

عنوان

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

نگارش

**زهرا دهقانیان**

استاد راهنما

**دکتر رضا صفابخش**

پاییز ۹۶

***از پدر عزیزم که در تهیه این گزارش با لطف بی حدشان مرا یاری کردند ، کمال تشکر را دارم و از خداوند منان خواهان طول عمری با برکت برای ایشان هستم.***

# چکیده

اینترنت اشیاء بستری است که در آن شبکه اینترنت موجود از سیستم های رایانه­ای به اشیاء یا موجودیت های دنیای واقعی متصل هستند؛ اشیاء ممکن است شامل موجودیت­ها، وسایل برقی خانگی، دستگاه­ها، ابزار، وسایل اسباب بازی و هر وسیله ای که قابلیت متصل شدن به اینترنت را داشته باشد. این اشیاء طبق زیرساخت مشخص و پروتکل­های استاندارد خاصی به اینترنت متصل شده و اینترنت اشیاء شکل می گیرد. در این تحقیق ما به فن­آوری بکار رفته در خانه­های هوشمند، چالش­های اصلی این حوزه و تهدیدات امنیتی موجود پرداخته و در نهایت برای حفظ حریم خصوصی و رفع دغدغه­های مطرح شده امنیتی راهکارهای مناسب ارایه داده می­شود.

**واژه های کلیدی:** اینترنت اشیاء، خانه هوشمند، تهدیدات امنیتی، امن سازی و حریم­خصوصی

# 

فهرست

[1 مقدمه 1](#_Toc502634784)

[2 خانه هوشمند 3](#_Toc502634785)

[2-1 فناوری های موجود 4](#_Toc502634786)

[2-1-1 Zigbee 4](#_Toc502634787)

[2-1-2 برچسب هوشمند 5](#_Toc502634788)

[2-1-3 ارتباطات میدان نزدیک 6](#_Toc502634789)

[2-1-4 شبکههای موبایلی 7](#_Toc502634790)

[2-1-5 بلوتوث 7](#_Toc502634791)

[2-1-6 Z-Wave 8](#_Toc502634792)

[2-2 تهدیدات خانه هوشمند 10](#_Toc502634793)

[3 چالشها و راهکارها 11](#_Toc502634794)

[3-1 چالش امنیت اطلاعات 11](#_Toc502634795)

[3-1-1 محرمانگی 11](#_Toc502634796)

[3-1-2 تمامیت 11](#_Toc502634797)

[3-1-3 دسترسی پذیری 12](#_Toc502634798)

[3-2 چالش حریم خصوصی 12](#_Toc502634799)

[3-3 راهکارها 12](#_Toc502634800)

[3-3-1 احراز هویت 13](#_Toc502634801)

[3-3-2 رمزنگاری 13](#_Toc502634802)

[3-3-3 دیواره آتش 13](#_Toc502634803)

[4 جمع بندی 14](#_Toc502634804)

[5 منابع 15](#_Toc502634805)

# 1 مقدمه

اینترنت اشیا یا IOT[[1]](#footnote-1) بخشی از اینترنت آینده است که شامل اینترنت موجود و در حال رشد و همچنین توسعه­های آینده شبکه می­شود. اینترنت اشیا به طور مفهومی می­تواند به عنوان یک زیر ساخت شبکه سراسری

پویا با قابلیت­های خود پیکربندی و مبتنی بر استانداردها و پروتکل­های ارتباطی جمعی و مشارکتی تعریف شود

که در آن "اشیا" فیزیکی و مجازی دارای شناسه­ها، صفات فیزیکی و مشخصه­های مجازی، از واسطه­های هوشمند استفاده کرده و به­طور یکنواخت و مستمر در یک شبکه اطلاعات مجتمع شده­اند.

