری برنامه ها باشد (Apple's Touch ID) • رمزنگاری در زمان انتقال داده توسط تمام برنامه های کاربردی موبایل تعریف شود. • امکان تعریف کلمه عبور قوی وجود داشته باشد. • کابران امکان تغییر credentialپیش تعریف شده را داشته باشند.
8. Insufficient Security Configurability	• امکان انتخاب بین احراز هویت دوفاکتوری و یا انتخاب کلمه عبور سخت وجود داشته باشد. • امکان انتخاب رمزنگاری وجود داشته باشد.(تنظیم اولیه AES-256 و نه AES-128 باشد.) • برای رویدادهای امنیتی مدیریت log امن تعریف شده باشد. • برای رویدادهای امنیتی سیستم هشدار و اطلاع رسانی در دسترس باشد.
9. Insecure Software/Firmware	• تجهیزات به روز شده باشند و زمان کشف آسیب‌پذیری، وصله مربوطه بروزرسانی شود. • فایلهای بروزرسانی رمزشده باشند و تمام فایلهای درحال انتقال در حال رمز منتقل شوند. • تمام فایلهای بروزرسانی امکان مجازشناسی را قبل از نصب داشته باشند(رمزنگاری متقارن) • بروزرسانی سرورها به صورت امن انجام شود. • محصولات توانایی تولید جداول بروزرسانی را داشته باشند.
10. Poor Physical Security	• تجهیزات با کمترین پورتهای فیزیکی (USB) پیاده‌سازی شود. • به سطح سیستم عاملها از طریق پورت های USB دسترسی نباشد. • سیستم در مقابل نفوذ ارتقا یافته باشد. • امکان غیرفعال کردن پورت ها باشد.

لایه حسگرها و تجهیزات

- **تهدید:**
  - مکانیزم‌های کنترل دسترسی ضعیف
  - سنسورهای سرقت شده
  - سنسورها و ارتباطات قابل شنود
- **مکانیزم الزام شده این لایه:**
  - امنیت فیزیکی، ممانعت از شنود، کنترل امنیت

