پروژه قفل های هوشمند

سینا انوری نژاد

درس : هوش مصنوعی سکشن چهارشنبه

استاد : عصایی معمم

فهرست

قفل هوشمند را می توان به عنوان جانشین مدرن قفل سنتی در نظر گرفت. این مقاله مروری بر فناوری‌های مختلف قفل هوشمند ارائه می‌کند. سیستم قفل هوشمند که امروزه در بسیاری از خانه‌ها و دیگر ساختمان‌های تجاری مورد استفاده قرار می‌گیرد، رویکردی نوآورانه است که با معایب قابل‌تحمل آن، مزایای کاربرپسند بسیاری را ارائه می‌کند.

1. معرفی

امروزه فناوری تأثیر بیشتری بر بسیاری از جنبه های زندگی ما گذاشته است. سیستم اتوماسیون خانگی یک شبکه کامپیوتری و خودکار از وسایل الکترونیکی است که برای نمایش کنترل بر لوازم خانگی و نظارت کارآمد بر آنها ساخته شده است. یکی از برنامه های کاربردی بلادرنگ در حال ظهور که بسیار مورد توجه قرار گرفته است، سیستم امنیت خانه است. سیستم قفل هوشمند چارچوبی نوظهور است که به دلیل راحتی و قیمت مناسب به تدریج جایگزین قفل های سنتی می شود.

قفل هوشمند یک دستگاه الکترومکانیکی است که عملیات قفل/باز کردن قفل را با استفاده از پروتکل های بی سیم انجام می دهد. شبکه‌های سیمی قبلاً با ارتباطات بی‌سیم جایگزین شده‌اند، زیرا تمایل دارند با نصب آسان انعطاف‌پذیری و توسعه‌پذیری بیشتری را فراهم کنند. قفل هوشمند به صورت بی سیم توسط یک کلید رمزنگاری در احراز هویت کار می کند که فقط به پرسنل مجاز دسترسی دارد. با پیشرفت تکنولوژی و تحقیقات، مکانیسم های امنیتی قوی تری توسعه یافته است. دسترسی به سیستم قفل هوشمند با استفاده از یک سیستم بیومتریک اثر انگشت باعث افزایش سطح امنیت می شود. برخی از قفل های هوشمند عملکرد دوربین را برای افزایش امنیت خود اضافه کرده اند. قفل هوشمند به طور قابل قبولی برجسته ترین جزء یک خانه متصل هوشمند است.

قفل هوشمند می تواند برای اهداف امنیتی تجاری (دفاتر، هتل ها، مراکز خرید و غیره) یا مسکونی (به عنوان مثال، امنیت خانه) استفاده شود. این به اشخاص ثالث اجازه می دهد تا با استفاده از یک کلید مجازی که از طریق Wi-Fi، برنامه تلفن همراه، حسگرهای مجاورت، دستگاه های دارای BLE و غیره به گوشی هوشمند گیرنده ارسال می شود، به قفل دسترسی داشته باشند. ادغام Wi-Fi در قفل هوشمند می تواند چندین مزیت داشته باشد. از جمله به روز رسانی های OTA وضعیت تمام وقت است.

تعداد کاربران گوشی های هوشمند به سرعت در حال افزایش است و استفاده از آن فوق العاده است. استفاده از گوشی هوشمند یا ابزارهای دیگر برای نظارت و کنترل امنیت ساختمان های خانگی یا تجاری کار را بسیار آسان می کند. با این حال، می‌توان به راحتی کلیدها را به جای گم کردن گوشی جا انداخت، از این رو، سیستم قفل هوشمند از این واقعیت به نفع خود استفاده می‌کند. علاوه بر این، برای اطمینان از امنیت بالا در هنگام استفاده از تلفن های هوشمند، می توان از رمزگذاری استاندارد AES استفاده کرد که به سختی به آن نفوذ کرد.

نسخه‌های مختلفی از قفل‌های هوشمند توسعه یافته‌اند و نیاز به بهبود امنیت، حوزه تحقیقاتی گسترده‌ای را ارائه می‌دهد. در این مقاله، تعداد کمی از نسخه‌های قفل هوشمند با ویژگی‌های برجسته‌شان توضیح داده شده‌اند.

2. اجزای اساسی

2.1 قفل الکترومکانیکی

برای عملکرد قفل هوشمند مانند قفل های سنتی نیاز به قفل و کلید دارد. در اینجا، قفل الکترومکانیکی عملیات قفل و باز کردن قفل را با استفاده از یک کلید رمزنگاری انجام می دهد

که دستورالعمل ها را با استفاده از یک پروتکل بی سیم دریافت می کند. این یک پیچ بسته الکترونیکی است که بر روی هر مکان دلخواه (معمولاً درب خارجی) نصب می شود.

