A Method for FIDO Management through Biometric Technology in IOT

Azamsadat Parei  
Information Technology Engineering - Electronic Commerce,  
Master Degree, K. N. Toosi University of Technology;  
as.parei@gmail.com

Hodjat Hamidi  
Information Technology Engineering Group; Department of  
Industrial Engineering; K. N. Toosi University of Technology;  
Corresponding Author h_hamidi@kntu.ac.ir

Received: 29, Jan. 2017  Accepted: 14, Mar. 2017

Abstract: Internet of Things (IOT) is a newly developed concept in the world of technology and communication which provides the ability to transfer technological information to everything, including human, animals, or objects, through communication networks such as internet or intranet. Biometric technology offers various applications. The main objective is to provide an appropriate alternative for control systems with traditional access. It is also utilized for personal protection or corporate finance. Simultaneous application of Biometric technology and Fast Identity Online (FIDO) may advance interaction with objects and authentication of those who want to access crucial information. This process is much more costly and time-consuming. This article presents a new approach for utilizing biometric technology in IOT, in order to manage biometric in IOT. The results demonstrate that fingerprint biometry obtains the highest priority as compared to other biometric techniques used in IOT, while it imposes the lowest implementation costs. Moreover, it provides a high level of security for the system management.

Keywords: Information Management, Internet of Things, Fast Identity Online (FIDO), Biometric
ارائه روتکردنی برای مدیریت تشخیص سریع برخط با استفاده از فتاوری بیومتریک در اینترنت اشیا

اعظمالعادات بروی

حجت‌الله حمیدی

کارشناسی ارشد؛ گروه فتاوری اطلاعات؛ دانشکده مهندسی صنایع؛ دانشگاه صنعتی خواجه نصیرالدین طوسی

as.parei@gmail.com

در کناری کامپیوتر؛ استادیار؛ گروه فتاوری اطلاعات؛ دانشکده مهندسی صنایع؛ دانشگاه صنعتی خواجه نصیرالدین طوسی;

h_hamidi@kntu.ac.ir

چکیده: اینترنت اشیا مفهومی جدید در دنیای فتاوری و ارتباطات است که قابلیت ارسال داده‌های فتاوری برای تمام اشیا را از طریق شبکه‌های ارتباطی امکان می‌دهد. این امکان فراهم می‌آورد که در زمینه‌های مختلف از فتاوری‌های زیست‌سنجی و تشخیص سریع برخط از داده‌های هم‌بینی ایجاد کند. همچنین، تشخیص هویت فرد از افراد مختلف بسیار سریع تر و با دقت بالاتر صورت می‌پذیرد. این در حالی است که گروه حمیدی از روش‌های قدیمی مانند سیستم‌های اثر انگشتی دارای بررسی بالاتر بوده و پرهزینه است. در این مقاله برای مدیریت تشخیص سریع برخط در اینترنت اشیا، به معرفی روش‌های جدید جهت استفاده از زیست‌سنجی در اینترنت اشیا پرداخته شده است. با توجه به نتایج مقاله، مشاهده می‌شود که زیست‌سنجی اثر انگشت دارای بالاترین اولویت نسبت به سایر تکنیک‌های زیست‌سنجی برای ایجاد استفاده در اینترنت اشیا بوده و در آینده ترین تحقیق‌های این راه پایان زده و برای پایان‌رسانی این روش مطالعه‌های جدیدی انجام شود.
کلیدواژه‌ها: اینترنت اشیا، فناوری بیومتریک (زیست سنجی)، تخصص سریع برخط، مدیریت اطلاعات

1. مقدمه

اینترنت اشیا، این گونه تعريف مي شود: زيرساختار شبکه جهاني بيشا كه داراي قابلیت‌های خودپرکنندي بر اساس پروتکل‌های ارتباطی استاندارد و هم‌کنش پذیر است؛ حاکی که در آن اشیا فیزیکی و مجازی داري هستند، مشخصه‌ فیزیکی و شخصیت مجازی هستند. از واسطه‌های هوشمند استفاده مي كنند، و بهطور بی نقص با شبکه اطلاعات ادغام مي شوند. زيرساخت اينترنت اشي با اساس تكنولوژي هاي متعدد تشكيل شده است. از آن جمله مي توان به موارد زير اشاره كرد: هوش محدوده ای، پروتکل اينترنتی، تكنولوژي ارتباطی (واي فاي، بلوتوث، زيرگب)، دستگاه‌های تعابي‌شده (اي‌ها جي‌ماش‌که‌های بي‌سیم) و برنامه‌های كاربردي. سیستم‌های زیست سنجی، گروهی از تکنولوژی‌ها و تکنیک‌هایی هستند که با استفاده از ویژگی‌های فیزیولوژی و رفتاری آن‌ها با رای تخصص‌ها همیشه و شناخت انسان به‌کار می‌روند. يکی از مهم‌ترین مراحل زیست سنجی این است که ویژگی‌های بیومتریک را كه به عنوان شناسه استفاده مي شود، نمي توان اماند داد. اين‌طوراً، به خريدارى كردن و خليه دشوار است كه بتوان آنها را جعل نمود. بر خلاف سایر فناورى‌های كنترل دسترسى، زیست‌سنجى را نمي توان فراموش كرد، اما دوچرخه وب‌وب. به عنوان مثال، گذراى‌ها يو براتى فراموش مي‌شوند و كليدها و كارتى‌ها به راحتى ممكن است گم شده با يا ور اين گرفته شوند. در حالی كه با استفاده از ویژگی‌های زیست سنجی ارتباط می‌باشد، اینترنت اشیا می‌تواند به سهولته و سه‌روگردان درآمده، به اين مطلب می‌پردازيم. این‌گونه است که با استفاده از WSN‌ها، فناورى با استفاده از اینترنت اشیا مورد بررسى قرار گرفته است. علاوه بر این این‌گونه است که با استفاده از RFID موارد مطرح بوده است.

1. internet of things (IOT)
2. wireless sensor network (WSN)
3. biometrics
4. Open Connectivity Foundation
5. Laurence Feng & Yang
6. Radio-Frequency IDentification (RFID)
ارائه رویکردهای برای مدیریت تنش خصوصی برخط با استفاده از فناوری بیومتریک در اینترنت اشیا

فرماتیاجنگین، نظریه شواهد (Zhang et al. 2014) موجود موبایل (Zhang et al. 2014) می‌رنا به سمت پیشرفته در اینترنت اشیا سوق می‌دهند. اینترنت اشیا مفهومی جدید در دنبال فناوری و ارتباطات بوده و به‌طور خلاصه، فناوری مدیریت است که در آن برای هر موجودی (انسان، حیوان و یا اشیا) قابل‌پیوند ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت با ارتباط فراهم می‌شود. بستر اینترنت اشیا بر امکان رادیویی به‌سیمی قرار دارد که به دستگاه‌های مختلف این امکان را می‌دهد که از طریق اینترنت با یکدیگر ارتباط برقرار کنند.

اینترنت اشیا دانه‌های اندیس و افزایش خواهد داد به شرطی که راه جدیدی از فرصت‌ها به روش فقیر تجربه باشد (Zeng et al. 2011). بیشتر کسی‌ها برای پیام‌سازی اینترنت اشیا در سطح خدمات ملی، راهبردهایی که حاکی از ایران کرده‌اند، به‌عنوان مثال، دسترسی به به‌عنوان یکی از مهم‌ترین تغییرات را برای ارتباط بین مورد، مورد و آشیا و اشیا و افراد آورده‌اند (Zhang et al. 2014). به‌طور مشابه، خانه‌های هوشمند در کره جنوبی مورد را قادر به سازد به اشیا از دوردست دسترسی داشته باشند (Srivastava 2004).

از طرف دیگر، اینترنت اشیا می‌تواند به داده‌ها نیز مرتبط شود. همانطور که می‌دانیم انسان همیشه به‌دلیل نمای برای بهبود وضعیت خود، برای رسیدن به اطلاعات موجود و به‌بیان داده‌ها جدید نشان‌دهنده‌اند. تجزیه و تحلیل ترافیک داده‌ها شدیداً تحت تأثیر اطلاعات موضعی و سیاسی، تحت تأثیر حریم خصوصی موقعیت هستند (Alur et al. 2016). تولید اطلاعات از داده‌ها برای تنظیم و تغییر دندان‌گی بسیار مهم و حیاتی است، به‌ویژه این که شرکت‌ها نیاز دارند داده‌ها را ذخیره کرده و آنها را تبدیل کند تا بتواند با سرعت در جهت رسیدن به اهدافی مانند مزیت رقابتی، تولید محصولات جدید و پیش‌رفت شرکت‌گان کامل به جلو بپردازند (Dijkman et al. 2015). با استفاده از داده‌ها می‌توان مقدار زیادی از اطلاعات را در محدوده وسیعی دختره، مدیریت و پردازش کرد. علاوه بر این، استفاده از داده‌ها و آنالیز آنها می‌تواند مزایا و تسهیلاتی را برای شکت‌ها، محققان و مصرف کنندگان ارائه کند. در نتیجه، اینترنت اشیا می‌تواند در حفاظت از دسترسی به داده‌های مهم نیز کارایی داشته باشد. علاوه بر این هم، امروزه شناسه و رمز کارت هایی که به کار می‌روند، دسترسی را محدود می‌کند. اما این روش‌ها به‌اختیار می‌توانند شکسته شوند. پس، غیرقابل اطمینان هستند. تکنولوژی زیست‌سنجی کاربردی‌های فراوانی دارد که هدف اصلی آن تهیه جانشینی مناسب برای سیستم‌های کنترل دسترسی است و برای...
حفاظت شخصی یا دارایی‌های سازمانی استفاده می‌شود.

