**تهدیدات امنیتی خانه هوشمند در لایه  
اشیا و راه های مقابله با آن**

**ارایه دهنده : زهرا دهقانیان**

**استاد راهنما: دکتر رضا صفابخش**

**دانشگاه صنعتی امیرکبیر**

**پاییز ۹۶**

***از پدر عزیزم که در تهیه این گزارش با لطف بی حدشان مرا یاری کردند ، کمال تشکر را دارم .***

چکیده

فهرست

فصل اول : مقدمه

* 1. مقدمه .....................................................................................................................

فصل دوم : بستر تحقیق

2-1- مقدمه......................................................................................................................

2-2- نهدیدات خانه هوشمند .......................................................................................

3-2- مولفه های امنیتی ................................................................................................

**فصل اول**

**مقدمه**

1-1-مقدمه

**فصل دوم**

**بستر تحقیق**

2-1-مقدمه

اینترنت اشیاء بستری است که در آن شبکه اینترنت موجود از سیستمهای رایانه‌ای به اشیاء یا موجودیتهای دنیای واقعی متصل هستند؛ اشیاء ممکن است شامل موجودیتها، وسایل برقی خانگی، دستگاه‌ها، ابزار و... باشد؛ وقتی این اشیاء طبق زیرساخت مشخص و پروتکلهای استاندارد خاصی به اینترنت متصل می‌شوند، «اینترنت اشیاء» نامیده می‌شود.

اشیاء در اینترنت هوشمند می‌توانند حقیقی یا مجازی و ثابت یا متحرک باشند در حالیکه اشیاء، شرکت‌کنندگان فعال در کل سیستم هستند، اشیاء، می‌توانند با یکدیگر و با انسان تعامل داشته باشند که این ارتباطات به ترتیب، ارتباط شی به شی و ارتباط شی با انسان نامیده می‌شوند.

اینترنت اشیاء شامل هشت حوزه‌ نقل‌وانتقال هوشمند، درمان هوشمند، کشاورزی هوشمند، خانه هوشمند، وسایل نقلیه هوشمند، مدرسه هوشمند، بازار هوشمند، و صنعت هوشمند است.

سیستم خانه هوشمند می‌تواند همانند آنچه در شکل 1 نشان داده شده، پیکربندی شود؛ سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است:



شکل 1 سیستم خانه هوشمند

ابتدا سرور‌خانه فرآیندهای ذخیره‌سازی، تجمیع و توزیع اطلاعات گردآوری شده از رسانه‌های مختلف موجود در خانه را انجام می‌دهد، سپس دروازه‌خانه، صاحب شبکه دسترسی را به شبکه خانگی متصل می‌کند؛ در نهایت دستگاه‌های خانه هوشمند قادر خواهند بود اطلاعات را میان دستگاه‌ها مبادله کرده و به اینترنت خارجی نیز دسترسی پیدا کند.

مؤلفه‌های تشکیل‌دهنده سیستم خانه هوشمند در مواجهه با تهدیدات داخلی یا خارجی قرار دارند زیرا اغلب این مؤلفه‌ها به اینترنت متصل هستند؛ برای غلبه بر چنین تهدیدات امنیتی، مانند تزریقات بدافزاری، دسترسی احراز هویت شده کاربر، افشای اطلاعات اساسی، لازم است تمهیدات امنیتی مطابق بر مشخصه‌های مؤلفه‌ای سیستم خانه هوشمند به کار گرفته شود.

2-2- تهدیدات خانه هوشمند

خانه های هوشمند از مؤلفه های متعددی تشکیل شده اند؛ این مؤلفه ها همواره در معرض تهدیدات مختلفی قرار دارند. حملات خانه های هوشمند به هفت گروه تقسیم شده اند که عبارتند از:

١. **حملات فیزیکی:** به دستکاری فیزیکی دستگاه ها اطلاق می شود؛ این حملات می تواند به انواع مختلفی از خطرات مانند فعالیت، سوءاستفاده نابهنجار یا استراق سمع، ممانعت یا سرقت منجر شود؛ معمولا یک حمله فیزیکی تمامی اموال را تحت تأثیر قرار می دهد.

٢. **خسارات ناخواسته (تصادفی) :** ممکن است از اطمینان نادرست و نابجا به افراد و آشنایان یا اشتباهات شخصی (مدیریتی، طراحی، عملکرد وغیره) ناشی شود؛ می تواند مراتب جبران ناپذیری همچون نشر اطلاعات، تغییرات غیرمعتبر یا حتی فقدان اطلاعات را با خود به همراه داشته باشد.

٣. **فجایع و قطع برق:** انکار خدمات برای کاربر را با خود به همراه دارد.

۴. **آسیب و فقدان:** نه تنها منجر به تخریب سرویس می شود، بلکه نشر اطلاعات را با خود به همراه دارد؛ در واقع باعث حذف اطلاعات حیاتی می شود.