2.2 کلید رمزنگاری

یک کلید رمزنگاری یا یک گوشی هوشمند یا یک جا کلیدی است که برای باز کردن خودکار درب احراز هویت می شود و با اجرای یک الگوریتم رمزگذاری تولید می شود. کلید مورد نیاز برای باز کردن قفل در حال حاضر لزوماً یک گوشی هوشمند نیست. فناوری‌ها تا حد زیادی تکامل یافته‌اند که اکنون عملیات قفل و باز کردن قفل را از طریق دستگاه‌های فعال BLE، حسگرها و پروتکل‌های مختلف دیگر مانند ZigBee و موارد مشابه، که در این مقاله مورد بحث قرار می‌گیرند، پیاده‌سازی می‌کنند.

3. حالت های کار

3.1 برنامه های موبایل/وب

قفل های هوشمند چسبانده شده دسترسی کاربران مجاز خود را از طریق کلیدهای دیجیتال فراهم می کند. کلیدهای دیجیتال صادر شده بسیار رمزگذاری شده اند و می توانند از طریق سطوح مختلف از جمله مالک، مقیم، مهمان مکرر و مهمان موقت دسترسی داشته باشند [2]. این قفل‌های هوشمند پس از نصب به کاربر نیاز دارند تا به برنامه تلفن همراه/وب مرتبط وارد شود تا احراز هویت شوند. امنیت و حریم خصوصی به عنوان یک نگرانی اصلی در نظر گرفته می شود. کاربران احراز هویت شده می توانند از طریق برنامه از هر نقطه با اتصال به اینترنت قوی به قفل هوشمند دسترسی داشته باشند. فرآیند مجوز با استفاده از یک پروتکل بی سیم و یک کلید رمزنگاری اجرا می شود. این برنامه‌ها به گونه‌ای طراحی شده‌اند که در صورت تلاش

برای باز کردن قفل یا دسترسی غیرمجاز، به دستگاه تلفن همراه کاربر هشدار می‌دهند. مالک می‌تواند هر زمان که بخواهد از طریق اشتراک‌گذاری کلیدهای مجازی از طریق پروتکل‌های پیام‌رسانی استاندارد (ایمیل، پیامک) به افراد مورد اعتماد اجازه دهد یا آن را لغو کند. دسترسی به مالک برای مشاهده تمام سیاههای دسترسی قفل و نظارت بر کل عملکرد آن فراهم شده است. کلیدهای مقیم دسترسی دائمی به خانه/ساختمان دارند، در حالی که کاربر تکراری طبق تنظیم مالک، دسترسی برنامه ریزی کرده است. مهمان موقت نیز دسترسی مشابهی در پنجره دسترسی کوتاه مدت دارد

بسیاری از قفل‌ها از جفت شدن با دستگاه‌ها از طریق اتصال بلوتوث پشتیبانی می‌کنند اما اکنون برای داشتن یک جفت قوی و طول عمر اتصال در سراسر ساختمان، بسیاری از اتصال Wi-Fi قوی نیز حمایت می‌کنند

3.2 حسگرها

چندین دستگاه اتوماسیون خانگی وجود دارند یا در حال حاضر در حال توسعه هستند که به مکانیسم های خودکار برای نظارت و کنترل دستگاه هایی که بخشی از سیستم امنیتی خانه هستند اجازه می دهند. در این مقاله، قفل هوشمند نگرانی اصلی است که نقش کلیدی در تضمین امنیت بالا برای کاربران در برابر سرقت یا سایر فعالیت‌های مجرمانه ایفا می‌کند که ممکن است امنیت یا حریم خصوصی آنها را مختل کند. ایده تعبیه سنسورها در قفل هوشمند، راه آسانی را برای قفل کردن یا باز کردن قفل درب تضمین می کند. حسگرهایی مانند PIR، حسگر نوری و مانند آن برای خواندن و تشخیص اشیاء استفاده می‌شوند.

رایج ترین سنسور حرکتی که در قفل های هوشمند استفاده می شود، سنسور PIR (Passive Infrared) است. سنسور PIR نور مادون قرمز تابش شده از اجسام را با کمک نیمه هادی

های الکترونیکی اندازه گیری می کند [1]. همه حیوانات خونگرم تابش IR را القا می کنند. این حسگرها شامل یک ماده فیلم پیرو الکتریک است که با تولید الکتریسیته به تشعشعات مادون قرمز پاسخ می‌دهد که زنگ هشدار سارق را فعال می‌کند. آنها وسیله ای موثر برای سیستم امنیتی خانه هستند زیرا انرژی کمتری مصرف می کنند و تقریباً طولانی مدت هستند.