همچنین با پیشرفت در محاسبات و ارتباطات بی­سیم، یک رویکرد جدید در اینترنت اشیاء تحت عنوان خانه­ هوشمند شناخته شده است و به سرعت تحقیقات جالب و انقلاب صنعتی مهمی را به راه انداخته است. بنابراین اینترنت اشیاء را می توان به عنوان یک شبکه فراگیر و جهانی تعریف نمود که سیستمی را برای نظارت و کنترل جهان فیزیکی از طریق جمع­آوری، پردازش و تجزیه و تحلیل اطلاعات تولید شده توسط دستگاه­های حسگر اینترنت اشیا فراهم می­آورد. این دستگاه در رابطه با سنجش و ارتباطات مانند حسگرها، دستگاه­های شناسایی فرکانس رادیویی، دستگاه­های موقعیت­یاب جهانی، حسگرهای مادون قرمز، لیزر، اسکنرها، دیسک، شبکه­های محلی بیسیم ساخته شده­اند. در واقع "همه چیز" را می توان به اینترنت متصل کرد و از این رو مدیریت از راه دور کنترل و مدیریت نمود.

اینترنت اشیا میتواند به عنوان تلفیقی از شبکه­های ناهمگن در نظر گرفت که نه تنها چالش­های امنیتی یکسانی را در شبکه­های حسگر، ارتباطات تلفن­های همراه و اینترنت به ارمغان می­آورد بلکه برخی مسائل عجیب و برجسته، مانند، مشکلات مربوط به حفظ حریم خصوصی در شبکه، چالش های احراز هویت و چالش­های کنترل و مسیریابی امن در این میان دستگاه­های ناهمگن به همراه دارد.

بنابراین مساله امینت درIOT را میتوان مهم­ترین چالش توسعه این فناوری در نظر گرفت. در این رابطه استانداردهای مختلفی در حال توسعه است؛ ولی همچنان نیازمندیهای امنیتی اینترنت اشیا و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است.

در این تحقیق، در فصل دوم ابتدا فناوری موجود در یک خانه هوشمند را بررسی کرده و در ادامه به بررسی تهدیدات امنیتی موجود در شبکه پرداخته می­شود. در فصل سوم ضمن اشاره به چالش­های امنیتی موجود در این بستر، راهکارهای مناسب معرفی می­گردد. در نهایت در فصل آخر جمع­بندی و نتیجه پایانی ارایه می­شود.

# 2 خانه هوشمند

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.

سیستم خانه هوشمند می‌تواند همانند آنچه در شکل2-1 نشان داده شده، پیکربندی شود؛ سیستم خانه هوشمند شامل سه مؤلفه اصلی سرور خانه، دروازه خانه و دستگاه‌های خانه هوشمند است:



شکل 2-1 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.

## 2-1 فناوری های موجود

در اینترنت اشیا براي ارتباط و تعامل اشیا با یکدیگر و با شبکه اینترنت فناوري هاي متفاوتی وجود دارد که در اینجا جدیدترین فناوري هاي مورد نیازبراي پیاده سازي آن را معرفی می کنیم.

### 2-1-1 Zigbee

فناوري zigbee جزء فناوري­هاي نو ظهوري می­باشد که در سال هاي اخیر رشد چشمگیري داشته است. نام zigbee از الگوي غیر ترتیبی زیگزاگی که زنبورها حین گرده افشانی دنبال می کنند، گرفته شده است.zigbee یک پروتکل مبتنی بر استاندارد IEEE802.15.4 براي کنترل و نظارت بر اهداف و سیستم­هایی است که به نرخ بالاي ارسال داده نیاز نداشته ولی هزینه پایین و جریان مصرفی کم از ملزومات آنها به شمار می­آید. در این فناوري نودها می­توانند تا زمانی که بی استفاده هستند در حالت خواب قرار بگیرند. zigbee به منظور تعریف یک تکنولوژي ساده­تر، ارزانتر و موثرتر از بلوتوث در مصرف انرژي و طول عمر، براي شبکه­هاي شخصی بیسیم بوجود آمده است. به کمک Zigbee می­توان بیش از 64000 وسیله را بطور بیسیم از طریق شبکه به هم متصل نمود.