در ادامه، این مقاله به صورت زیر بخش‌بندی شده است: در بخش دوم، دیدگاه‌های مختلف الگوی اینترنت اشیا به صورت جدولی از مقالاتی بازیبی شده ارائه و باهم مقایسه شده‌اند. در بخش سوم، تکنولوژی‌های اصلی و توأم‌نام اینترنت اشیا معرفی شده است و در بخش چهارم، داده‌ها و اینترنت اشیا توضیح داده می‌شود. در بخش پنجم، امکان‌های اینترنت اشیا بررسی می‌شود و در بخش ششم، به معرفی تکنولوژی‌های زیست‌سنجی و تشخیص سرعت برابر از ۱ می‌پردازیم. در بخش هفتم، روش پیشنهادی در جهت رفع چالش‌های امکان‌پذیری ارائه می‌گردد. در بخش هشتم، یافته‌های مقاله بسط داده شده و در بخش نهم، نتیجه‌گیری ارائه شده است.

2-1. زیست‌سنجی

یک خصوصی‌های از انسان را می‌توان به عنوان یک ویژگی در زیست‌سنجی به کار برد، به شرطی که دارای ۴ ویژگی زیر باشد:

جهتی بودن ۴: همگانی باشد (عومومی بودن);
تمایزی در دو فرد مشابه نباشند (متفاوت بودن).

1. Fast Identity Online (FIDO)
2. Gartner Inc.
3. Cisco
4. universality
5. distinctiveness
دائمی بودن: در طول زمان تغییر نیابد (دوام داشتن)
قبلاً جمع آوری: یعنی به صورت کمی قابل اندازه‌گیری باشد.
در کاربردهای زندگی روزمره سه فاکتور دیگر نیز بازی رعایت شدند کارایی (از لحاظ دقت، سرعت)، دسترسی و امنیت بالا (2005). با توجه به این که تبیین سریع و امنیت در حوزه اینترنت اشیا مطرح است، در جدول 1 و شکل ا، به بررسی مقالاتی که در مورد کاربرد زیر سنتی مطالعه شده، می‌پردازیم.

جدول 1: مقالات مطالعه‌شده در زمینه زیرسنتی

<table>
<thead>
<tr>
<th>توضیحات</th>
<th>عنوان مقاله</th>
<th>نام زورنال</th>
<th>نویسندگان</th>
</tr>
</thead>
<tbody>
<tr>
<td>در این مقاله یک مدل احراز هویت در سیستم بانکی برخط با رمزگاری کوانتومی پیشنهاد شده است</td>
<td>احراز هویت در سیستم بانکداری برخط از طریق رمزگاری کوانتومی</td>
<td>International Journal of Engineering and Technology</td>
<td>Sharma and Lenka (2013)</td>
</tr>
<tr>
<td>بررسی ارث پیری گوی عنبیه با استفاده از گوشه ای یون د ۴۴ نمونه</td>
<td>پیدایش پیری گو در تشخیص عنبیه</td>
<td>Access, IEEE</td>
<td>Fenker, Ortiz, and Bowyer (2013)</td>
</tr>
<tr>
<td>ارائه روش جدید مبتنی بر تجزیه و تحلیل الگوهای ورودی از کاربران بانکداری</td>
<td>پانکدری تلفن همراه ایمن در دستگاه‌های تلفن همراه هوشمند و رویکرد احراز هویت مبتنی بر الگو</td>
<td>International Journal of Scientific Research in Computer Science</td>
<td>Dedeepya, Swetha, and Raju (2013)</td>
</tr>
<tr>
<td>بررسی اثبات الگوی گوی عنبیه با استفاده از گوشه ای یون د ۴۴ نمونه</td>
<td>الگوی گو در تشخیص عنبیه</td>
<td>Handbook of Iris Recognition</td>
<td>Baker et al. (2013)</td>
</tr>
</tbody>
</table>

1. permanence
2. collectability
<table>
<thead>
<tr>
<th>توضیحات</th>
<th>عنوان مقاله</th>
<th>تاپ زورتال</th>
<th>نویسندگان</th>
</tr>
</thead>
<tbody>
<tr>
<td>بحث در مورد سیستم‌های وزن‌سنجی موجود برای دستگاه‌های لفتن همراه</td>
<td>سیستم‌های امتیازی وزن‌سنجی موبایل</td>
<td>International Symposium on Digital Forensics and Security</td>
<td>Yıldırım and Varol (2014)</td>
</tr>
<tr>
<td>برای امرور و آنده برای امتیاز وزن‌سنجی</td>
<td>توضیح تشخیص عنبیه و صورت برای تعامل با موبایل</td>
<td>Image and Vision Computing</td>
<td>Marsico et al. (2014)</td>
</tr>
<tr>
<td>توضیح تشخیص عنبیه و صورت برای تعامل با موبایل</td>
<td>اثر برای امتیاز وزن‌سنجی</td>
<td>Biomedical Engineering Systems and Technologies</td>
<td>Czajka (2015)</td>
</tr>
<tr>
<td>اثر برای امتیاز وزن‌سنجی</td>
<td>اطمنان تشخیص</td>
<td>Computing for Sustainable Global Development</td>
<td>Indu and Jain (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی جوهر و عنبیه برای استفاده با موبایل</td>
<td>Biometric Technology Today</td>
<td>Hamid (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
<tr>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>بررسی اثرات پریکارگی عنبیه با استفاده از VeriEyeMIRLIN IRIS و OSIRIS</td>
<td>Journal of Systems and Information Technology</td>
<td>Jung and Hong (2015)</td>
</tr>
</tbody>
</table>
احترام به تاریخ، یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

شناختی، هدف اصلی اینترنت از جمله اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

شناختی، هدف اصلی اینترنت از جمله اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

شناختی، هدف اصلی اینترنت از جمله اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

شناختی، هدف اصلی اینترنت از جمله اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

شناختی، هدف اصلی اینترنت از جمله اشتراک‌گیری اینترنتی است. در حال حاضر، اینترنت به عنوان یکی از ابزارهای اصلی اشتراک‌گیری اینترنتی در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.

در تحلیل داده‌ها و تحقیقات و بررسی‌های علمی مورد استفاده قرار می‌گیرد.
جدول ۲. فناوری‌های مورد استفاده در اینترنت اشیا

<table>
<thead>
<tr>
<th>مراجع</th>
<th>فناوری</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Dominikus 2010; Khoo 2010; Schmidt 2009; Welbourne 2009; Sheng 2010)</td>
<td>RFID</td>
</tr>
<tr>
<td>(Broll 2009; Garrido 2010)</td>
<td>NFC</td>
</tr>
<tr>
<td>(Hong 2010; Tozlu 2011; Zhu 2010; Li 2013)</td>
<td>شبکه سنسورها</td>
</tr>
<tr>
<td>(Aberer 2006; Bandyopadhyay 2011; Blackstock 2010; De 2011; Dong 2010; Gómez-Goiri and López-de-Ipiña 2010; Huang and Li 2010a; Katasonov 2008; Kirtsis 2011; Puliafito. 2010; Roalter 2010; Song 2010; He and Xu 2014)</td>
<td>میانفازار</td>
</tr>
<tr>
<td>(Garcia-Macias 2011; Ostermaier 2010)</td>
<td>معماری جستجوگرها</td>
</tr>
<tr>
<td>Castellani 2010, 2011; Gronbaek 2008; Guinard 2011; James 2009; Michael and Darianian 2010; Spiess 2009; Wang 2012</td>
<td>معماری نرمافزار</td>
</tr>
<tr>
<td>(Giner 2010; Kawsar 2010)</td>
<td>معماری فراکسیونی</td>
</tr>
<tr>
<td>(Främling and Nyman 2008; Kortuem 2010; Ning and Wang 2011; Xiaocong and Jidong 2010)</td>
<td>عملیت دیسکارتهدنگی</td>
</tr>
<tr>
<td>(Darianian and Michael 2008; Heil 2007; Li 2011; Liu 2011; Schaffers 2011; Vicini 2012; Fang 2013)</td>
<td>زیرساخت‌های هوشمند</td>
</tr>
<tr>
<td>(Bui and Zorzi 2011; Dohr 2010; Domingo 2012; Jara 2010a, b; Luo 2009; Rohokale 2011)</td>
<td>بهداشت و درمان</td>
</tr>
<tr>
<td>(Alcaraz 2010; Babar 2010; Diamini 2009; Hancke 2010; Mahalle)</td>
<td>امیت و چالش‌ها</td>
</tr>
<tr>
<td>(Medaglia and Serbanati 2010; Oleshchuk 2009; Sarma and Girão 2009)</td>
<td>حریم خصوصی فیزیکی</td>
</tr>
<tr>
<td>(Weber 2009, 2011)</td>
<td>فوانین علومی</td>
</tr>
<tr>
<td>(Bandyopadhyay and Sen 2011; Christin 2009; Coetzee and Eksteen 2011; Ma 2011; Mattern and Floerkemeier 2010; Mayordomo 2011; Shen and Liu 2011; Zhang 2011)</td>
<td>مدل کسب‌وکار</td>
</tr>
<tr>
<td>(Bohli 2009; Haller 2009; Fu 2011; Li 2012)</td>
<td>آینه‌گرگی</td>
</tr>
</tbody>
</table>
| (Akyildiz and Jornet 2010; Guinard and Trifa 2009) | اطلاعات انتشار‌افته و همسکاری ماشینی به ماشین و ماشین به انسان است (Farooq et al. 2015). در ایامه اولیه اینترنت اشیا تصور این است که هر روز وسایلی مثل وسایل نقلیه،
پیچیده‌ترین، لوزی‌پاترکی و به‌طور کلی، کالاهای مرتفعی به قابلیت سنگین‌سازی از روی دور و ردیابی مجهز‌شوند. هنگامی که این ابزار کاملاً واقعی شد، اینترنت اشیا مناسب‌تر برای سیستم اطلاعاتی بر تک‌پیغه‌ای از نرم‌افزار و سخت‌افزار و معماري تأکید می‌کند. توسعه اصلی اینترنت اشیا در شکل ۲ به تصویر کشیده شده است (Alur et al. 2015).