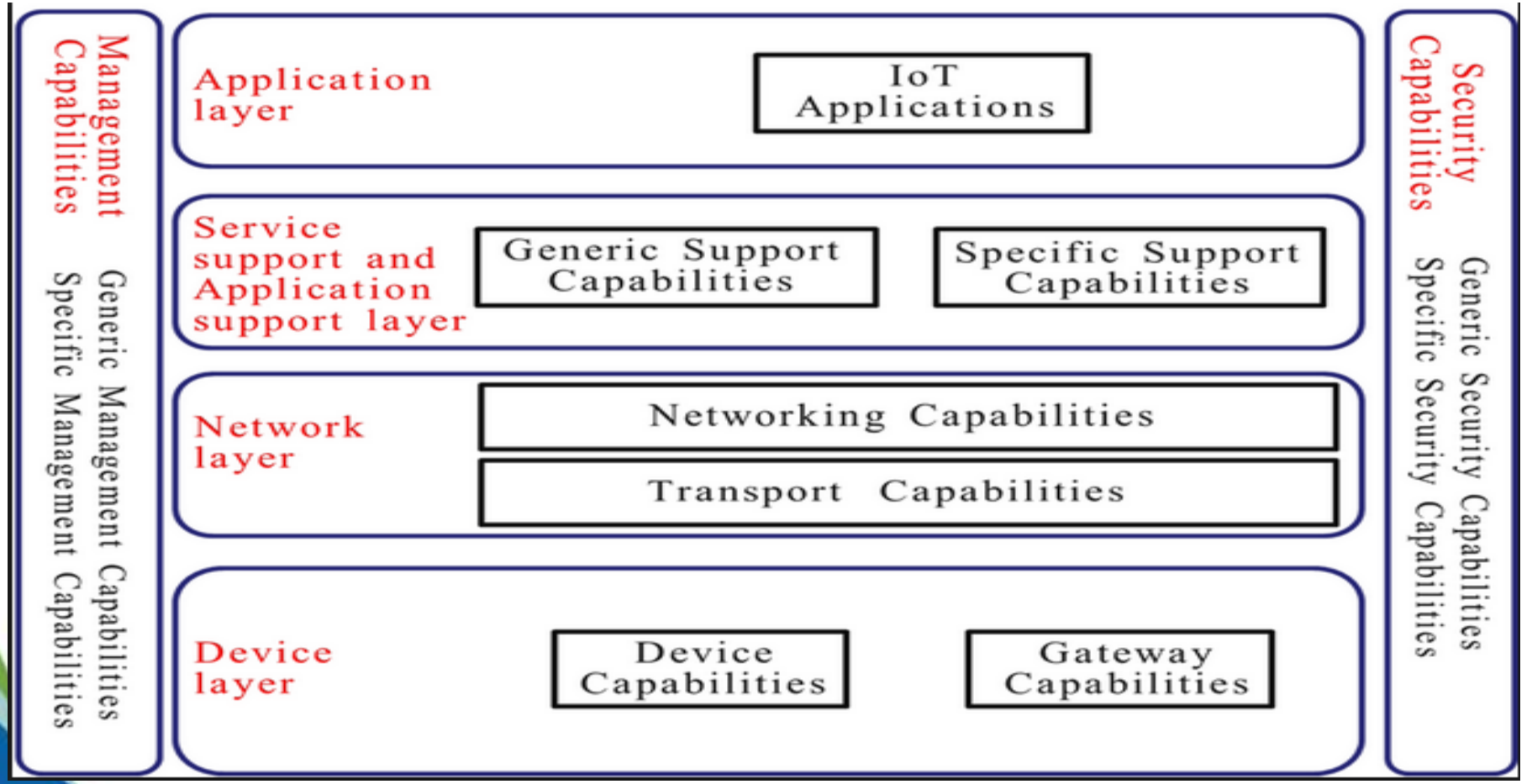
لایه انتقال و شبکه

- **تهدیدها:**
  - ارتباطات شبکه‌ای نا امن (عدم رمزنگاری)
  - دسترسی غیرمجاز
  - عدم وجود یکپارچگی داده
- **مکانیزم الزام شده برای این لایه:**
  - مکانیزم‌های محافظتی شبکه‌ای نظیر استفاده از دیوار آتش
  - احراز اصالت چند وجهی
  - رمزنگاری (حفظ حریم خصوصی و یکپارچگی انتقال داده)
  - استفاده از TLS , SSL و یا اتصال از طریق VPN در انتقال داده
  - جداسازی ترافیک IoT در شبکه‌های خصوصی

لایه سکو و سرویس

- **تهدید:**
  - حریم خصوصی داده کاربر
  - سرقت و یا صدمه به داده
  - دسترسی غیرمجاز به داده
- **مکانیزم الزام شده برای این لایه:**
  - امنیت اطلاعات جامع برای برنامه‌های کاربردی بستر ابر
  - مکانیزم‌های محافظتی شبکه‌ای نظیر استفاده از دیوار آتش / رمزنگاری و احراز اصالت
  - کنترل دسترسی و احراز اصالت قوی در سطح تجهیزات
  - انتقال داده رمزگذاری شده

طرح معماری امن پیشنهادی
(مدل مرجع IOT در استاندارد ITU-T Y.2060)