پشته پروتکل ZigBee شامل چهار لایه است: لایه فیزیکی، لایه کنترل دسترسی رسانه لایه شبکه و لایه کاربرد. از نقطه نظر عملکرد، لایه فیزیکی فراهم کننده ارتباطات رادیویی و لایه کنترل دسترسی میانی، فراهم آورنده انتقال تک­گام مطمئن می­باشد. لایه شبکه توپولوژي­هاي پیچیده­تر و مسیریابی را معین می­کند و لایه کاربرد مشخص کننده توابع مدیریتی شبکه و دستگاه­ها و همچنین قالب پیام را مشخص می­کند.



شکل 2-2 پشته پروتکلی zigbee

بسیاري از دستگاه­هایی که تحت فناوري zigbee عمل می­نمایند، نیازمند نرخ داده ارتباطی پایینی می­باشند. نمونه بارز این موضوع، بحث روشنایی می­باشد که با در نظر گرفتن یک بیت صفر یا یک براي روشن یا خاموش نمودن آن بکار می­رود. در نتیجه با توجه به کم مصرف بودن این فناوري باتري می­تواند بالغ بر 10 سال کار کند. کاربردهاي زیر از مواردي است که zigbee براي آن توسعه داده شده است:

* هزینه پایین
* توان کم
* نرخ انتقال پایین
* امنیت
* انعطاف پذیري
* قابلیت توسعه آسان و ارزان
* قابلیت اطمینان

### 2-1-2 برچسب هوشمند

فناوري برچسب هوشمند یا RFID[[2]](#footnote-2) بیانگر سیستم­هایی است که از امواج رادیویی براي انتقال اطلاعات مربوط به هویت یک شیء استفاده می­کنند. این تگ­ها نوع پیشرفته­تري از بارکدها هستند چراکه هم قابلیت خواندن و هم قابلیت نوشتن دارند، داده­هایی که روي تگ­هاي RFID ذخیره می­شوند را می­توان تغییر داد، به روز رسانی کرد و یا حتی قفل کرد .این فناوري موفق شده است تا قابلیت و کارایی خود را به عنوان یک ابزار مقرون به صرفه در بهبود عملکرد و کاهش زمان و هزینه­هاي نیروي انسانی و منابع در بسیاري از موارد ثابت نماید.

افراد با قرار دادن تگ­هاي RFID مرتبط در محیط­هاي هوشمند، به اتوماتیکی کردن آن محیط کمک می­کنند. در یک سناریوي کلی وقتی که قسمت هاي تولیدي به پردازش می­رسند، به وسیله دستگاه برچسب خوان یک رویداد مانند خواندن شماره RFID و ذخیره آن رخ می دهد، که اطلاعات مهمی را در اختیار ما قرار می دهد.

اجزاء بکار رفته در RFID عبارتند از:

* برچسب
* برچسب خوان
* آنتن
* نرم افزار مدیریت اطلاعات

اگر بخواهیم برچسب­ها را بر اساس منبع انرژي که استفاده می­کنند، تقسیم­بندي کنیم سه نوع اصلی از آنها را خواهیم داشت. برچسب­هاي فعال، غیرفعال و نیمه غیر فعال. برچسب­هاي فعال انرژي مورد نیاز خود را از باتري همراهشان دریافت می­کنند درحالیکه برچسب­هاي غیرفعال به خودي خود داراي منبع انرژي نبوده و براي به کار افتادن باید از انرژي امواج الکترومغناطیسی منتشرشده از برچسب­خوان استفاده نمایند و البته محدوده و دامنه خواندن کمتري نسبت به برچسب­هاي فعال دارند. نوع دیگري از برچسب نیز برچسب نیمه غیرفعال می­باشدکه علاوه بر استفاده از باتري داخلی­اش، می تواند از انرژي امواج منتشر شده از برچسب­خوان نیز استفاده نماید.