![ددا. ۲. توبع اصلی اینترنت اشیا](downloaded from jipm.irandoc.ac.ir at 21:12 IRST on Wednesday October 30th 2019)

به‌طور خلاصه، ۳ خصوصیت اصلی سطح سیستم اینترنت اشیا را، همان‌طور که در ادامه آمده، از سر می‌گردد:

۱. هر چیزی ارتباط بروز می‌کند: اشیا هوشمند قادر به برقراری ارتباط به‌صورت بی‌سیم در میان خودشان هستند و شبکه‌های شک یک کار اشیاء متصل را شکل می‌دهند.

۲. هر چیزی شناسایی می‌شود: اشیاء هوشمند با یک کهکشان دیجیتالی شناخته می‌شوند. ارتباط بین اشیا می‌تواند در قلمرو دیجیتالی، هر زمانی که اتصال فیزیکی را نمی‌کنند

آباد آمد، از سر می‌گردد.

۳. هر چیزی تعامل دارد: اشیاء هوشمند می‌توانند با محیط محلی طی دریافت و به‌کاراندازی قابلیت‌ها در هر زمانی که آرائه می‌شوند، تعامل کنند.

اینترنت اشیا (اینترنت اشیا)
3. فناوری زیست‌سنجی و تشعیص سریع برخط
عملکردن اساسی مورد نیاز در زیست‌سنجی بی‌پایان چهار میلیارد دقت، مقیاس اندیس امنیت و حمایت خصوصی اندازه گیری می‌شود. برای تمام دستگاه‌های زیست‌سنجی پنج عنصر مشترک وجود دارد. این عناصر عبارتند از: نگه‌داشتن الگوی زیست‌سنجی، مقایسه، شبکه و ویژگی‌های زیست‌سنجی شخصی.
آقای امنگ و همسران طی مطالعه‌ای در سال ۲۰۱۵ تکنیک‌های مختلف زیست‌سنجی را بر اساس هفت ویژگی در حالات مشترک به صورت تجربی ارزیابی کرده‌اند. عمومیت، منحصر به فردودن، پایداری، جمعآوری، عملکردن، مقیاس دهی، و عبور از آن ویژگی بیان‌شده در این مطالعه هستند. این ارزیابی در دو زمینه زیست‌سنجی فیزیولوژیکی و زیست‌سنجی رفتاری انجام شده است. تحقیق اثر انگشت، تحقیق چهره، تحقیق عنی، تحقیق هندسه دست و تحقیق کف دست از زیست‌سنجی‌های فیزیولوژیکی بررسی شده است.
و تحقیق صدا، تحقیق امضا، تحقیق راه رفتن، پردازش فناری، ضربه‌زن‌، کلد دیمیک، و لمس دیمیک از زیست‌سنجی‌های رفتاری ارزیابی‌شده است. در مقایسه با روش‌های سنتی تحقیق هویت، مانند رمز عبور و کارت شناسایی می‌توان به مزایای زیست‌سنجی اشاره کرد که به‌ویژه داده‌های نمایندگی، دیدگاه نمایندگی، گرم و یا فراموش نمایندگی، خراب نمایندگی، غیرقابل حذف زدون و غیرقابل فراموشی هستند. با توجه به شکل ۳ حداکثر ۴۸ درصد از بانک‌های جهان از زیست‌سنجی اثر انگشت در عملیات بانکی خود استفاده می‌کنند. بنابراین، می‌توان با امنیت بیشتر و استفاده از استاندارد تحقیص سریع برخط در اینترنت اشیا نیز از آن استفاده کرد.
۳. شکل. نقاط ضعف و قوت انواع تکنیک‌های بیومتریک
پس از مراحل مربوط به استفاده از این فناوری، ارزیابی دیگری در مورد عملکرد و مقبولیت ویژگی‌های دیگر زیست‌سنجی نیز انجام گرفت. که در قابل جدول ۳، به نمایش گذاشته شده است. در این بخش نقاط قوت و ضعف تکنیک‌های زیست‌سنجی را بیان می‌کنیم. پس از بررسی های عمل آمده معلوم شد که یکی از زیست‌سنجی‌های مهم اثر انگشت است که با تکنیک‌های دیگر مقایسه شده است.

d| مقارنة تکنیک‌های زیست‌سنجی |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>نقاط قوت</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>دقت خوب</td>
</tr>
<tr>
<td>عدم کارایی در شرایط خاص</td>
</tr>
<tr>
<td>نیازمند به سخت‌افزار اضافی</td>
</tr>
</tbody>
</table>
| نیازمند به سخت‌افزار اضافی، هزینه بالا زمان بالای احراز هویت | نیازمند به سخت‌افزار اضافی، هزینه بالا | نیازمند به سخت‌افزار اضافی | درست
| متوسط | سادگی استفاده، کمتر قابل تقلیل | تشخیص هندسه دست |
| شرایط عمومی، دقت بالا | پذیرش عمومی، دقت بالا | تشخیص کف دست |
| دقت نسبتاً بالای، عدم کارایی در شرایت کسانی | پذیرش کسانی، راحتی استفاده، احراز هویت | تشخیص صدا |

811
1- روشن‌های اصلی اصلاح‌سنجی (احراز هویت)
این روشن‌ها جهت دسترسی افراد به سامان‌های بزرگ در سازمان‌ها یا دسترسی به اطلاعات بیماران در سیستم‌های بیمارستانی و استفاده از آنها مستلزم با اینترنت همراه مورد استفاده قرار می‌گیرند. این روشن‌ها به سه بخش زیر تقسیم می‌شوند:
بر پایه‌ «دانش»، مانند پسوردها؛
بر پایه «مالکیت»، مانند استفاده از کارت هوشمند یا پهنک إسکن‌افزاری;
بر پایه «پوسته»، مانند استفاده از ویژگی‌های رفتاری و ذاتی زیست‌سنجی (صدای امضا، تایب، عنبیه، شبکه‌ای، اثر انگشتی، هندسه دست، تشخیص چهره)، پس از بررسی‌های صورت گرفته معلوم شد که روشن‌های اینهای است که برای صدا و امید، بالاترین رخ‌‌دار است.
احراز هویت زیست‌سنجی اثر انگشت با استفاده از نمایش نشانه‌های دار از برابر دیگری‌های پوست مانند نقاش دوشاک، بر آمادگی کوتاه، نقاط انتها در انگشت انگاج می‌شود. دستگاه‌های ثبت اثر انگشت عمده‌ با صورتر حرارتی، نوری، خاکی و فراصلی هستند. در روش ابداعی حرارت به ولتاژ تغییر می‌یابد. در روش بعدی از نوری مرنی برای هندسه اثر انگشت استفاده می‌شود و در روش خاکی پیکسل‌های خاکی موجود دارند که در جزء وظیفه ثبت پیکسل از تصویر نهایی را دارد (جدول ۴).