لایه‌های IoT مبتنی بر استاندارد ITU-T Y.2060

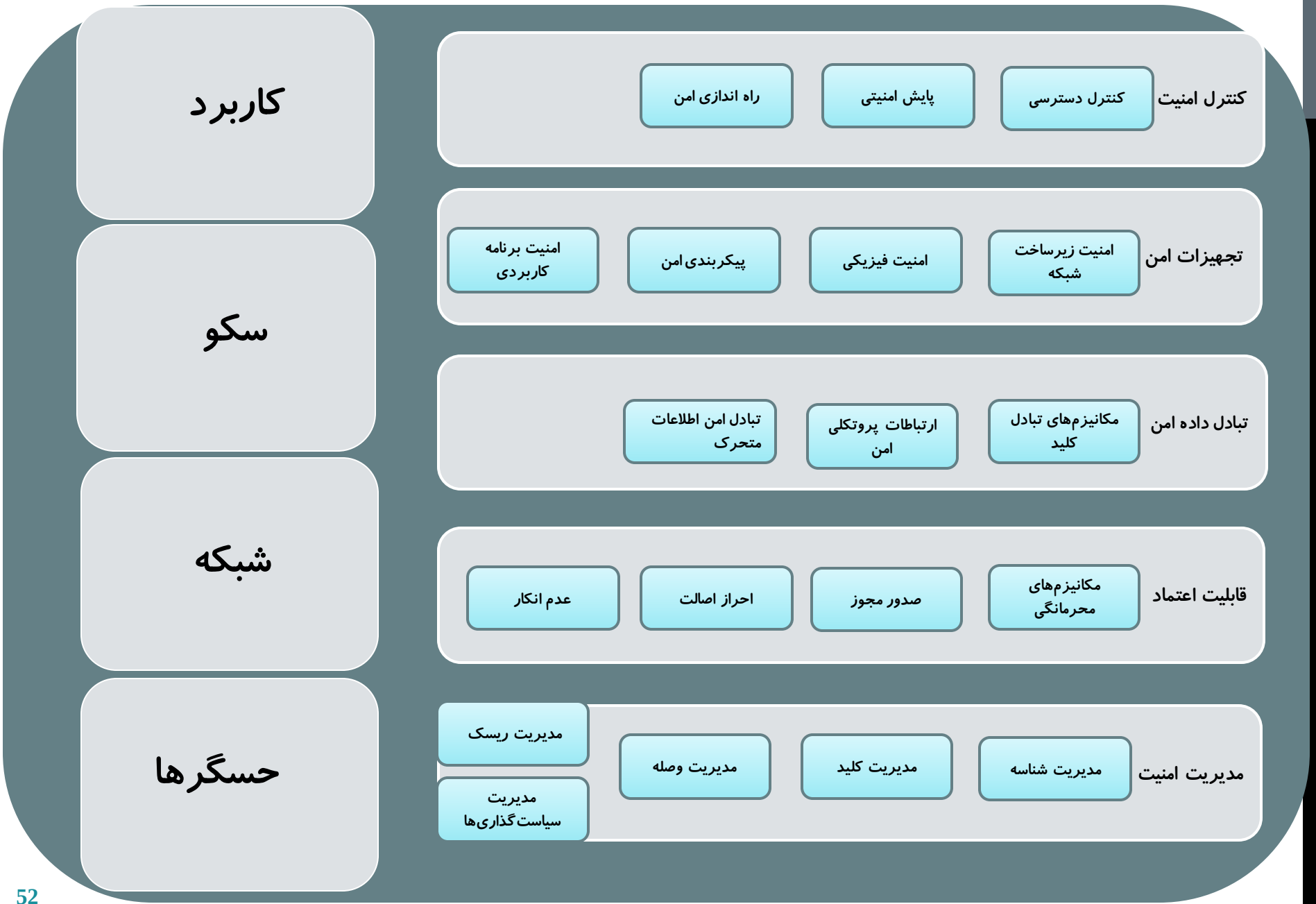
طرح معماری امن پیشنهادی
(شاخص های امنیتی سطح اول)

ماژول های امنیتی	حسگر	شبکه	سکو و سرویس
۱- کنترل امنیت	√	√	√
۲- تجهیزات امن	√	√	√
۳- تبادل داده امن (Secure data exchange)	√	√	√
۴-قابلیت اعتماد (Trust) و حریم خصوصی	√	√	√
۵- مدیریت امنیت	√	√	√