### 2-1-3 ارتباطات میدان نزدیک

ارتباطات میدان نزدیک عبارتست از قابلیت ارتباطی جدید که میتوان براي اتصال امن بین دو دستگاهی که در فاصله کمی از یکدیگر قرار دارند استفاده کرد .علاوه بر مجاورت دو ابزار لازم است تا هر دوي آنها از سخت افزار مخصوصی بهره ببرند. در حقیقت NFC[[3]](#footnote-3) نسخه جدیدتري از RFID است که برد ارتباطی آن به 4 اینچ محدود شده است. این موضوع NFC را براي کاربردهاي حساس مانند موارد استفاده از کارت اعتباري)مثل پرداخت­هاي الکترونیک با استفاده از گوگل والت(و یا ورود به محل هاي امنیتی بسیار کارامد می­کند. دستگاه­هایی که از فن­اوري NFC پشتیبانی می کنند به آسانی این امکان را به کاربر می­دهند که اطلاعات مورد نظر را با یک لمس یا نزدیک کردن دستگاه خود به دستگاه دیگر ارسال یا مبادله کنند.



شکل 2-3 NFC

### 2-1-4 شبکه­های موبایلی

نسل پنجم شبکه­هاي مخابراتی موبایل با شتاب بالایی در حال انجام است. علی­رغم اینکه هنوز برخی از کشورها شبکه­ي ارتباطی خود را به نسل چهارم ارتقا نداده­اند، اما نسل پنجم در حال توسعه است و دانشمندان با هیجان بالایی در مورد آن صحبت می­کنند. استفاده از پهناي باند بالا، نرخ انتقال دادهي زیاد و تسهیل در ارتباطات مبتنی بر اینترنت همچون مکالمات ویدئویی، تنها گوشه­اي از قابلیت­هایی است که با پیاده­سازي شبکه­هاي نسل پنجم در اختیار کاربران قرار خواهد گرفت. یکی از مورادي که نیاز به پهناي باند بالا را افزایش می­دهد، مفهوم اینترنت اشیا است.

### 2-1-5 بلوتوث

بلوتوث یک فناوري بی سیم براي ارتباط کوتاه برد است که مبتنی بر استاندارد IEEE 802.15.1 می­باشد. بلوتوث کم انرژي (BLE[[4]](#footnote-4))تبدیل به یک بلوک ساختمانی کلیدي براي اینترنت اشیاء شده است. سازندگان تراشه در تلاشند تا با استفاده از فن­آوري، منجر به کاهش مصرف برق دستگاه شوند و به توسعه دهندگان براي اجراسازي آن کمک کنند .نسخه 4.2 این فناوري در سال 2014 معرفی شد و درآن برخی ویژگی­هاي اساسی براي اینترنت اشیاء اضافه شده است. سرعت و امنیت بلوتوث 4.2 نسبت به نسخه­هاي قبلی بهینه شده و در عین حال توان مصرفی کمتر است. این ویژگی­ها بلوتوث کم انرژي را به رقیبی جدي در برابر فناوري zigbee تبدیل کرده است. یکی از ویژگی­هاي اساسی استاندارد بلوتوث این است که نسخه جدید، با نسخه هاي قبلی سازگاري دارند. بلوتوث بر خلاف فرستنده مادون قرمز و گیرنده آن که می­بایست در مقابل هم قرار بگیرند تا ارسال اطلاعات صورت گیرد، می­تواند در صورت وجود داشتن مانعی در بین راه، انتقال اطلاعات را به درستی انجام دهد.

### 2-1-6 Z-Wave

Z-Wave یک پروتکل ارتباطی بی سیم است که توسط زنسیس طراحی شده است و توسط ائتلاف Z-Wave براي اتوماسیون در محیط­هاي مسکونی و تجاري کم تراکم ترویج شده است. هدف اصلی Z-Wave ارایه یک انتقال مطمئن از پیام هاي کوتاه از یک واحد کنترل به یک یا چند گره دیگر در شبکه است. Z-Wave داراي معماري پنج لایه­اي است که عبارتند از: لایه فیزیکی، لایه مک ، لایه انتقال، لایه مسیریابی و لایه کاربرد. لایه مک مربوط به این فناوري، مکانیسمی را تعریف می ­ند که امکان ارسال فریم را در زمان در دسترس بودن کانال فراهم می­کند. در صورتی که کانال در دسترس نباشد، انتقال به زمانی دیگر موکول می­شود و این زمان به صورت تصادفی است. لایه انتقال ارتباط بین دو گره متوالی را مدیریت می­کند و این لایه یک مکانیسم انتخابی براي انتقال مجدد را براساس تصدیق فراهم می­کند. Z-Waveدو نوع از تجهیزات را تعریف می­کند: کنترل کننده­ها و پیروها. کنترل­کننده­ها دستورات را صادر و به پیروها ارسال می­کنند و تجهیزات پیرو دستورات را اجرا می­کنند.