2- احراز هویت زیست‌سنجی با روش فراصول
شرکت کوالکام، ۲ در سال ۱۹۸۵ میلادی در شهر «سن‌دلیگو» ایالات متحده آمریکا
تأسیس شد. در دهه ۱۹۹۰ میلادی اقدام به تولید تجهیزات مخابرات راه دور و تأسیس شرکت پردوزنده‌های اسکورپیون و کرایت از سری اسنپ دراگون، را عرضه کرده است. تکنولوژی تصویر سه‌بعدی اثر انگشت قابل‌پوش سازگاری با سری ایندیوگرافی در بیزین‌کردن می‌باشد. در این حسگر، ابتدا امواج مافوق صوت به سطح انگشت ارسال می‌شود و انرژی نیرویی ایجاد از سطح انگشت انتقال می‌یابد. سپس، انرژی وارد سطح پوست حساسیت ندارد. قابلیت تشخیص منابع در زیر و سطح پوست را دارد و از همه مهم‌تر این که قابلیت سازگاری با سایر پایگاه داده‌های اثر انگشت را دارد.

جدول ۴: بررسی دستگاه‌های ثبت اثر انگشت

<table>
<thead>
<tr>
<th>فراوصت</th>
<th>نویز</th>
</tr>
</thead>
<tbody>
<tr>
<td>خارجی</td>
<td>داخلی</td>
</tr>
<tr>
<td>هزینه</td>
<td>متوسط</td>
</tr>
<tr>
<td>زیاد</td>
<td>قابل عبور در تجهیزات کوچک</td>
</tr>
<tr>
<td>کم</td>
<td>قابل عبور در تجهیزات کوچک</td>
</tr>
<tr>
<td>دقت</td>
<td>حساسیت به لبه یا آب</td>
</tr>
<tr>
<td>عدم حساسیت به لبه و آب</td>
<td></td>
</tr>
</tbody>
</table>

با توجه به این که فراوانی و فراموشی گذشته‌ها، سرعت گذشته‌ها، فشینگ، حمله و جست و جوی کور کورانه از مشکلات اساسی گذشته‌های اسکورپیون، کرایت و مسائل کاربردی نیز می‌توان سخت‌تر بپسورد در تلفن‌های همسر را نمایند بردار. بنابراین، وجود راه حلی جهت حفظ امنیت ضروری است.

همان‌طور که می‌دانید، امروزه برای حصول اطلاعات در زمینه امنیت در فناوری‌های مختلف استاندارد‌های مختلفی تدوین می‌گردد، این است که برای استخراج استاندارد بین‌المللی جهت استفاده در کاربردهای مختلف می‌توانید صورت گیرد. تا روشی واحد با دقت بهینه و سرعت مناسب انتخاب شود. به عنوان مثال، استاندارد ISO/IEC ۲۷۰۰۱ می‌تواند مبتنی بر امنیت اطلاعات است. این است که سازمان‌ها صورت استفاده قرار می‌گیرد. در زمینه استفاده از ویژگی‌های چندین‌تکنیکه نیز هر نیازمندی استفاده از استانداردهای بکارگیرنده با دقت بالا احساس

1. Information Security Management Systems
می‌شود. به‌همین منظور، فهرستی از استانداردهای مختلف جمع‌آوری شده که در جدول 5 نمایش داده می‌شود.

جدول 5. بررسی استانداردهای معتبر جهانی

<table>
<thead>
<tr>
<th>شرح</th>
<th>تام استاندارد</th>
<th>صنعت</th>
</tr>
</thead>
<tbody>
<tr>
<td>نیاز به همه اعضای اتحادیه اروپا برای اتخاذ دستور امتنی</td>
<td>استاندارد امینت اطلاعات صنعت</td>
<td>اتحادیه اروپا (EUDPD)</td>
</tr>
<tr>
<td>تعیین نیاز‌های امنیتی پانکاداری برخط</td>
<td>استاندارد امینت اطلاعات مالی و فراکده پرداخت خرد</td>
<td>مالی / پانکی</td>
</tr>
<tr>
<td>جامعه برای پرداخت امتنی</td>
<td>استاندارد امینت اطلاعات مالی</td>
<td>GLB/ (Bliiley)</td>
</tr>
<tr>
<td>داده‌های کارت پرداخت: احراز هویت، تحقیق حکم برون و پیشگیری</td>
<td>استاندارد امینت اطلاعات مالی و فراکده پرداخت خرد</td>
<td>GLBA</td>
</tr>
<tr>
<td>کنترل دسترسی، حساب‌رسی، یکپارچگی داده‌ها، استانداردهای رمزگذری برای داده‌های سلامت</td>
<td>مراقبت‌های بهداشتی مدارک پاسخگو به قانون</td>
<td>دارویی</td>
</tr>
<tr>
<td>استانداردهای محرمانگی برای حقوق آموزشی خانواده و قانون</td>
<td>اداره آموزش و پرورش آمریکا</td>
<td>دولت آمریکا</td>
</tr>
<tr>
<td>داده‌های دانش آموز شامل نمرات، ثبت نام، صدور صورت حساب</td>
<td>حقوق خصوصی (FERPA)</td>
<td>مدارس آمریکا</td>
</tr>
<tr>
<td>تعیین احراز هویت، مدیریت کلید رمزگذاری و امنیت فیزیکی در سازمان‌های آمریکا</td>
<td>استاندارد پرداخت اطلاعات قدرال از مؤسسه ملی استاندارد و تکنولوژی (NIST)</td>
<td></td>
</tr>
</tbody>
</table>

3-3. تشخیص سریع برتبخ و حذف پسوردها

در سال 2013، "مایکل بارتر" مدیر امینت اطلاعات "پی بان"، در نمایشگاه "اینتراوپ" در آمریکا با نمایش سنتگ قبری منتفش به وازگان بیان داشت که استفاده از گذرواژه‌ها در اینترنت به شکست منتفش می‌شود و نشان داد که عمر گذرواژه‌ها به پایان رسیده است. انتلاف تشخیص سریع برتبخ یک سازمان غیرانتفاعی است که در تابستان سال

1. Michael Barrett
2. Paypal
3. Interop
ارائه روش‌های برای بازیابی نوشته‌های از افزایش کاربران برای انتخاب از رفتارهای نامناسبی در اینترنت

1. RSA
توسط بنگاه‌های اقتصادی و تجاری اهمیت‌های امنیت تبدیل اطلاعات در این فضا مطرح

بوده و یکی از جالب‌‌ترین بزرگ‌تر استفاده از ابر متصل به اینترنت و دسترسی به
داده‌گان در شرکت‌ها و... است. با توجه به این که هر چه امنیت با گسترش اینترنت و ارائه انواع
خدمات الکترونیکی، نفوذ افراد غیرمجاز و سوء‌استفاده کندگان گسترش دیده است،

ارائه راهکارهای جدید و با قدرت جهت تأمین امنیت تبدیل اطلاعات نیاز اساسی این
بحث است. امروزه، استفاده از کلیه عبور و گذرواژه‌ها برای این امر در نظر گرفته شده
است که خود، با جالب‌ترین فراوانی روابط. یکی از مشکلات اساسی گذرواژه‌ها
فرایش و فرمولی گذرواژه و سرقت گذرواژه، تکراری بودن آنها به جهت پیادآوری
آسانتر استفاده از موارد معمول و قابل دسترسی، شماره شناسانه با تاریخ تولد،
حمله فیشینگ، حمله جست وجوی کور کردن است. از مسائل کاربردی نیز، سختی تایب
پسورد در تلفن‌های همراه، استفاده از اینترنت اشیا و دسترسی به اطلاعات جهیز قابل ذکر

است (شکل ۶).

با توجه به موارد ذکر شده استفاده از راهکاری جهت حفظ امنیت، احراز هویت به

اصلت سنجی که شامل تایید هویت یک شخص، با اطمینان از اصلیت یک نرم‌افزار

است، ضروری احساس می‌شود.

۴-۱. استاندارد شناسی سریع برهنگ

داده‌ها در بالانکداری برخی: یکی از مؤلفه‌های کلیدی در بحث اعتماد مشتریان به

بانکداری اینترنتی مسئله احراز هویت و تایید هویت است که عموماً بر شناسه و رمز
عبور بمنی است. استفاده از شیوه‌های زیست‌سنجی در این حوزه ضروری است.

انتخاب درست یک چند زیست‌سنجی جهت احراز هویت مشتریان چالش اصلی

در این حوزه است;

پرداخت‌های تلفن همراه: بهره‌گیری از سرعت و امنیت احراز هویت زیست‌سنجی

برای جلوگیری از تقلب در تمامی تراکنش‌ها مانند پرداخت از
برنامه‌های کاربردی موبایل، نقل و انتقال بول P2P تجارت الکترونیک بدون کارت;

سایر خدمات تجارت الکترونیک: تجارت در بازارهای جهانی ناپایدار امنیت و اجرای

بدون افشاگری اطلاعات است و از آنجا که تجارت الکترونیک رودرو نیستند، لذا بحث

احراز هویت به عنوان یکی از موارد امنیت الکترونیک محصول می‌شود. اگر بتوان با

816
روشی مطمئن ثابت کردن که طرفین تجارت هر دو مسیر هستند که ادعا می‌کنند، مسلمًاسم یکی از جالش‌های موجود در تعاملات الکترونیک بطرف خواده شد.