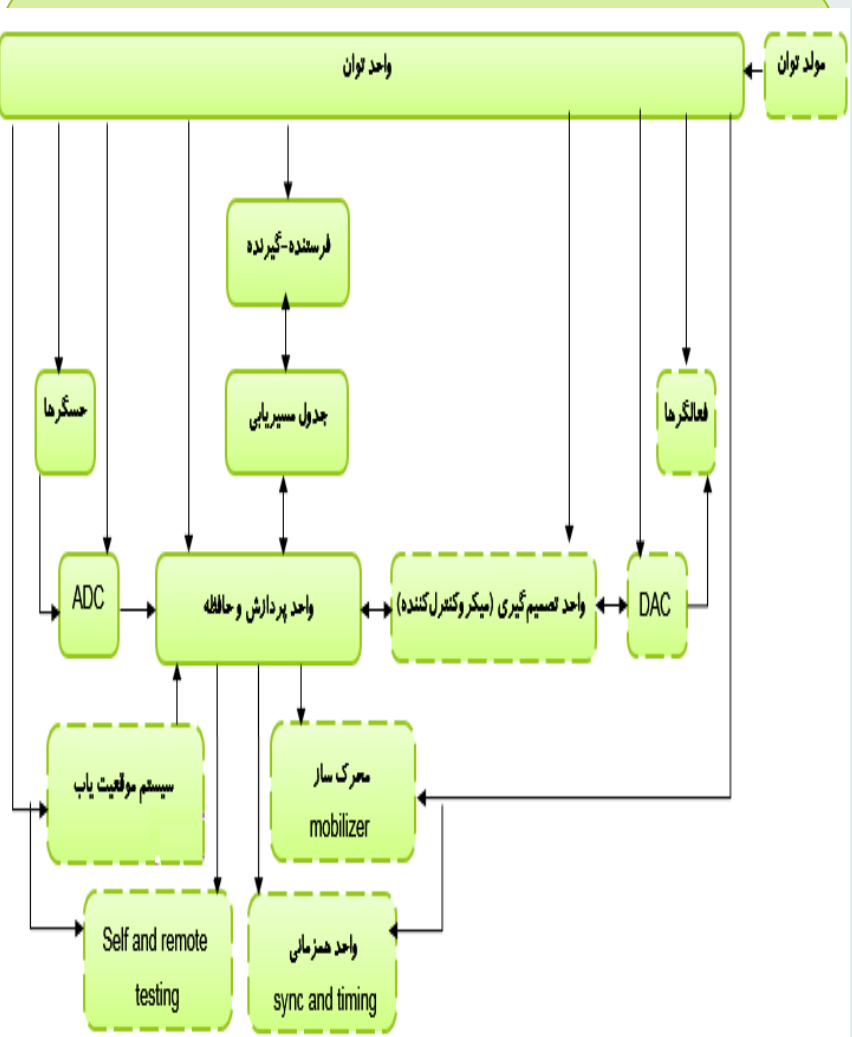
طرح معماری پیشنهادی (شاخص های امنیتی سطح دوم)