.

شکل 2-5 پشته پروتکلی Z-Wave

## 2-2 تهدیدات خانه هوشمند

خانه­های هوشمند از مؤلفه­های متعددی تشکیل شده­اند؛ این مؤلفه­ها همواره در معرض تهدیدات مختلفی قرار دارند. حملات خانه­های هوشمند به هفت گروه تقسیم شده اند که عبارتند از:

١- **حملات فیزیکی:** به دستکاری فیزیکی دستگاه­ها اطلاق می­شود؛ این حملات می­تواند 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 می­دهد.

٢- **خسارات ناخواسته (تصادفی):** ممکن است از اطمینان نادرست و نابجا به افراد و آشنایان یا اشتباهات شخصی (مدیریتی، طراحی، عملکرد وغیره) ناشی شود؛ می­تواند مراتب جبران­ناپذیری 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 می­شود، بلکه نشر اطلاعات را با خود به همراه دارد؛ در واقع باعث حذف اطلاعات حیاتی می­شود.

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

۶- **استراق­سمع، ممانعت و سرقت:** سوءاستفاده ناهنجار به تهدیدات سایبری و نیز حریم­شخصی مربوط می­شود؛ این دو مقوله به عنوان تهدیدات امنیتی در نظر گرفته می­شود؛ 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 داده­های خصوصی یا ازدست­دادن کنترل یک دستگاه خواهد شد.

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

# 3 چالش­ها و راهکارها

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 حریم­خصوصی به­عنوان دو مولفه اساسی و مهم در حوزه اینترنت اشیاء نقش پررنگی در این کاربردها خواهند که در ادامه به این دو مهم می­پردازیم.

## 3-1 چالش امنیت اطلاعات

امنیت اصلی­ترین نگرانی شبکه­هایي است که در مقیاس بزرگ پیاده­سازي می­شوند. دنیاي دیجیتال، با داده­هاي شخصی و اشتراکی و ثبت­شده توسط افراد اشباع شده است و نگرانی­هایی را در زمینه امنیت و حفاظت از اطلاعات افراد و دولت­ها فراهم کرده است. همچنین مشکلات ناشی شده از انتقال و پردازش داده­هاي ناخواسته، موجب نگرانی­هاي 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 می­تواند زمینه سرقت از خانه را فراهم کند. به­طور کلی، سرویس­هاي امنیتی که در این حوزه قرار است ارائه شوند باید ویژگی­هاي محرمانگی، تمامیت و دسترسی­پذیری را فراهم نمایند. در ادامه به بررسی این عناصر می­پردازیم:

### 3-1-1 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.

### 3-1-2 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 می­کند که پیام­هاي قدیمی­تر تکرار نمی­شوند. این امر به جهت تضمین کانال ارتباطی در مقابل حملات تکرار مهم است.

**صحت:** این ویژگی نیز تضمین کننده­ی درستی اطلاعات در تمامی مراحل ارتباط می­باشد.

### 3-1-3 دسترسی پذیری

اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کار­کردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سیستم‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار، و ارتقاء سیستم در دسترس باقی می‌ماند. یکی از راه­های از دسترس خارج کردن اطلاعات و سیستم اطلاعاتی درخواست‌های زیاد از طریق خدمات از سیستم اطلاعاتی است که در این حالت چون سیستم توانایی و ظرفیت چنین حجم انبوه خدمات­دهی را ندارد از سرویس دادن بطور کامل یا جزیی عاجز می‌ماند.