شکل 1. بلوک دیاگرام استاندارد تشخیص سریع برخط

مأموریت اصلی انتلاف تشخیص سریع برخط تغییر روشنی‌های احراز هویت برخط تعیین شد. نسخهٔ اول پروتکل‌های تشخیص سریع برخط در 9 دسامبر سال 2014 میلادی منتشر شد. این انتلف از طرفیکی به طیف گسترده موارد استفاده و حالات استقرار دو پروتکل متفاوت ارائه می‌دهد. که به‌طور مستقیم با اینترنت اشیا در ارتباط است و از موارد مهم کاربرد آن برای دسترسی به داده‌های عظیم و به‌همیث سازمان‌های است. دو پروتکل هستند که در ادامه به توضیحات آنها می‌پردازیم.

1. Universal Authentication Framework (UAF)

یک پروتکل فاقد کلیه‌ای عبور که از ورگی‌های زیست‌شناسی کاربران برای احراز هویت استفاده می‌کند. این پروتکل اجازه می‌دهد یک دستگاه فعال مثل لفن همراه هوشمند یا تبلت در یک سرور یا وب سایت پشتیبانی کننده تشخیص سریع برخط را به کاربر می‌دهد. کاربر دستگاه و سرویس‌های دقیق داده‌هایی قابلیت UAF را حسب می‌کند یا یک pin یا کارت سیستمی محلی ارائه می‌دهد. در این راه‌های کاربر دستگاه خود را از طریق انتخاب یکت مکانیسم احراز هویت محلی مانند اثر انگشت، نگه‌گاه به دوربین، صحیح

1. Universal Authentication Framework (UAF)
با میکروفن، وارد کردن Pin و ... ثبت می کنید. پروتکل UAF به سرویس این امکان را می دهد. که مکانیسم های ارائه شده به کاربر را انتخاب کند. پس از ثبت نام اولیه، کاربر به سادگی می تواند عملیات احراز هویت محلی را در هر زمان و مکان انجام دهد. این پروتکل همچنین، امکان تکیب مکانیسم های تایید هویت چندگانه مانند اثر انگشت به همراه را نیز فراهم می کند. پروتکل UAF شامل عملیات ثبت نام، احراز هویت، تأیید تراکنش، و لغو ثبت نام است (شكل 7).

شکل 7. بلوک دیگرام نحوه کار کردن پروتکل UAF

UAF: پروتکلی است که با استفاده از یک کوک ساخت افزاری احراز هویت انجام می دهد.

این پروتکل به منظور احراز هویت کاربر با استفاده از یک فاکتور ثانویه قوی یک کلید لمبیسی بر روی ابزار طراحی شده است. کاربر، دستگاه U2F را که قابلیت کلید لمبیسی بر روی ابزار طراحی شده است، داشته باشد. این راهکار اجازه می دهد که خدمات برخط امتحان زیرساخت رمز عبور موجود خود را با اضافه کردن یک کلید دوم دوم فوی برای ورود کاربر به سیستم تقویت کند. کاربر به سادگی با فشار دادن یک کلید دوم ارتباط برقرار می کند.

1. Universal 2nd Factor (U2F)
2. finger touch
حال برای کاربر برنامه زیر ارائه می‌شود:

```javascript
u2f.register([{
    'version' : 'U2F_V2',
    'challenge' : 'KSDJsdASAS-AIS_AsS',
    'appId' : 'https://www.google.com/facets.json'
}], callback);

callback = function(response) {
    sendToServer(
        response['clientData'],
        response['registrationData']);
};
```

و در ادامه، برای ثبت نام کاربر با استفاده از شماره کلی زیر، اطلاعات اسکن‌شده کدگذاری می‌شود (شکل 8).
شکل 8 کد گذاری در FIDO

شکل 9 ساختار جدید استفاده از FIDO در اینترنت اشبا
ساختار پیشنهادی شکل 9، می تواند تاکنون سطحی در اینترنت اشبا به وجود آورد. در این ساختار در مرحله اول، ویژگی زیست ستندی در دستگاه کاربر ثبت می گردد. این دستگاه می تواند وسایل الکترونیکی شخصی مانند تلفن همراه، تبلت و لپ تاب با سیستم های هوشمند خانگی و اشیا متصل به اینترنت باشد. از طرف دیگر، در سمت کاربر یا سرویس گرندر یک پردازنده کاربردی که با استاندارد FIDO سازگاری دارد، نصب می گردد. این برنامه با پروتکل انتقال در سمت سرویس گرندر از یک سو و با ابزار تحت پوشش از سوی دیگر در ارتباط است، پس از این که اسکن اثر انگشت ثبت گردید، کلید عمومی در سطح کاربر تولید می شود که کلید احراز هویت و تایید هویت است. به جای ارسال عکس اسکن اثر انگشت یا تبدیل آن به کد را با استفاده از زیرساخت کلید عمومی آن با صورت محورمانه ارسال می کند. در مرحله بعد، در سمت سرویس دهنده گوشه انتقال اثر انگشت بررسی می شود و در صورت درستی آن، سرویس دهنده FIDO درستی به اطلاعات برقراری ارتباط را از طریق پردازنده کاربردی جلوگیری می کند. با استفاده از ابزار ثبت اثر انگشت و استاندارد FIDO شرکت یک فعالیت در زمینه فناوری زیست ستندی می تواند با یک پروتکل مشترک و امینت بالا با پردازش زیراکننده، این ایجاد در وابستگی الکترونیکی و شرکت های سازنده تلفن همراه استفاده شود یا در دسترس در صفای پیشرفت و نرم افزار مشابه کاربردی در زمینه اینترنت اشبا و نرم افزارهای تلفن همراه ارائه گردد. در صورتی که این ابزارها مجهز به این استاندارد باشد، امینت برقراری ارتباط آنها با استفاده از یک زبان مشترک تضمین می گردد.

همانطور که در مقالات متعددی در زمینه زیست ستندی بحث شده، در پژوهش‌های پیشین با استفاده از اسکن اثر انگشت می توانستیم با ابزارهای مختلف ارتباط برقرار کنیم. به این صورت که اگر کاسه زیراکننده اثر انگشت افراد استخراج شده و برای سرویس جهت ارسال می گردد که متأسفانه احتمال هارکس و درباره این سرویس حاصل نمی شود. در حالی که در مدل جدید بانکی دیگر، که در زیراکننده اثر انگشت افراد به زیرساخت کلید عمومی تبدیل شده و جابجایی می شود، در این حالت چالش حفظ حریم اخلاقی نیز بر روش فشرده ای می شود، سپس که اطلاعات کلید عمومی روی سرور قرار می گیرد و حتی هک شدن سرویس باعث از بین رفتن اطلاعات زیست ستندی افراد نمی شود. بنابراین، استاندارد FIDO می تواند تفاوت های مؤثری در برقراری ارتباط با اشبا
و احراز هویت افراد برای دسترسی به داده‌های مهم ایجاد کننده. همچنین، تشخیص هویت
فرد از افراد مختلف بسیار سریع تر با دقت بالاتری صورت می‌پذیرد. این در حالتی
است که در شیوه‌های قدیمی این بررسی بسیار زمانبر و پرهزینه بوده است. با استفاده
تکنیکی از پروتکل‌های TLS نام گذاری که TLS تأیید هویت یک طرف به دوطرفه برای دسترسی
رمزشده، به شکل‌ها فراهم می‌شود و بخش هایی مانند حفاظت از بسته‌داده، محدود‌نمرده
و بهینه‌سازی اندزه‌بسته و انتخاب یک‌گره ای‌گیر توسط TLS توسط یک مکان‌پذیر
می‌شود. در نهایت، می‌توان نتیجه گرفت که امنیت و کیفیت ارتباط بین دو طرف بستگی
به نوع این‌گیره‌های توافق‌صدای بین آنها دارد. استاندارد FIDO امکان پذیر
ارتباط در شبکه می‌تواند تجربه زیادی در زمینه استفاده مؤثر از اینترنت اشیا به وجود
آورد. در راه‌های ارائه‌شده‌های دومه و پیچیدگی احراز هویت به طوری چشم‌گیر کاهش
می‌یابد و کاربران به جای به کار گیری کلمات عبور می‌توانند با استفاده از روش‌های
کاربرسپند نظر اثر انگشت، تشخیص چهره و ... احراز هویت شوند.

از مهم‌ترین مزایای استفاده از راه‌های استاندارد FIDO می‌توان به موارد زیر

اشارد کرد:

1. یک‌سانی از همه سناریوهای احراز هویت (اثارگشت، تشخیص چهره، صدا و ...؟)
2. کاهش پیچیدگی و هزینه احراز هویت;
3. امکان استفاده از قابلیت‌های امنیتی دستگاه‌های موجود نظیر تلفن همراه هوشمند,
4. تبلت‌ها و ...؟
5. کاهش خط افت اطلاعات کاربران در اثر نفوذ به سرور;
6. کاهش نیاز کاربران برای به خاطر سیردن کلمات عبور.