یک سنسور PIR را می توان با یک سنسور مایکروویو ترکیب کرد تا در مناطق مختلف طیف عمل کند. سنسور مایکروویو پالس های مایکروویو را برای تشخیص انعکاس از اجسام متحرک ساطع می کند. بنابراین، چنین حسگرهای حرکتی با فناوری دوگانه، احتمال بسیار کمتری برای ایجاد هشدارهای کاذب دارند. بسیاری از پیشرفت‌های اخیر ترکیب دوربین‌های فیلمبرداری را با پردازش سیگنال پیشرفته که توسط حسگرهای حرکتی کنترل می‌شوند، توصیه می‌کنند.

چندین حسگر نوری که بیشتر برای تشخیص بدون تماس استفاده می شوند در قفل های هوشمند گنجانده شده اند. یک حسگر نوری مقدار فیزیکی نور را ارزیابی می کند و آن را به شکل قابل خواندن برای دستگاه اندازه گیری یکپارچه بر اساس حسگر مربوطه تبدیل می کند. احراز هویت بیومتریک به شناسایی انسان ها با ویژگی ها یا صفات آنها اشاره دارد [4]. در حین اجرای احراز هویت بیومتریک برای قفل‌های هوشمند، کاربر باید انگشت خود را از طریق حسگر نوری وارد کند که الگوی تصاویر انگشت را تولید می‌کند که با الگوهای مشابه از کتابخانه مقایسه می‌شوند. تأیید اثر انگشت شامل تولید الگوهای اثر انگشت است که به عنوان تصاویر یا الگوریتم‌های بیومتریک ذخیره می‌شوند. این کار تطبیق و تأیید اثر انگشت را با اثر انگشت های از پیش تعیین شده و ذخیره شده در کتابخانه ها آسان تر می کند. این سیستم سطوح افزایش یافته ای از احراز هویت کاربر را ارائه می دهد تا فقط برای کاربران مجاز دسترسی داشته باشد.

3.3 بلوتوث

بلوتوث به عنوان یک راه حل شبکه بی سیم در حوزه شبکه های خانگی در نظر گرفته می شود. بلوتوث یک راه حل ابتدایی، مقرون به صرفه و مطمئن را ارائه می دهد که استفاده از آن را در دستگاه های تلفن همراه بسیار گسترده کرده است. بلوتوث یک استاندارد فناوری بی سیم کوتاه برد است که هدف آن تبادل ساده داده ها بین دستگاه ها از طریق امواج رادیویی UHF با طول موج کوتاه در شبکه است [5]. با کمک سیستم بلوتوث، کاربر می تواند سیگنال هایی را به درب ارسال کند تا با هر دستگاه BLE موجود (تبلت، گوشی هوشمند و غیره) قفل یا باز شود. این فناوری به مدیر یا مالک این امکان را می‌دهد که سیگنال‌های دیجیتالی را به سایر افراد قابل اعتماد ارسال کند تا دسترسی به دستگاه‌های مجهز به NFC را فراهم کند.

به طور کلی، کاربران برای جلوگیری از دسترسی غیرمجاز و نظارت بر عملکرد سیستم امنیتی، ملزم به نصب برنامه تلفن همراه قفل بر روی تلفن هوشمند/تبلت خود هستند تا یک حساب کاربری تأیید شده داشته باشند. پس از نصب، دستگاه تلفن همراه از طریق یک کانال بی‌سیم محلی (بلوتوث کم انرژی) با قفل جفت می‌شود. این قفل ها به دستگاه تلفن همراه کاربر بستگی دارد که به عنوان یک دروازه اینترنتی عمل می کند که اطلاعات را بین سرور و دستگاه تلفن همراه در محدوده BLE قفل منتقل می کند. هنگامی که دستگاه ها جفت شدند، هر زمان که در محدوده BLE دستگاه ها متصل می شوند، و کاربر می تواند از تمام عملکردهای موجود برای کنترل قفل استفاده کند. دستگاه‌های دارای BLE می‌توانند بسته به کلاس دستگاه‌های بلوتوث، در محدوده 10 تا 100 متری با سرعت حداکثر 3 مگابیت بر ثانیه کار کنند. آنها روی باند فرکانسی 2.4 گیگاهرتز کار می کنند [6]. همچنین ارسال کلیدهای الکترونیکی از طریق اپلیکیشن موبایل را تسهیل می کند و قابلیت تشخیص حضور کاربر از دیگر ویژگی هایی است که استفاده از آن را افزایش داده است.

3.4 وای فای

Wi-Fi به خانواده فناوری های شبکه بی سیم گفته می شود که اینترنت پرسرعت و اتصال شبکه را فراهم می کند. از امواج رادیویی برای اطمینان از تبادل آسان، ایمن و سریع داده بین دستگاه ها از طریق شبکه استفاده می کند. استفاده از تلفن های هوشمند به سرعت افزایش یافته است و برنامه های مختلف نیاز به یک اتصال اینترنتی قوی دارند که با داشتن یک اتصال Wi-Fi قوی قابل ارائه است. در حال حاضر از تلفن های هوشمند به عنوان ابزاری برای کنترل فناوری خانه های هوشمند نیز استفاده می شود که با سرعت بسیار بالایی در حال رشد است.