ماژول های امنیتی	زیرماژول ها	حسگر	شبکه	سکو و سرویس
۱- کنترل امنیت	کنترل دسترسی (Access Control)	√	√	√
	پایش امنیتی (SOC,NOC,CERT, Firewall, IDS, WAF, ..)	-	√	√
	راه‌اندازی امن (Bootstrapping)	√	-	-
۲- تجهیزات امن	امنیت زیرساخت شبکه (infrastructure)	-	√	√
	امنیت فیزیکی (physical Security)	√	-	-
	پیکربندی امن (secure configuration)	√	√	√
	امنیت برنامه کاربردی (secure application)	-	-	√
۳- تبادل داده امن (Secure data exchange)	تبادل کلید (Key Exchange)	√	√	√
	ارتباطات پروتکلی امن (Secure protocol)	–	√	√
	تبادل امن اطلاعات متحرک (Secure Mobile Interface)	√	-	-
۴-قابلیت اعتماد (Trust) , حریم خصوصی (Privacy)	مکانیزم‌های محرمانگی (Encryption ,Anonymization)	√	√	√
	مجوزدهی (Authorization)	√	√	√
	احراز اصالت (Authentication)	√	√	√
	عدم انکار (Non Repudiation)	√	√	√
۵- مدیریت امنیت (security management)	مدیریت شناسه (Identity management)	√	√	√
	مدیریت کلید (Key management)	–	√	√
	مدیریت وصله (Patch management)	-	-	√
	مدیریت ریسک (DRM, RiskManagement)	√	√	√
	مدیریت سیاست‌گذاری‌ها (Policy Mngmnt)	√	√	√

شاخص‌های امنیتی لایه‌ها



شاخص‌های امنیتی لایه حسگرها



کنترل امنیت
- کنترل دسترسی
- راه اندازی امن

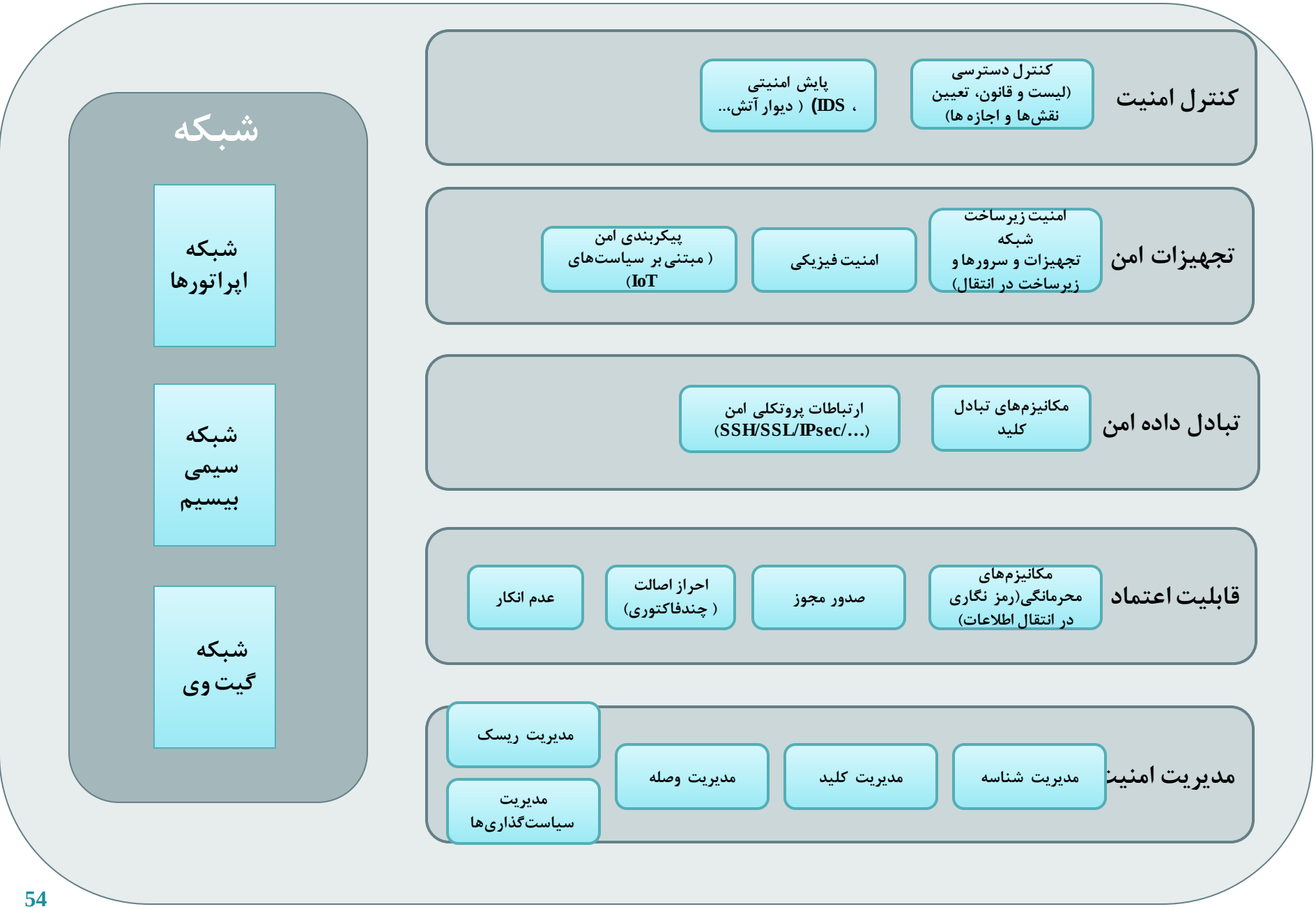
تجهیزات امن
- امنیت فیزیکی
- پیکربندی و بروزرسانی امن