تعاریف مهمی در این زمینه وجود دارد که به اهم‌اندیشی می‌پردازند.

دستگاه احراز هویت کننده: دستگاهی که به وسیله آن احراز هویت زیست‌سنجی
صورت می‌گیرد.

طرف اعتماد کننده: به برنامه‌کاری‌گری گفته می‌شود که به سرور اعتماد می‌کند و جهت
احراز هویت کاربران خود از این سرور استفاده می‌کند.

سرویس دهنده: واحدی که وظیفه اجرای فرایند احراز هویت و نگهداری اطلاعات کاربران
را بر عهده دارد.
سرویس گیرنده: بخشی از برنامه کاربر که به روا دستگاه کاربران اجرا می‌شود و جهت احراز هویت ارتباط لازم را با سرویس دهنده برقرار می‌کند.

5. باقی‌ها

اینترنت آشیا به چند دلیل نسبت به خطرات، ضعیف عمل می‌کند و شکنده است. اول این که اغلب، از عناصر آن مراقبت نمی‌شود و ممکن است به طور فیزیکی در معرض خطر باشند. از طرف دیگر، با توجه به این که ارتباطات بیشتر از طریق بی‌سیم است، استراق سعی به ساده‌ترین شکل ممکن خواهد شد. در نهایت این که، بیشتر عناصر اینترنت آشیا به نظر ارزی و چه از لحاظ مالی، رابطه ای، یا پایین‌تر با رخوردارند و بنا براین، نمی‌توانند مسئولیت بپذیرند استقلال ایمنی را اجرا کنند.

به‌طور خاص، مشکلات بزرگ بیشتر مربوط به تصمیم‌گیری و یکپارچه‌سازی داده‌های مانند توصیف هویت کاربران، بسیار سخت است، چرا که نیازمند زیرساخت‌ها و سرویس‌های است که از طریق انتقال پایه‌ای مناسب با دیگر گروه‌ها به اهداف خود دست پیدا می‌کند. در اینترنت آشیا چنین رویکردهایی امکان‌پذیر نیستند، زیرا برچسب‌های RFID تعداد بسیار بالا‌های پیام را نمی‌توانند به سرورها انتقال دهد و این مسئله در مورد گروه‌های حساس نیز صادق است. طی سال‌های اخیر، راهحل‌های بسیاری برای RFID سیستم‌های بیشتری شده است. اگرچه هنوز مشکل آن گونه که پایین حلق نشده است و با مسائل جدی رو به رشد، اما در این مقاله راه‌حل جدیدی برای حل این مشکل به وجود می‌آید. در واقع، هیچ کدام از راه‌حل‌های موجود نمی‌توانند در حل مشکل هم معروف هستند، گفته کند. راهحل‌های man-in-middle attack که به هنوز مشکل RFID اطلاعات را در مسیر به دو تغییر انتقال دهد. مسائل و مشکلات جدیدی ممکن است پیش بیاید. وقتي سیستم‌های RFID با اینترنت ادغام می‌شوند، در بیشتر موارد آنها به‌درستی کنترل نمی‌شود. داده‌ها ممکن است در زمانی که ذخیره می‌شوند و یا از شبکه عبور می‌کنند، توسط حمله کننده‌ها تغییر پیدا کند. برای حفاظت از داده‌ها و اطلاعات در برایر اولین نوع حمله در سیستم از تکنولوژی‌های دارای برچسب، حافظه محفظته می‌شود و

1. Proxy
راه حلی برای شیبک‌های حسگر پی سیم ارائه نشده است. برای حفاظت از داده‌ها در مقابل دومن نوع حمله‌ها، پیام‌ها بر اساس الگوی HMAC حفاظت می‌شوند. این حفاظت بر اساس یک کلید رمز مشترک بین بخش مورد مقصود پیام است که با یک عملکرد ادغامی به کار می‌رود تا آنیت لازم را ریزی و بی‌پایان. بدون اطمینان از خصوصی بودن در دنیای حسگرهای متقابل به هم و دستگاه‌ها، کاربران نمایندگان که این تکنولوژی‌ها را پذیرفته‌اند. گزارش واحد ارتباطات مخابراتی بین المللی در مورد پیشرفته و ارتباط اینترنت بیان می‌کند که نگرانی‌ها در مورد حضور خصوصی و حفاظت داده‌ها گسترده شده است؛ به‌ویژه این که حسگرهای برجسته‌ای هوشمند می‌توانند حرفه‌های کاربر، عادات او و رفتارها در حالت کلی، برای پیاده‌سازی و استفاده از فناوری FIDO ابتدایی طبق مراحل شکل 10 ثابت نام کاربر انجام شود. در این ساختار شناسایی و تشخیص هویت ابتدایی در 28 مرحله صورت می‌پذیرد که از این کاربرد می‌توان در کاربردهای بانکداری الکترونیکی برای دسترسی به داده‌ها و اینترنت اشبی بهره برد.

شکل 10: ساختار کلی فراکنید ثبت زیست‌سنجی در تکنولوژی FIDO
در طول عملیات ثبت نام در سمت کاربر، به کاربران اجازه داده می‌شود که خود را به یک یا چند شاخص احراز هویت کنند. کدهای قابل پذیرش بایستی از ثبت ثبت نام کننده در این مرحله در سمت کاربر پیدا کنند. در بازار شبکه‌های قابل پذیرش بایستی از کلید عمومی بی‌سرویس ارسال و کلید خصوصی به صورت آنلاین در سمت کاربر ذکر شود. سرویس ارسال کلید استفاده از کلید احراز هویتی که قبلی‌تر منتشر شده است، اصلی بودن احراز هویت کننده را بررسی می‌کند و بین تریب‌ها، خطر جعل عنوان یا تغییر هویت به حذافل می‌رسد. آغاز فرآیند ثبت نام به این صورت است که درخواست ثبت نام کاربر جدید به سرویس ارسال می‌شود. سپس سرویس لیست احراز هویت کننده‌های قابل پذیرش و سیاست قابل پشتیبانی را به کلیه ارسال می‌کند. ثبت نام کردن کاربران انتخاب شده و منطقه بر تولید زوج کلید است. کلید عمومی به سرویس ارسال می‌شود و در آخر تایید احراز هویت کننده با استفاده از کلید تایید انجام می‌گردد (جدول ۶).

جدول ۶. ساختار کلی فرآیند ثبت

<table>
<thead>
<tr>
<th>شرح فرآیند ثبت نام</th>
<th>ردیف</th>
</tr>
</thead>
<tbody>
<tr>
<td>ابتدا درخواست کاربر در مورورگ وارد می‌شود.</td>
<td>1</td>
</tr>
<tr>
<td>درخواست به رپر (relying party) که می‌تواند برگه‌ای کاربردی یا سرویس دهنده آن را ارسال می‌کند.</td>
<td>2</td>
</tr>
<tr>
<td>صفحه ورود به سیستم مورد نظر داده می‌شود.</td>
<td>3</td>
</tr>
<tr>
<td>فرم ورود به سیستم برای کاربر نامهای داده می‌شود.</td>
<td>4</td>
</tr>
<tr>
<td>نام کاربری و رمز عبور در این بخش وارد می‌شود.</td>
<td>5</td>
</tr>
<tr>
<td>فرم ورود به سیستم ثبت می‌گردد.</td>
<td>6</td>
</tr>
<tr>
<td>در این مرحله درستی ثبت نام کاربری و رمز عبور بررسی می‌شود.</td>
<td>7</td>
</tr>
<tr>
<td>پیام متن‌سازی فرآیند ثبت نام به سرویس دهنده ارسال می‌شود.</td>
<td>8</td>
</tr>
<tr>
<td>درخواست ثبت را تولید کد.</td>
<td>9</td>
</tr>
<tr>
<td>UAF reg. request.</td>
<td>10</td>
</tr>
</tbody>
</table>

1. provisioning
<table>
<thead>
<tr>
<th>ردیف</th>
<th>شرح فرایند لیست نام</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>UAF reg. request + session binding</td>
</tr>
<tr>
<td>12</td>
<td>UAF reg. request + App ID + TLS binding</td>
</tr>
<tr>
<td>13</td>
<td>Retrieve list of Facet IDs identified by app ID (URL)</td>
</tr>
<tr>
<td>14</td>
<td>Return facet ID list</td>
</tr>
<tr>
<td>15</td>
<td>Select authenticator according to policy</td>
</tr>
<tr>
<td>16</td>
<td>Trigger registration</td>
</tr>
<tr>
<td>17</td>
<td>Generate KHAccess Token</td>
</tr>
<tr>
<td>18</td>
<td>Trigger registration</td>
</tr>
<tr>
<td>19</td>
<td>Trigger user verification</td>
</tr>
<tr>
<td>20</td>
<td>Verify user</td>
</tr>
<tr>
<td>21</td>
<td>Generate Uauth key pair specific to App ID (and username)</td>
</tr>
<tr>
<td>22</td>
<td>Return KRD object (incl. attestation and Uauth.pub)</td>
</tr>
<tr>
<td>23</td>
<td>Return KRD</td>
</tr>
<tr>
<td>24</td>
<td>Return UAF reg. response (contains KRD)</td>
</tr>
<tr>
<td>25</td>
<td>Return UAF reg. response (contatains KRD)</td>
</tr>
<tr>
<td>26</td>
<td>Send UAF reg. response</td>
</tr>
<tr>
<td>27</td>
<td>Verify attestation and store new Uauth. publickey</td>
</tr>
<tr>
<td>28</td>
<td>Return verification result</td>
</tr>
</tbody>
</table>