سیستم قفل هوشمند نیاز به اتصال به یک اتصال LAN خانگی دارد که کاربر به آن متصل است. گفته می شود که اتصال محلی (LAN) که می تواند توسط یک روتر ساده ایجاد شود، ضروری ترین و کلیدی ترین جزء سیستم قفل هوشمند است که بر اساس امنیت Wi-Fi ساخته شده است. سیستم قفل هوشمند به گونه‌ای طراحی شده است که از یک سیستم کنترل مرکزی تشکیل شده است که عملکردهایی مانند خواندن دستورات، ذخیره داده‌ها، عملیات قفل/باز کردن قفل و سایر عملکردهای حیاتی برای سیستم را انجام می‌دهد. یک برنامه تلفن همراه تمام کنترل ها را در اختیار کاربر قرار می دهد تا سیستم قفل را همانطور که می خواهد نظارت کند. تمام کلیدهای دیجیتال را ذخیره می کند و کاربر همچنین می تواند کلیدهای موقت را برای مهمانان یا هر یک از افراد مورد اعتماد ایجاد و ارسال کند [3]. این سیستم فرآیند نصب آسانی دارد و با بهره برداری از آن، با حداقل پیچیدگی و امکان سنجی قوی، چشم انداز سیستم قفل بهتری را فراهم می کند [3].

Locks	Interaction Model	Devices	Interface
Kevo	Touch-to-unlock	smartphone, key fob	Mobile app, website
August	button in mobile app; automatic unlocking	smartphone	Mobile app
Lockitron	button in mobile app or web interface	Smartphone, website	Mobile app, website
Dana	button in mobile app; automatic unlocking	Smartphone	Mobile app, website

4. چند نمونه از قفل هوشمند

4.1 تئودور

قفل Teodoor یک قفل با فناوری بلوتوث قابل اعتماد است که از آخرین فناوری های رمزگذاری درجه نظامی استفاده می کند. با کمک پردازشگر رمزنگاری خود که امکان استفاده از الگوریتم های رمزگذاری ایمن تری را فراهم می کند که زمان پردازش را کاهش می دهد، همچنین مصرف انرژی را کاهش می دهد. انرژی آن توسط باتری های لیتیومی قابل تعویض تامین می شود. همچنین در حالت هندزفری کار می کند که در آن درب را با شناسایی صاحب خود قفل/باز می کند. قفل Teodoor عملکردهای دسترسی دقیق برنامه ریزی شده را تسهیل می کند و همچنین راهی آسان و سریع برای ارائه حقوق دسترسی به افراد مورد اعتماد توسط مالک ارائه می دهد. [7]

Kevo 4.2

قفل‌های هوشمند Kevo توسط Kwikset تولید می‌شوند که یک تولیدکننده قفل و قفل آمریکایی است که متعلق به گروه سخت‌افزار و Home Improvement Spectrum Brands است. قفل هوشمند Kevo از سطوح مختلف رمزگذاری درجه نظامی برای افزایش امنیت قفل هوشمند استفاده می کند. احراز هویت دو مرحله ای امنیت بیشتری را به سیستم قفل هوشمند اضافه می کند. در صورت گم شدن تلفن، می‌توانید به صورت آنلاین به حساب Kevo خود وارد شوید تا کلیدهای الکترونیکی را به حالت تعلیق درآورید و تلفن‌های خود را غیرفعال کنید. اکثر قفل‌های Kevo تلفن هوشمند و قفل را با استفاده از بلوتوث به هم متصل می‌کنند. این امکان ایجاد کلیدهای الکترونیکی را فراهم می کند که می توانند با افراد مورد اعتماد به اشتراک گذاشته شوند. یکی دیگر از ویژگی های مهم Kevo fob است که در غیاب گوشی هوشمند قابل استفاده است. خانواده Kevo شامل قفل Kevo Contemporary است که راحتی لمسی برای باز کردن را فراهم می کند، قفل سنتی Kevo، قفل Kevo Convert که دارای کیت تبدیل قفل هوشمند است، Kevo plus که دسترسی از راه دور را فراهم می کند، و Kevo fob. [8]

4.3 اوت

آگوست قفل هوشمند Wi-Fi خود را راه اندازی کرده است که دسترسی از راه دور به قفل/باز کردن درها، اعطای کلیدهای مجازی به افراد مورد اعتماد یا استفاده از دستیار صوتی برای کنترل آن را فراهم می کند. با وای فای داخلی خود، برای اتصال به پل نیازی ندارد. سیستم قفل هوشمند امکان جفت شدن با گوشی های هوشمند یا سایر دستگاه های بالقوه را برای فعال کردن دسترسی بدون کلید فراهم می کند. لازم است مالک یک کاربر مجاز در برنامه آگوست باشد که یک رابط کارآمد برای نظارت و کنترل قفل و بررسی وضعیت و هرگونه به روز رسانی ارائه می دهد.