## 3-2 چالش حریم خصوصی

مفهوم حریم­خصوصی همواره همراه با امنیت به کار برده شده است، اما در این تحقیق مناسب است که توجه جداگانه­اي به آن شود؛ چرا که در اینترنت اشیاء اطلاعات خصوصی بیشتري نسبت به وضعیت کنونی بر روي شبکه قرار می­گیرد. حریم خصوصی شامل قابلیت پنهان نگهداشتن اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می­افتد است. طبیعت اشیاء متصل و کاربردهاي گسترده، متنوع و همه جا حاضر اینترنت اشیاء و از همه مهم­تر، تأثیر این اشیاء در بالابردن کیفیت زندگی باعث نفوذ روزافزون آنها در زندگی روزمره­ي انسان­ها می­گردد؛ از طرفی دیگر، چنین سیستم­هایی که فعالیت­هاي روزانه­ي افراد را جمع­آوري و ثبت می­نمایند می­توانند به آسانی به عنوان سیستم­هاي جاسوسی و استراق­سمع توزیع شده مورد استفاده قرار گیرند. به دلیل آنکه اطلاعات مربوط به فعالیت­هاي روزانه­ي کاربران (براي نمونه مسیرهاي مسافرتی، عادت­هاي خریدکردن و غیره) توسط بسیاري از انسان­ها در زمره اطلاعات شخصی و محرمانه در نظر گرفته می­شوند که نباید فاش شوند، حفظ حریم خصوصی یکی از ملزومات کاربردهاي همه­جاحاضر محسوب می­گردد . هرچند بسیاري از مردم در ارتباط با موج جدید فن­آوري که در حال آمدن است یک جنبه احتیاطی در پیش گرفته­اند؛ اما واقعیت این است که این دستگاه­ها به گونه­اي طراحی شده­اند تا اطلاعات شخصی زندگی انسان را با بیشترین جزییات ممکن، جمع­آوري کنند. برای مثال یکی از این اطلاعات خصوصی، سبک زندگی افراد است؛ این که چه ساعاتی را در خانه به سر می­بریم، به کجا مسافرت می­کنیم، با چه کسانی معاشرت می­کنیم، چه فیلم­هایی تماشا می­کنیم و حتی این که چه غذایی می­خوریم. کمی خطرناک به نظر می­رسد، که ما به سرعت اقدام به طراحی و بازیابی راه­حل­هایی با هدف بهبود زندگی روزمره شهروندان داشته باشیم؛ به طوريکه برخی از جنبه­هاي حریم­خصوصی یا امنیت اطلاعات را در این زمینه نادیده بگیریم. ضمن اینکه فن­آوري­هاي کلیدي اینترنت اشیا هنوز به بلوغ خود نرسیده­اند و همچنین تحقیقات و کاربردهاي اینترنت اشیا در مراحل اولیه خود هستند. پس براي حضور و فراگیر شدن اینترنت اشیا در زندگی روزمره، امنیت و حریم­خصوصی باید به طور جدي­تري در نظر گرفته شود.

## 3-3 راهکارها

برای ارایه پاسخ مناسب به دغده­های اصلی در خانه هوشمند، راه­حل­های زیر ارایه می­شود:

### ****3-3-1 احراز هویت****

دستگاه­ها باید در برابر سیستم­های دیگر تصدیق شوند و برای این منظور به یک شناسه منحصر بفرد و کلمه عبور نیاز دارند. دستگاه­های هم چون تلویزیون هوشمند یا دوربین مدار بسته و یا دستگاه­های ویدئویی و تجهیزات آنتن ماهواره می­توانند در این زمینه مورد استفاده قرار گیرند. در هنگام به روز رسانی یک دستگاه باید حتما احراز هویت صورت پذیرد و سرورهای داخلی و دستگاه های مجاز بازیابی شوند. برای جلوگیری کنترل غیرمجاز با استفاده از پروتکل­های امنیتی (مانند پروتکل­هایSSLTLS,) کاربران تصدیق هویت می­شوند و با این روش امکان کنترل غیرمجاز از بین می­رود.