تبادل داده امن
- مکانیزم‌های تبادل کلید(کلید مشترک)
- ارتباطات پروتکلی امن DTLS,Coap,6lowPAN
- تبادل امن اطلاعات متحرک

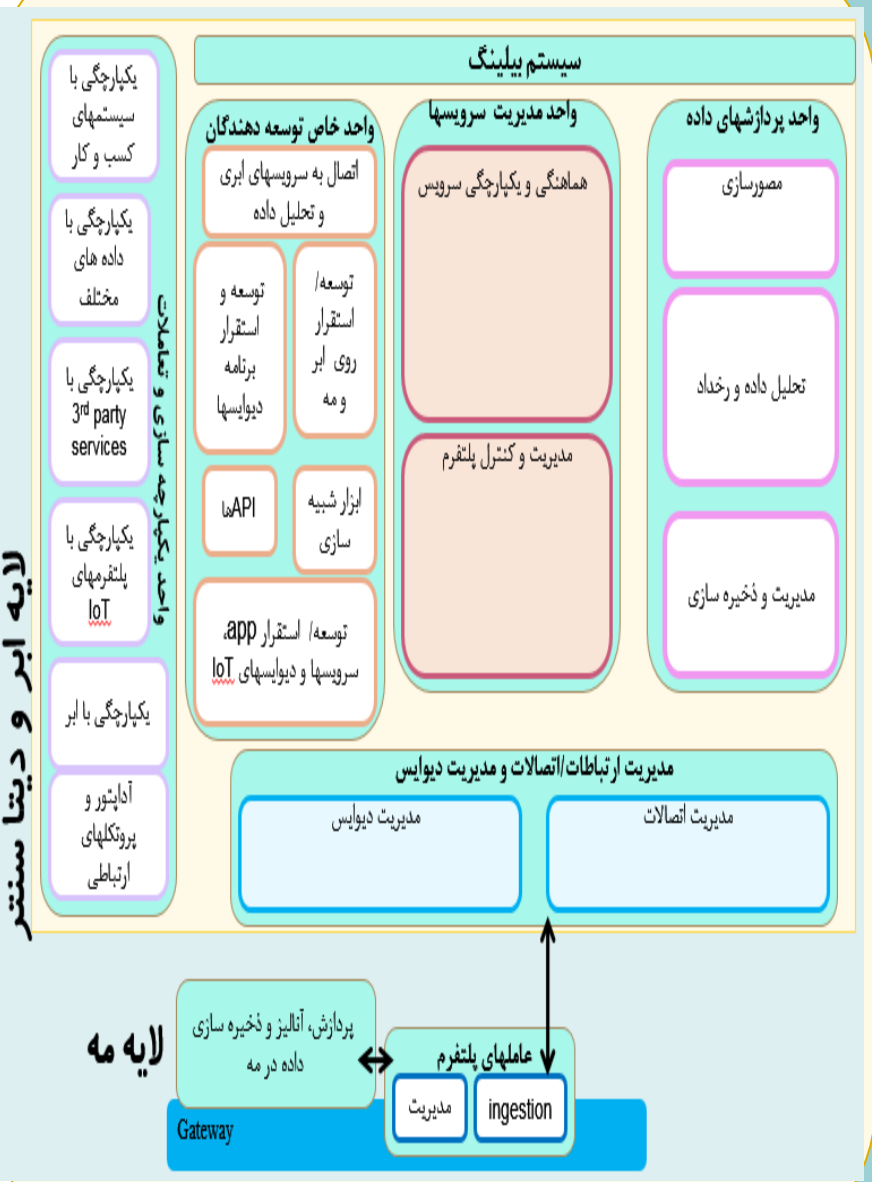
قابلیت اعتماد
- مکانیزم‌های محرمانگی (رمزنگاری) Lblock, speck
- صدور مجوز
- عدم انکار
- احراز اصالت