عملکرد کتاب مهمان برای پیگیری تمام داده‌های دسترسی اخیر یک ویژگی مهم است که در آن تعبیه شده است زیرا مالک را در مورد تمام فعالیت‌ها آگاه می‌سازد تا خانه‌ای حتی ایمن را به روشی هوشمندتر فراهم کند. سیستم قفل هوشمند تا آگوست (نسل اول یا نسل دوم و غیره) از استانداردهای رمزگذاری قوی استفاده می کند که شامل فناوری های رمزگذاری BLE و TLS در برنامه های تلفن همراه است [9].

5. مزایا

نصب قفل هوشمند برای افزایش امنیت منازل یا هر ساختمان تجاری بسیار راحت و آسان ساخته شده است. همچنین، استانداردهای امنیتی آنها را به یک جایگزین قابل اعتماد برای قفل های معمولی تبدیل می کند. این فناوری یک سیستم قفل/باز کردن خودکار را اجرا می‌کند که می‌تواند توسط گوشی‌های هوشمند یا خواننده‌های بیومتریک فعال شود که معضل قفل شدن یا نابجا بودن leyها را از بین می‌برد. ویژگی کلیدی ارائه دسترسی انحصاری به کاربران مجاز باعث افزایش امنیت می شود و این قفل ها به راحتی قابل دستکاری نیستند. قابلیت شناسایی متجاوزان یا هر شخص و ثبت فعالیت های آنها در محدوده جغرافیایی تعیین شده موجود در بسیاری از سیستم های قفل هوشمند، خانه هوشمند بسیار مطمئن و مطمئنی را تضمین می کند. این به عنوان یک ابزار ایده آل برای تضمین امنیت در ساختمان های تجاری و محیط های کاری عمل می کند زیرا این سیستم فقط به پرسنل مجاز اجازه می دهد تا کنترل دسترسی به یک منطقه خاص را داشته باشند. علاوه بر داشتن فرآیند نصب آسان، فعال سازی و دسترسی به قفل را آسان تر می کند زیرا آن را به گوشی های هوشمند محدود نمی کند. نسخه های پیشرفته از جا کلیدی و سایر دستگاه های BLE تشکیل شده است که می توانند به طور همزمان به قفل ها دسترسی داشته باشند. با وجود داشتن شناسه بیومتریک یا دسترسی گوشی هوشمند برای قفل/باز کردن قفل، بسیاری از قفل ها اکنون صفحه کلیدی برای ایجاد پین یا رمز عبوری ارائه می دهند که کاربر مجاز را شناسایی می کند.

6. معایب

عیب اصلی قفل های هوشمند زمانی است که صاحب آن سعی می کند با یک گوشی هوشمند با باتری کم به قفل دسترسی پیدا کند. در شرایط باتری کم، گوشی هوشمند بسیاری از ویژگی‌های آن غیرفعال است و ممکن است برای انجام عملکرد قفل/باز کردن قفل آن به اندازه کافی کارآمد نباشد زیرا ممکن است باتری را بیشتر تخلیه کند. همچنین، در هنگام خاموشی واحد کنترل یا هر گونه شرایط معیوب، کاربر به دلیل عدم دسترسی به سیستم، سرگردان می شود. مانند هر نرم افزاری، مزاحمان می توانند از آسیب پذیری های آن سوء استفاده کرده و دستگاه را دستکاری کنند. بنابراین سازندگان تلاش‌های مداومی برای انتشار به‌روزرسانی‌های منظم انجام می‌دهند که استانداردهای رمزگذاری آنها را بهبود می‌بخشد تا نفوذ کاربران غیرمجاز را سخت‌تر کرده و امنیت سیستم را افزایش دهد.

7. پیاده سازی

پروژه ما به ساخت یک قفل بیومتریک اقتصادی و کم‌هزینه با استفاده از حسگر اثر انگشت موجود در تلفن هوشمند کمک می‌کند. اولین قدم ایجاد یک برنامه با استفاده از Arduino IDE و آپلود آن در یک میکروکنترلر است، در این مورد Arduino Nano است. این برنامه یک لینک ارتباطی بین نانو برد و گوشی هوشمند از طریق بلوتوث ایجاد می کند. این لینک ارتباطی به میکروکنترلر در اجرای دستورات ارسال شده توسط گوشی هوشمند کمک می کند. اولین گام در توسعه برنامه ایجاد یک متغیر رشته ای است که شناسه منحصر به فرد دستگاه را برای قفل ذخیره می کند و سپس کتابخانه سروو اضافه می شود. ایده اصلی پشت کار قفل درب در شناسه ارسال شده توسط تلفن اندرویدی با استفاده از برنامه توسعه یافته نهفته است. برای دریافت داده های ارسال شده توسط گوشی از ماژول بلوتوث HC-05 با نرخ باود پیش فرض 9600 استفاده می کنیم. این ماژول با همان نرخ باود به برد نانو آردوینو (میکروکنترلر) متصل می شود (شکل 1 را ببینید).

```
#include <Servo.h>
String reads;


Servo myservo;

void setup() {
  Serial.begin(9600);
  myservo.attach(9);
  // put your setup code here, to run once:

}
```

