ایده نواورانه قفل هوشمند

محمد رضوانی

مقدمه

در دنیای امروز، تکنولوژی به سرعت در زندگی ما جای گرفته و کارها را بسیار آسان تر کرده است. در مباحث امنیت نیز، تکنولوژی نقش بسازایی ایفا کرده است. یکی از این متدهای امنیتی ، قفل های هوشمند هستند که به کاربران امکانات جدیدی در حفظ امنیت و کنترل دسترسی به محیط‌های مختلف را فراهم کرده است.

قفل های هوشمند با بهره‌گیری از ترکیب فناوری‌های مدرن از قبیل تشخیص اثر انگشت، تشخیص چهره، یا حتی سیستم‌های تشخیص صوت، به کاربران امکان مدیریت و کنترل بیشتری بر روی امنیت فیزیکی محیط خود ارائه می‌دهند. این اقدام نه تنها به افزایش امنیت کمک می‌کند بلکه تجربه کاربری را نیز بهبود می‌بخشد.

از این میان میتوان به قفل های هوشمندی همچون Schlage Encode Smart , Yale Assure Lock SL , Nuki Smart Lock 2.0 , August Smart Lock Pro , WiFi Deadbolt Samsung SHS-P718 Digital Door Lock اشاره کرد که بازار را به قبضه خود درآورده اند.

مفهوم PEAS و عامل مبتنی بر حل مسئله

در این پژوهش به قفل هوشمند پیشنهادی خودمان خواهیم پرداخت.

در ابتدا بایستی به مفهوم PEAS و عامل مبتنی بر حل مسئله بپردازیم زیرا در طراحی سیستم های هوشمند نقس اساسی و پایه را ایفا میکند.

PEAS شامل موارد زیر میباشد:

اندازه‌گیری عملکرد (Performance measure):

این عنصر نشان‌دهنده معیار یا معیارهایی است که سیستم باید به آنها پاسخ دهد و عملکرد خود را بر اساس آن ارزیابی کند.

محیط (Environment):

این عنصر بخشی از دنیای فیزیکی یا محیطی مجازی است که سیستم در آن عمل می‌کند یا با آن تعامل دارد.

عملگرها (Actuators):

عنصری که مسئول اعمال تصمیمات و اقدامات سیستم در محیط است.

حسگرها (Sensors):

عنصری که اطلاعات از محیط را به سیستم منتقل می‌کند تا سیستم بتواند تصمیمات خود را براساس این اطلاعات بگیرد.

همچنین شایان ذکر است که عامل مبتنی بر حل مسله در یک قفل هوشمند، شامل چهار مرحله حصول اطلاعات، تحلیل اطلاعات، تصمیم گیری و اقدام مباشد تا بتوان بر مکانیزم قفل تکیه کرد.

قفل هوشمند پیشنهادی

حال به سراغ متد قفل هوشمند پیشنهادی خودمان میپردازیم.

در متد اینجانب از احراز هویت سه مرحله ای استفاده کرده ایم به نحوی که با توجه به رفتار کاربر بین یک تا سه مرحله به احراز هویت نیاز داشته باشد، حدودا شبیه آنچه که در گوشی های موبایل و شبکه های اجتماعی و یا حتی ایمیل ها صورت میپذیرد با این تفاوت که درجه امنیت بسیار بالاتر است.

در متد پیشنهادی از سه شیوه اسکن قرنیه چشم، تشخیص صوت و همچنین رمز عبور که آن نیز به صورت صوت میباشد، استفاده شده است.

در این روش نواورانه، قفل هوشمند بر اساس تحلیل آماری رفتار کاربر عمل می‌کند. این سیستم با جمع‌آوری و تحلیل داده‌های مربوط به نحوه استفاده کاربر از قفل، الگوهای حرکتی و زمانی را شناسایی می‌کند. سپس، بر اساس این آمارها و اطلاعات، تصمیم‌گیری هوشمندی انجام می‌دهد که آن افزایش درخواست احراز هویت میباشد.

ویژگی‌های این سیستم عبارتند از:

تحلیل الگوهای حرکتی:

سیستم به طور مداوم الگوهای حرکتی کاربر را مانند سرعت باز کردن قفل، زمان حاضر بودن در محدوده قفل و تعداد دفعات باز کردن در یک بازه زمانی مشخص، مورد تحلیل قرار می‌دهد.

تشخیص اتفاقات نامعمول:

در صورت شناسایی الگوهای غیرمعمول یا ناهماهنگ با رفتار معمول کاربر، سیستم هوشمند به صورت خودکار واکنش نشان داده و احراز هویت بعدی را از کاربر تقاظا میکند.

تعامل دینامیک با کاربر:

سیستم قادر است با تغییرات در الگوهای رفتاری کاربر تعامل داشته باشد و در صورت لزوم تصمیماتی مبتنی بر این آمارها اعمال کند.

امکان اطلاع‌رسانی به کاربر:

سیستم می‌تواند با اطلاع‌رسانی به کاربر در مورد رفتارهای مشکوک یا تغییراتی در امنیت، از آگاهی کامل کاربر اطمینان حاصل کند.