۵. **خرابیها و بد عملکردها:** مهمترین نقطه شروع حمله توسط مهاجم است؛ مهاجم با بهره جویی از این فرصت، مبادرت به فعالیت، سوءاستفاده نابهنجار و استراق سمع، ممانعت و سرقت می کند.

۶. **استراق سمع، ممانعت و سرقت:** سوءاستفاده ناهنجار به تهدیدات سایبری و نیز حریم شخصی مربوط می شود؛ این دو مقوله به عنوان تهدیدات امنیتی در نظر گرفته می شود؛ مهاجم با تغییر طراحی یا به کارگیری نواقص، یک یا چند دارایی و موجودیت را به خطر خواهد انداخت که در نتیجه منجر به نقض محرمانگی داده های خصوصی یا از دست دادن کنترل یک دستگاه خواهد شد.

٧. **قانونی:** این نوع تهدید مراتبی همچون تهدیدات گذشته خواهد داشت اما نسبت به سایر تهدیدات از وقوع کمتری برخوردار است

3-2-.چالش های کلیدی

# زمانی که تمامی اشیاء اطراف انسان قابلیت کاربرد اینترنت را پیدا نموده و در نهایت مفهوم اینترنت اشیاء محقق گردد، انواع جدیدي ازکاربردها موجود خواهند بود. دو مبحث امنیت و حریم خصوصی به عنوان دو مولفه اساسی و مهم در حوزه اینترنت اشیاءنقش پررنگی در این کاربرد ها خواهند که در ادامه به این دو مهم میپردازیم.

3-2-1 امنیت اطلاعات

امنیت اصلی ترین نگرانی شبکه هاي است که در مقیاس بزرگ پیاده سازي می شوند. دنیاي دیجیتال، با داده هاي شخصی و اشتراکی و ثبت شده توسط افراد اشباع شده است و نگرانی هایی را در زمینه امنیت و حفاظت از اطلاعات افراد و دولت ها فراهم کرده است. همچنین مشکلات ناشی شده از انتقال و پردازش داده هاي ناخواسته، موجب نگرانی هاي کاربران و مسائل قانونی شده است. در صورت نقض امنیت ، رخداد حمله و اختلال در عملکرد ، مزایاي هوشمندسازی کمرنگ میشود . چنانچه هکرها کنترل شبکه را به عهده بگیرند رویدادهاي ناگواري به وقوع خواهد پیوست. براي مثال با در دست گرفتن کنترل درب خانه توسط نفوذگران به شبکه می تواند زمینه سرقت از خانه را فراهم کند .

به طور کلی، سرویسهاي امنیتی که در این حوزه قرار است ارائه شوند باید ویژگی هاي محرمانگی، تمامیت و دسترسی پذیری را فراهم نمایند. در ادامه به بررسی این عناصر می پردازیم :

 محرمانگی:

اولین قدم براي برقراري امنیت، برآورد محرمانگی است. محرمانگی بدین معنی است که مهاجم نباید هیچ دانشی از محتواي پیام هاي تبادلی مابین موجودیت هاي حاضر در اینترنت اشیاء همانند یک گرهي حسگر و هر موجودیت اینترنتی دیگري به دست آورد.

#  تمامیت :

# در حالت کلی در مبحث امنیت ، موجودیتی "تمام" است که سه ویژگی زیر را داشته باشد :

# یکپارچگی: در تمامی مراحل ارتباط ، داده رد و بدل شده باید بدون تغییر باقی بماند. به عبارت دیگر، هرگونه تغییر )احتمالی( در پیامها باید توسط گیرنده پیام قابل تشخیص باشد.

# تازگی: این ویژگی تضمین می کند که پیامهاي قدیمیتر تکرار نمیشوند. این امر به جهت تضمین کانال ارتباطی در مقابل حملات تکرار مهم است.

# صحت : این ویژگی نیز تضمین کننده ی درستی اطلاعات در تمامی مراحل ارتباط می باشد.

# دسترسی پذیری: همچنان که برنامهها و سرویسهاي حوزهي IoT با مقیاس بالایی در حال گسترش میباشند، نیاز به چهارچوبی است که کاربران سیستم را قادر سازد تا اطمینان یابند اطلاعات و سرویسهایی که میان طرفین مبادله میشوند به راستی قابل اعتماد و اتکا هستند. چهارچوب اعتماد نیاز به این دارد که بتواند با انسانها و ماشینها به عنوان کاربران سروکار داشته باشد، یعنی این چهارچوب نیاز دارد تا اعتماد را به انسانها منتقل نماید و همچنین نیاز دارد تا به اندازهي کافی در مقابل حملاتی چون منع

سرویسدهی 3 (DoS) مقاوم E\_\_\_\_\_\_\_\_\_باشد

3-2-2 حریم شخصی