مرحله بعدی ایجاد یک تابع حلقه است که شناسه دستگاه ارسال شده از طریق بلوتوث را ذخیره می کند. این در رشته "خوانده" ذخیره می شود. سپس، یک "شرط اگر" برای تأیید شناسه دستگاه ارسال شده توسط بلوتوث استفاده می شود. هنگامی که اثر انگشت کاربر توسط گوشی هوشمند اسکن می شود، ابتدا با اثر انگشت موجود در برنامه احراز هویت می شود. پس از احراز

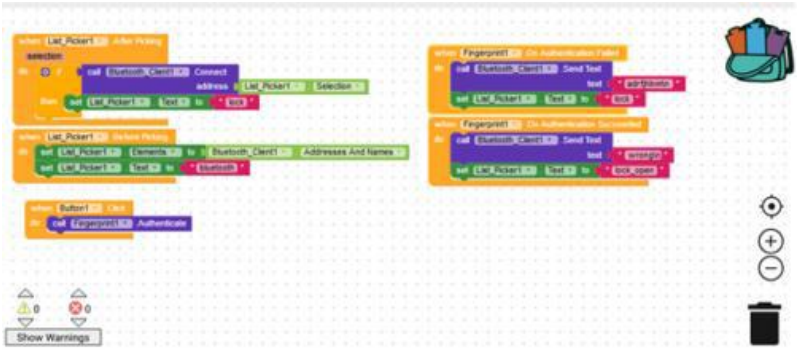
هویت موفق، برنامه شناسه دستگاه را به برد آردوینو نانو ارسال می کند. در صورتی که این شناسه با شناسه موجود در آردوینو مطابقت داشته باشد، در آن نقطه سروو موتور قفل را به حالت باز حرکت می دهد. در صورتی که بلوتوث اثر انگشت نامناسب را بخواند، در آن نقطه به طور طبیعی سروو موتور را در موقعیت قفل قرار می دهد. اگر از قبل در موقعیت قفل باشد هیچ حرکتی وجود ندارد. (به شکل 2 مراجعه کنید).

```
void loop() {
  while (Serial.available()==0);
reads=Serial.readStringUntil('\n');

    if (reads== "adrfjhlnm")
    {
   myservo.write(0);
   }
    if (reads== "wrong")
    {
   myservo.write(79);

}}
```

اپلیکیشن اندروید مورد نیاز را می توان به دو روش مختلف ساخت. می توان آن را با استفاده از Android Studio یا با استفاده از Kodular پخت. ما در پروژه خود از Kodular استفاده کرده ایم زیرا استفاده از آن آسان است و ما را از نوشتن کدهای طولانی دور می کند. وب سایت kodluar را می توان با استفاده از هر مرورگر وب باز کرد. هنگام ساخت برنامه، اجزای زیر باید در طرح اضافه شوند:

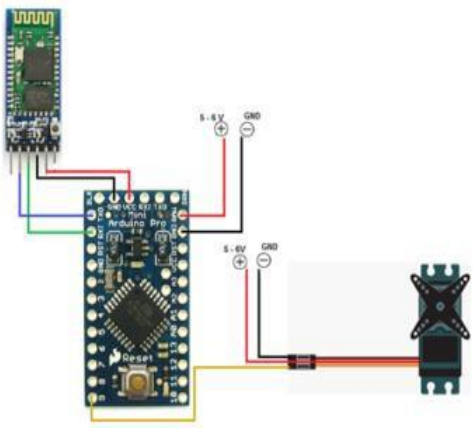
1. بلوتوث کلینت
2. اثر انگشت
3. نمای لیست
4. دکمه تصویر

علاوه بر این، تمام بلوک های کد با هم ترکیب می شوند. اکنون که برنامه پخته شد، apk. استخراج شده و سپس بر روی گوشی هوشمند نصب می شود. (به شکل 3 مراجعه کنید).



پس از نصب برنامه در گوشی هوشمند و آپلود کد در گوشی هوشمند. اجزای زیر به هم متصل و لحیم می شوند.