مدیریت امنیت
- مدیریت شناسه
- مدیریت کلید
- مدیریت ریسک
- مدیریت سیاست‌گذاری‌ها

شاخص‌های امنیتی شبکه



شاخص‌های امنیتی لایه سکو



کنترل امنیت

- کنترل دسترسی Access control list, rule
- پایش امنیتی /Firewall/WAF/SOC/ CERT…

تجهیزات امن

- امنیت زیرساخت شبکه Server/DC/AD/…
- پیکربندی امن
- امنیت برنامه کاربردی

تبادل داده امن

- مکانیزم‌های تبادل کلید(متقارن-نامتقارن)
- ارتباطات پروتکلی امن TLS/SSH/SSL

قابلیت اعتما

- مکانیزم‌های محرمانگی(رمزنگاری)
- صدور مجوز
- احراز اصالت (چندفاکتوری)
- عدم انکار

مدیریت امنیت

- مدیریت شناسه
- مدیریت کلید
- مدیریت وصله
- مدیریت ریسک
- مدیریت سیاست‌گذاری‌ها

جمع‌بندی و نتایج بخش معماری امن

- ✓ دو حوزه امنیتی Privacy و Trust مهمترین مباحث امنیتی در اکوسیستم IoT محسوب می‌شوند.
- ✓ تامین امنیت مربوط به سازوکارهای هر لایه بر عهده آن لایه است. (نظیر پیاده‌سازی امن لایه، رعایت policy های مربوط به نصب و راه اندازی ابزارها و برنامه‌ها (آخرین patchها، بروزرسانی‌ها، آنتی ویروس‌ها، دیوار آتش، ...)
- ✓ بین لایه‌های تقسیم شده مطابق با استاندارد ITU-T Y2060، بیشترین اهمیت امنیت در لایه حسگرها می‌باشد، به دلیل اینکه تمام اطلاعات کاربران جمع آوری می‌گردد.
- ✓ در این ارایه تنها به سازوکارهای الزام شده به دلیل معماری IoT بر روی هر لایه پرداخته شده است.

جمع‌بندی و نتایج بخش معماری امن

- ✓ مدیریت شناسه، مکانیزم‌های کنترل دسترسی (role based, access control list)
- ✓ اتصال راه دور با VPN و احراز اصالت چند فاکتوری
- ✓ یک معماری چند کاربره (multitenant) که بسترداده و انتقال هر سازمان مجزا شده باشد.
- ✓ انتقال داده رمز شده باشد و ذخیره داده باید مبتنی بر استاندارد (SAS 70-SSAE 16) انجام پذیرد.
- ✓ کنترل دسترسی و احراز اصالت قوی در سطح تجهیزات
- ✓ جداسازی ترافیک IoT در شبکه‌های خصوصی
- ✓ امنیت اطلاعات جامع برای برنامه‌های کاربردی بستر ابر