### ****3-3-2 رمزنگاری****

دستگاه اینترنت اشیا مجریان اعتماد مبتی­ بر سخت­افزار[[5]](#footnote-5) می­باشند ولی همزمان از اعتماد بوسیله فرآیندهای خاصی استفاده می­کنند تا بدین شکل بتوانند مطالب خود را به صورت خصوصی نگهدارند و در برابر حملات نرم افزارهای غیرقابل اطمینان از آنان محافظت نمایند. برای حفظ محرمانگی اطلاعات شخصی و رعایت حریم­خصوصی، تمامی اطلاعات به­صورت رمزشده ذخیره و یا تبادل می­شود. با این روش اطلاعات حساس و مهم شخصی در مقابل دسترسی غیرمجاز محافظت می­شوند. به­عنوان مثال اطلاعات موجود بر روی تراشه های داده­های متصل به اینترنت اشیا می­تواند مورد سرقت قرار گیرد برای همین با استفاده از رمز گذاری و رمز گشایی از اطلاعات محافظت می­شود. دستگاه­های اینترنت اشیا بوسیله رمزگذاری و استفاده از پروتکل های مانند TSL به انجام تراکنش های حساس مانند تراکنش های مالی می پردازند. TLS می­تواند مانع حمله مرد میانی شود و برای موارد محرمانه بسیار پرکاربرد خواهد بود.

### 3-3-3 دیواره­ آتش[[6]](#footnote-6)

یکی از چالش اصلی حملات منع­سرویس(DOS[[7]](#footnote-7)) می­باشد، که مهاجم با مراجعات مداوم عملا سیستم را مختل می­کند. با این روش از دستیابی غیرمجاز به یک سیستم رایانه جلوگیری می‌کنند. در برخی از این [نرم‌افزارها](https://fa.wikipedia.org/wiki/%D9%86%D8%B1%D9%85%E2%80%8C%D8%A7%D9%81%D8%B2%D8%A7%D8%B1)، برنامه‌ها بدون اخذ مجوز قادر نخواهند بود از یک رایانه برای سایر رایانه‌ها، داده ارسال کنند.

# 4 نتیجه­گیری

در این تحقیق ابتدا به مزایای خانه هوشمند را بررسی و فناوری­های که در خانه هوشمند مورد استفاده قرار می­گیرد را معرفی کردیم. و ادامه ضمن اشاره به مخاطرات استفاده از خانه هوشمند، به چالش­های اصلی که شامل امنیت و حریم­خصوصی است، اشاره کردیم. برای مقابله با تهدیدات و مخاطرات امنیتی، راه­حل­ احراز هویت برای حفظ تمامیت، رمزنگاری برای حفظ محرمانگی و حریم­خصوصی، همچنین استفاده از دیواره آتش برای حفظ دسترس­پذیری پیشنهاد شد. البته امنیت در خانه هوشمند یک موضوع نسبی است و بسته به اهمیت و حساس بودن اطلاعات می توان راهکارهای مختلفی ارایه کرد.

# 5 منابع

* **I**oT Security: Ongoing Challenges **and** Research Opportunities. Zhang, Zhi Kai and Yi Cho, Michael Cheng. s.l. : IEEE, 2014.
* *Internet of Things (IoT): A vision, architectural elements, and future directions.* Gubbi, Jayavardhana, et al., et al. s.l. : elsevier, 2013, Future Generation Computer Systems.
* *Survey on secure communication protocols for the Internet of Things.* K.-T. Nguyen, M. Laurent, N. Oualha,. s.l. : Ad-hoc Networks, 2015, pp. 1-15.
* Song, Yuanjun. Security in Internet of Things. Stockholm, Sweden : KTH Information and Communication Technology, 2013.

1. Internet Of Things [↑](#footnote-ref-1)
2. Radio Frequency Identification [↑](#footnote-ref-2)
3. Near Field Communication [↑](#footnote-ref-3)
4. Bluetooth Low Energy [↑](#footnote-ref-4)
5. Hardware-based [↑](#footnote-ref-5)
6. Firewall [↑](#footnote-ref-6)
7. Denial Of Service [↑](#footnote-ref-7)