Pins	Components
Rx	Bluetooth Tx
Tx	Bluetooth Rx
5V	Bluetooth 5V
GND	Bluetooth GND
GND	Servo Motor GND
Pin 9	Servo Motor Signal Wire

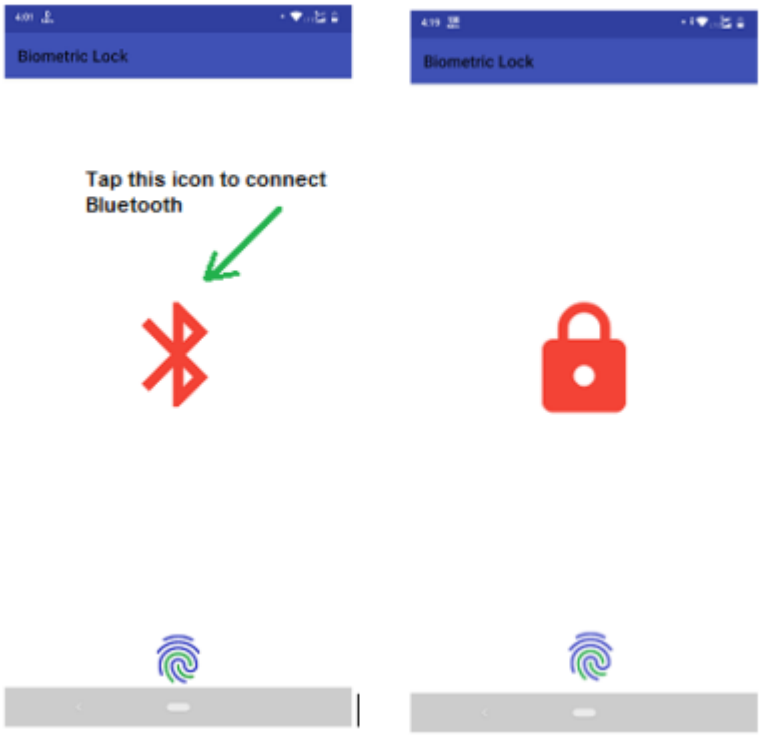


مرحله بعدی تهیه یک قفل فیزیکی برای سیستم قفل بیومتریک است. مراحل زیر برای رسیدن به این هدف دنبال می شود: 1. باید از قفلی که قبلا باز شده یا شکسته استفاده شود. (به شکل 5 مراجعه کنید). 2. محور متحرک سروو موتور برای حرکت به اهرم قفل متصل می شود. 3. مرحله آخر این است که تمام قطعات الکترونیکی را در چهارچوب قفل قرار داده و سپس روی آن را می پوشانیم. (به شکل 6 مراجعه کنید).

Fig -5: Broken Lock.

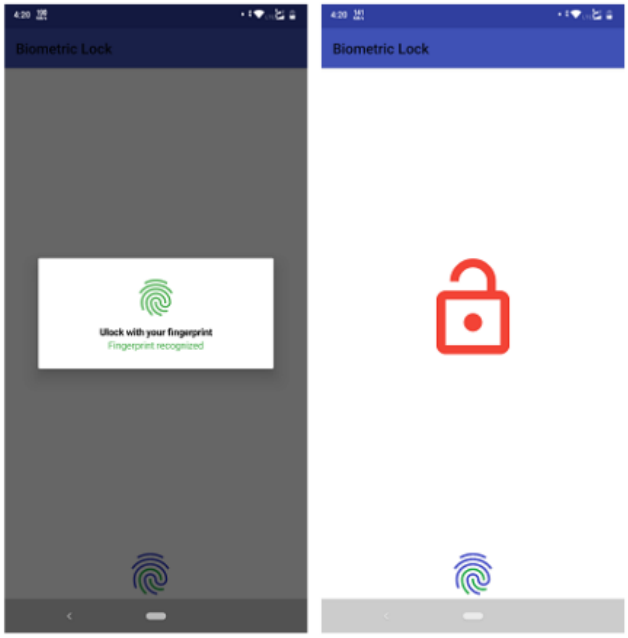
Fig -6: Servo attached to lever.

بعد، قفل با استفاده از یک باتری 5-9 ولت تغذیه می شود. علاوه بر این، بلوتوث گوشی هوشمند روشن شده و با ماژول بلوتوث متصل به برد آردوینو جفت می شود. با باز کردن برنامه، نماد بلوتوث به نماد قفل تبدیل می شود. (به شکل 7 مراجعه کنید).