این سیستم، با تحلیل داده‌ها به صورت آماری و استفاده از الگوریتم‌های یادگیری ماشین، به بهبود امنیت و انطباق با رفتار کاربران در طول زمان منجر میشود.

تکنولوژی و سنسورها

حال به سراغ تکنولوژی های لازم برای تشخیص فعالیت کاربر بپردازیم.

سنسور حرکتی (Motion Sensor):

برای تشخیص حرکت کاربر در محدوده قفل و جمع‌آوری داده‌های مربوط به الگوهای حرکتی.

سنسور زمان (Time Sensor):

برای رصد زمان باز و بسته شدن قفل و تحلیل الگوهای زمانی مرتبط با استفاده از قفل.

سنسور سرعت (Velocity Sensor):

جهت اندازه‌گیری سرعت عمل باز کردن قفل و شناسایی الگوهای سرعتی مرتبط با رفتار کاربر.

سنسور صوتی (Audio Sensor):

برای ضبط و تحلیل الگوهای صوتی محیط مانند صداهای دستگاه‌های الکتریکی یا حرف‌زدن کاربر.

سنسور تشخیص حالت (Pose Detection Sensor):

برای تشخیص حالت بدن کاربر، مثلاً زمانی که شخص در حال خوابیدن یا ورزش کردن است.

سنسور ارتباطات (Communication Sensor):

برای ارتباط با شبکه‌های اینترنت یا دیگر دستگاه‌ها جهت انتقال داده‌ها و دریافت دستورات.

حال به سراغ تکنولوژی های هر سه مرحله احراز هویت بپردازیم

برای باز شدن در وهله اول که قرنیه چشم میباشد به حسگرهای زیر نیاز داریم

حسگر اول، حسگر تصویر قرنیه میباشد که بدین صورت است که از یک دوربین مخصوص برای گرفتن تصویر قرنیه با دقت و وضوح بالا استفاده میکند.

حسگر بعدی یک سیستم نوری مخصوص میباشد که نور مورد نیاز برای اسکن قرنیه و افزایش دقت در تشخیص و شناسایی را فراهم میکند.

حسگر سوم، حسگر حرکت قرنیه چشم میباشد که برای تشخیص حرکت قرنیه و تمرکز بر روی قرنیه به کار میرود.

همچنین به پردازشگری قوی و الگوریتمی بسیار بهینه برای پردازش تصویر گرفته شده از قرنیه و شناسایی ویژگی های منحصر به فرد آن نیازمند هستیم.

در دومین مرحله احراز هویت برای تشخیص صدای فرد از حسگرها و تکنولوژی های زیر استفاده میکنیم.

از یک یا چند میکروفون با حساسیت بالا برای ضبط صدای فرد استفاده میکنیم

همچنین به یک سیستم پردازشگر صوتی برای تحلیل و پردازش صدا به منظور استخراج ویژگی های منحصر به فرد صدای آن شخص کمک میگیریم و بایستی از یک الگوریتم بهینه تشخیص صوت برای تفسیر ویژگی های صدا و اعتبارسنجی کاربر استفاده کنیم.

این مکانیزم به یک سیستم مقایسه و اطمینان و همینطور سیستم ضد تقلب نیاز دارد که در وهله اول از تطابق صدای ضبط شده با الگوهای ثبت شده برای تشخیص هویت اطمینان حاصل کند و از هرگونه تلاش سواستفاده جویانه مانند استفاده از صداهای از پیش ضبط شده و یا تولید صدای مشابه جلوگیری شود.

در وهله سوم برای وارد کردن رمز به صورت گفتار که مکمل مرحله دوم است علاوه بر تعدادی از سنسورهای بالا مثل میکروفون و سیستم پردازش صوت و الگوریتم های مقایسه و اطمینان، به الگوریتم تبدیل گفتار به متن (sst) نیاز داریم که صدای ضبط شده را به رمز نوشتاری تبدیل کند.

چالش ها

لازم به ذکر است که چنین قفل هوشمندی دارای چالش های خاص خود نیز میباشد که به تعدادی از این مسائل در زیر اشاره خواهیم کرد.

ضریب خطای دستگاه به دلیل محدودیت های نرم افزاری و سخت افزاری بالا میباشد بدین گونه که ممکن است الگوریتم در تشخیص هویت فرد همچون تشخیص قرنیه چشم ناپایدار عمل کند همچون اینکه در شرایط مختلف نوری نتواند به درستی اطلاعات را دریافت و پردازش کند که برای حل این مسله نیازمند صرف وقت و هزینه بالاتری برای بهبود عملکرد الگوریتم خود شویم.

همچنین محدودیت هایی در تامین انرژی دستگاه وجوددارد که در صورت استفاده از باطری نیازمند شارژ دوره ای و مسطحلک شدن باطری در طول زمان هستیم.

و مورد سوم افزایش هزینه ساخت بسیار بالا بدلیل وجود سنسور ها و تکنولوژی های متعدد هستیم.