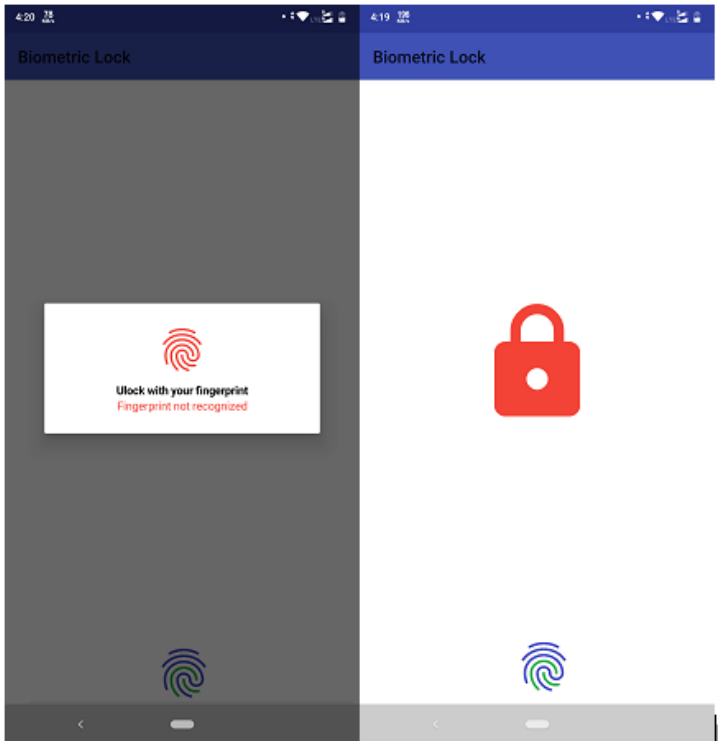


با لمس نماد اثر انگشت، کادر پیامی که درخواست باز کردن قفل با اثر انگشت را دارد ظاهر می‌شود. سپس حسگر اثر انگشت گوشی هوشمند را لمس کنید. در صورتی که با اثر انگشت تنظیم شده در گوشی هوشمند مطابقت داشته باشد، در آن نقطه قفل را به حالت روشن تبدیل می کند و به طور همزمان نماد قفل به نماد قفل تبدیل می شود. (به شکل 8 مراجعه کنید).

SOFTWARE	HARDWARE
Kodular	Bluetooth HC 05
Arduino IDE	Broken Lock
	Arduino Nano
	Servo motor
	Wires-10 cm
	Battery 5-6 V



اگر اثر انگشت اسکن شده با اثر انگشتی که قبلاً ذخیره شده مطابقت نداشته باشد، قفل به حالت قفل باز می گردد. (به شکل 9 مراجعه کنید).



8. نتیجه گیری

سیستم قفل هوشمند امروزه در بازار جهانی اهمیت زیادی پیدا کرده است. تلاش های مستمری برای بهبود استانداردهای امنیتی و تسهیل عملیات و کنترل سیستم امنیتی خانه هوشمند انجام می شود. این مقاله به تشریح ویژگی‌های مختلفی می‌پردازد که در حال حاضر در قفل‌های هوشمند موجود است. با در نظر گرفتن نسخه‌های مختلف مورد بحث، درک کافی از این که چگونه سیستم قفل هوشمند با ارائه دسترسی بدون دردسر از هر نقطه، امنیت خانه یا محل کار را افزایش می‌دهد، به ما می‌دهد.

9. REFERENCES

[1] Jayant Dabhade, Amirush Javare, Tushar Gayal, Ankur Shelar, Ankita Gupta 2017. “Smart Door Lock System: Improving Home Security using Bluetooth Technology”, International Journal of Computer Applications (0975 – 8887) Vol. 160 (8), pp.19-22.

[2] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, David Wagner 2016. “Smart Locks: Lessons for Securing Commodity Internet of Things Devices”, in ASIA CCS’16: Proceedings of the

11th ACM on Asia Conference on Computer and Communications Security, pp. 461-472.

[3] Abdallah Kassem and Sami El Murr, Georges Jamous, Elie Saad and Marybelle Geagea 2016. “A Smart Lock System using Wi-Fi Security”, in 2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA), pp.222-225.

[4] Anu and Bhatia, D. 2014. “A smart door access system using finger print biometric system”, Int. J. Medical Engineering and Informatics, Vol. 6, No. 3, pp.274–280.

[5] Stogu Pavel 2015. “Smart Lock System”, https://www.theseus.fi/handle/10024/98023

[6] Lubhansh Kumar Bhute, Gagandeep Singh, Avinash Singh, Vikram Kansary, Preetam Rao Kale, Shailendra Singh 2017. “Automatic Door Locking System Using Bluetooth Module”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Vol. 5 (V), pp.1128-1131.

[7] Martin K, Teodoor, your personal doorman – Kickstarter, accessed 26 June 2019, <https://www.kickstarter.com/projects/1947538842/teodoor-smart-lock>

[8] Spectrum Brands, Inc. n.d., Kwikset - Kevo, 2019 <https://www.kwikset.com/kevo/smart-lock/security>

[9] August Home, designed in San Francisco, California, 2019, August Wi-Fi Smart Lock <https://august.com/products/august-wifi-smart-lock>