در مرحله بعد، هویت گوینده تصمیم و مطابقت با اطلاعات لیست شده از کاربران در مرحله انجام می‌شود. دیگر کام تصدیق هویت گوینده در پروتکل UAF به مرحله می‌رود. در شکل 11، نشان داده شده است.
فرآیند احراز هویت شامل دو بخش است: احراز هویت محلی کاربر به کلاینت و احراز هویت کلاینت به سرور. احراز هویت به سرور با استفاده از پروتکل Challenge-Response اجرا می‌شود و درخواست احراز هویت سرور یک کلاینت تولید می‌کند و به کلاینت می‌فرستد. سرور همچنین، یک چرخه احراز هویت کننده قابل پذیرش را اعلام می‌کند و کلاینت نیاز به احراز هویت کننده‌ها انجام می‌دهد که اگر در درخواست انجام می‌دهد اجرا نماید (جدول ۱). در نهایت، این فرآیند دارای مراحل زیر است:

۱. آغاز مرحله احراز هویت و ارسال شناسه برنامه کاربردی و نام کاربردی به سرور;
۲. ارسال جالش و سپس به کلاینت توسط سرور;
۳. احراز هویت کاربر با استفاده از احراز هویت کننده انتخاب‌شده مطابق بر سیستم سرور مانند اثر انگشت;
۴. ارسال پاسخ احراز هویت به WEB APP.
5. تأیید اعتماد پاسخ احراز هویت با کلید عمومی.

جدول 7. ساختار کلی فرایند ثبت زیست سنجی در تکنولوژی FIDO

<table>
<thead>
<tr>
<th>شرح فرایند ثبت نام</th>
<th>رنگ</th>
</tr>
</thead>
<tbody>
<tr>
<td>ابتدا درخواست کاربر در مرورگر وارد می شود.</td>
<td>Open URL 1</td>
</tr>
<tr>
<td>درخواست به RP یا relying party که می‌تواند برنامه کاربردی یا سرویس به دشته باشد، ارسال می شود.</td>
<td>Open https URL 2</td>
</tr>
<tr>
<td>صفحه ورود به سیستم به مورگ نشان داده می شود.</td>
<td>http OK + legacy login form 3</td>
</tr>
<tr>
<td>فرم ورود به سیستم با رای کاربر نمایش داده می شود.</td>
<td>Show legacy login form 4</td>
</tr>
<tr>
<td>نام کاربری و رمز عبور در این بخش وارد می شود.</td>
<td>Enter legacy password and submit 5</td>
</tr>
<tr>
<td>فرم ورود به سیستم ثبت می‌گردد.</td>
<td>Submit form 6</td>
</tr>
<tr>
<td>در این مرحله درستی نام کاربری و رمز عبور بررسی می شود.</td>
<td>Verify password 7</td>
</tr>
<tr>
<td>پیام آماده سازی فرایند ثبت نام به سرویس دهنده ارسال می شود.</td>
<td>Trigger UAF reg. request 8</td>
</tr>
<tr>
<td>درخواست ثبت را تولید می کند.</td>
<td>Generate reg. request 9</td>
</tr>
<tr>
<td>درخواست ثبت برای RP ارسال می شود.</td>
<td>UAF reg. request 10</td>
</tr>
<tr>
<td>پیام ثبت را به کاربر نشان می دهد.</td>
<td>UAF reg. request + session binding 11</td>
</tr>
<tr>
<td>مرورگر درخواست ثبت را دریافت می کند.</td>
<td>UAF reg. request + App ID + TLS binding 12</td>
</tr>
<tr>
<td>فرایند TLS را بررسی می کند. کلاس هم گویا هنامه دارد. برای این که آگ کسی در حین برقراری ارتباط شود کنن، تنواند و برای کاربر واقعی دسترسی ایجاد شود.</td>
<td>Retrieve list of Facet IDs identified by app ID (URL) 13</td>
</tr>
<tr>
<td>بررسی می شود از کدام وب سایت با برنامه کاربردی ارتباط برقرار شده است.</td>
<td>Return facet ID list 14</td>
</tr>
<tr>
<td>در سمت سرویس گیرنده FIDO قوانین و دسترسی ها را استخراج و فراخوانی می کند (برای مثال این که چه یکی قیمت سنجی را باشد شناسایی کنن، مثل اثر انگشت).</td>
<td>Select authenticator according to policy 15</td>
</tr>
<tr>
<td>سرویس گیرنده پیام را به رابط می فرستد.</td>
<td>Trigger registration 16</td>
</tr>
<tr>
<td>رابط پیک تاکنو دسترسی تولید می کند و به همراه پیام آن را به ابزار ثبت سنجی ارسال می کند.</td>
<td>Generate KHAccess Token 17</td>
</tr>
<tr>
<td>دسترسی ارسال می شود.</td>
<td>Trigger registration 18</td>
</tr>
<tr>
<td>فرایند ثبت اثر انگشت انجام می شود.</td>
<td>Trigger user verification 19</td>
</tr>
</tbody>
</table>
در نهایت، سرویس دهنده بر روی زیرساخت طرف اصلی - منکی 1 اجرای می‌شود.

سرویس گیرنده بخشی از برنامه کاربر است که بر روی دستگاه کاربر اجرای می‌شود. احراز هویت کننده با دستگاه کاربر یکپارچه است و پس از طلایش این مراحل کاربر می‌تواند به راحتی به سیستم متصل شود.

همچنین، ایجاد دیگری که می‌توان مورد ارزیابی قرار داد، استفاده از چندین روش احراز هویت به صورت همزمان است که دقت و امنیت سیستم بالا را تضمین خواهد کرد.

بحث

با توجه به نتایج به دست آمده، هر سیستم می‌بایست سنجی شامل موارد زیر است:

1. ابزار اندازه‌گیری: ابزار اندازه‌گیری واسط کاربر را تشکیل می‌دهد. وابسته استفاده، یک فاکتور مهم دیگر برای سنجش کاربر است. ابزار با این مزایا باید غیرپیش باشد و فضای کمی برای خطا انجاد کننده. این ابزار همچنین، با ابزار قابل استفاده برای دامنه وسیعی از مردم و به‌ویژه برای افراد ناتوان باشد.

1. relying party
در این فیلد، بررسی می‌کنند که آیا فرد با هویت ادعاهده مطابق است یا خیر؟

1. identifi cation
2. verifi cation
تأیید فقط شامل مقایسه با یکی قابل خاصی است که ادعا شده است. بنابراین، از استفاده می‌شود که هدف از آن چگونگی برای استفاده از یکی همیشه افراد متعدد است (DINardo 2008). در پی بررسی از طریق زیست‌سنجی و روش‌های مختلف مورد همگام قرار می‌گیرد. این نوع حملات شامل حمله به پایگاه داده، حمله به پردازه ورودی سیستم، و حمله به سیستم شناسی هویت از طریق زیست‌سنجی جعلی است. سفارقان معمولاً جهت فرض سیستم‌های تشخیص هویت از روش‌های مختلفی بهره می‌برند؛ از جمله: استفاده از عکس جهت یا نسبت فرد متقابل دور، ضبط باکیفیت صدای شخص در سیستم‌های زیست‌سنجی جعلی، استفاده از اثر انگشت زلزلی و حتی استفاده از لاش‌انگشت توسط سفارقان جهت ورود به سیستم. فرآیند تشخیص هویت می‌تواند هم از طریق نرم‌افزاری (خواندن و پردازش اطلاعات زیست‌سنجی) باشد و هم از طریق سخت‌افزاری که در امر تشخیص به ما کمک می‌کند. یک روش برای جلوگیری از حمله به سیستم تشخیص هویت (جلوگیری از ورود زیست‌سنجی جعلی)، استفاده از سیستم زیست‌سنجی های ترکیبی و افراشی تخداد زیست‌سنجی های سنجش هویت است. هرچند این روش ممکن است افراشی هزینه و صرف وقت بیشتری را در پی داشته باشد، اما بسیار مفید است (Jain, Kumar & Ross 2015). راه حل نهایی جهت کاهش آمدن بر مشکلاتی که علیه از فناوری زیست‌سنجی به همراه دارد، استفاده همزمان از چند زیست‌سنجی مختلف در یک سیستم است. به این روش اصطلاحاً سیستم چندپاره گفته می‌شود. در بعضی از سیستم‌های فوق امتحانی، متخصصان از روی لایه‌ای استفاده می‌کنند. سیستم‌ی چندپاره‌است که جهت روش شناسایی از طریق زیست‌سنجی را با هم ترکیب می‌کند؛ مثل اسکن عنبیه و الگوی صدا. و بدین ترتیب ضرب امتیاز را افزایش می‌دهد. برای این کار ابزار به محاسبه اولویت‌ها پردازش و بر اساس بیشترین امتیاز، تکنیک را انتخاب کنیم. در این مرحله به این صورت عمل می‌کنیم که ابزاری یا یگانی مربوط به هر تکنیک بر اساس معیار خاص، را در وزن همان معیار ضرب کرده و به هم جمع می‌کنیم. به این ترتیب، اولویت هر تکنیک محاسبه می‌شود:

1. layered
2. multimodal
با توجه به نتایج به دست آمده در نمودار شکل 12، مشاهده می‌شود که زیست‌سنجی اثر انگشت دارای بالاترین اولویت نسبت به دیگر زیست‌سنجی‌های دیگر. پس از آن ضریب به کلید بالاترین اولویت را دارد. نتایج حاصل از آزمون تناسب‌رسی به پایگاه‌های داده بزرگ از اینگونه اثرات به کارگیری زیرین ممکن است و با مستند کردن شوی برای استفاده در اینترنت اشیا و دسترسی به مطمئن‌کردن داده‌ها به‌همراه داده به کلید بالاترین اولویت را دارد و سطح امنیت بالایی را برای سیستم برقرار می‌کند.

جدول 8: نتایج ارزیابی تکنیک‌های زیست‌سنجی بر اساس 7 ویژگی

<table>
<thead>
<tr>
<th>زیست‌سنجی</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
<th>عملکرد مشوق</th>
</tr>
</thead>
<tbody>
<tr>
<td>تشخیص اثر انگشت</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
</tr>
<tr>
<td>تشخیص چهره</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>تشخیص عنیه</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>تشخیص هندسه</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
<td>بالا/متوسط</td>
</tr>
<tr>
<td>دست تشخیص کف دست</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>تشخیص سدا</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>تشخیص امسال</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>تشخیص راه رفتین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>پروفاک پرفتار</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>ضریب به کلید</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
<tr>
<td>لمس دینامیک</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
<td>بالا/پایین</td>
</tr>
</tbody>
</table>
با یک بررسی اجمالی در نتایج ارائه‌شده در جدول ۸ می‌توان به این نتیجه رسید که تکیک‌های زیست‌سنجی فیزیولوژیکی دارای نتایج بهتری نسبت به تکیک‌های زیست‌سنجی رفتاری هستند. بنابراین، احتمال موافقت در استفاده از زیست‌سنجی فیزیولوژیکی در کاربردهای مختلف بالاتر از تکیک‌های رفتاری است.

۷ نتیجه گیری

امروزه استفاده روزافزون از اینترنت توسط عموم جامعه و ارائه خدمات الکترونیکی توسط بنگاه‌های اقتصادی و تجاری از طرفی و گسترش ابزار و تجهیزات و روش به فضاي سایبر از طرف ديگر، اهمیت تامين امتیا تبادل اطلاعات در فضای مجازی را روز به روز پرورنگتر می‌کند؛ چرا که هر هم‌مان با گسترش اینترنت و ارائه انواع خدمات با این فناورى، نفوذ افراد غيرمجاز و سوء استفاده کنندگان بهطور فراينده پيچيده و گستردگي شده است. لذا، ابتدا و تدوين راهگار های جديد و پيشرفت تامين تبادل اطلاعات، بهطور مداوم مورد نياز بوده و در حال انجام است. در اين مقاله به تعريف و پژوهي هاي اساسى اينترنت اشيا، توصيف فناورى هاي مورد نياز آن و همچنين، پيشيني برنهماى كاربردی برای دسترسي امن پرداختيم. علاوه بر اين، درباره حالش عمداىى كه در راه تحقق اينترنت اشيا با آنها مواجه هستيم، بحث شد و روش بيشندايى اى استفاده از ويزيگى های زیست‌سنجی شرح داده شد. بنا توجه به اين كه اينترنت به شکلي بسيار گستردگي نوحه زدنگي ما را تغيير داده است، ارتباطات مردم در سطح مجازی را چه در حيطة شغلي و در پا در روابط اجتماعي تحت تاثير قرار داده است. اينترنت اشيا نيز اين پانيل را دارد كه بعده ديگری را به اين فرآيند اضافه كند و ارتباط بين اشیاء هوشمند را با استفاده از روش هاي اينترنت و جديد ممكن سازد و در نتیجه به چشم‌انداز «هر زمان، هر كجا، هر رسانه، هر چيز» دنيای ارتباطات دست پیدا كند. گسترش نسل جديدى از اشیاء مجهم به همکارى مصنوعي به همراه توانايي پر قرار ارتباط و حرکت باعث حرکت سریع برای تحقيق اينترنت اشيا شده است. با توجه به اين تاملان در حال ظهور همچنين یک درجه به یک زنجیره مجازى از اشیاء به پييت و در دایر نشاني در دنیای پيروي شبكه متصل خواهد شد. با توجه به اهميت اتصال اين اشيا به اينترنت و دسترسى به آنها، از ويزيگى های زیست‌سنجی به عنوان شناسه استفاده مي‌شود. زيرا آنها را نمي‌توان امانت داد یا خريد یا فراموش کرد و خيلي دشوار است كه بتوان آنها را جعل نمود. در اين مقاله با استفاده از ويزيگى های...
زیست سنگی و استاندارد تشخیص سریع برخط، دسترسی ایمن تر به اینترنت اشیا بررسی شد و با توجه به آن می‌توانیم شاهد پیشرفت‌های چشمگیری در این زمینه باشیم.

محدودیت‌ها: از یک نظر، اینترنت اشیا شبکه‌ای از موضوعات فیزیکی (اشیا) را با کمک تکنولوژی جامعی شده و مورد استفاده برای تعاملات داخلی در داخل شبکه و برای تعاملات اینترنتی و محیط تکنولوژی خانه‌های هوشمند، شبکه هوشمند ارتباطات مانند برتریت کنترل و سیستم‌های ناهنجاری و پیش‌بینی آزمایش و آزمایش‌های مبتنی بر اینترنت و روش‌های مبتنی بر اینترنت کار می‌کنند. این مبتنی بر مفهوم اینترنت اشیا است که ممکن است داشته باشد در درسته‌های اینترنت اشیا یا با طور مختلف در سطح پایه‌ای، اینترنت اشیا در واقع معنا مرتبط با در دست سیستم‌های هوشمند و هوشمندتر محقق شود. همانند دیگر فناوری‌های جدید، اینترنت اشیا نیز می‌تواند در ابتدا مفهومی سردرگم کننده به علت پیامدهای ذیل و همچنین اینکه با‌وجود آن می‌تواند مفاهیم جدید و ویژگی‌های بی‌پایان از نظر دیگر، با توجه به چالش‌های امتحان‌های موجود برای برقراری ارتباط باید با توجه به اقدامات انجام شده، برای برطرف نمودن چالش‌های امتحانی استفاده از زیست‌سنگی پیشنهاد می‌شود. البته باید در نظر داشت که سیستم‌های زیست‌سنگی هر چند کام به نتایج دارای ضعف‌هایی هستند که برای برطرف شدن این ضعف‌ها سیستم‌زیست‌سنگی ترکیبی پیشنهاد می‌شود. با توجه به اینکه در ترکیب کردن مجدد زیست‌سنگی ها محدودیت‌هایی از قبیل هزینه و یپچی‌گی پیاده‌سازی وجود دارد، یک ترکیب بهینه برای سیستم اینترنت اشیا معرفی کرده‌میا. با TIDO توجه به نتایج حاصل از تحلیل سلسله مراتبی ترکیب اثر انتخاب در اساس تکنولوژی FIDO و ضریب به کلید را به عنوان ترکیب بهینه معرفی می‌نماییم.

پیشنهادهای برای آینده: اینترنت اشیا ممکن است جهش بزرگی و به جلو بیدری در ICT بخش را موجب شود. احتمال ادامه یکپارچه جهان واقعی و مجایی از طریق گسترش
عظمی دستگاه‌های تعیین‌شده، مسیرهای مهیج و جدید، هم برای پژوهش و هم کسب و کار ایجاد می‌کند. با اجرای این شیوه، در نهایت ممکن است محیط پرآمون بشر به جزیی شبیه آنچه که در فیلم‌ها و داستان‌های تخیلی اشاره می‌شود، نزدیک شود. به عنوان مثال، بهره‌گیری از این روش باعث می‌شود که کلیه وسایل هوشمند پرآمون‌ها پویانداز در زمان مشخص فعال شده، فعالیت از قبل تعیین‌شده را انجام داده و سپس خاموشی شوند. امیدواریم که این بررسی برای پژوهشگران و شاغلان در این زمینه مفید واقع شود و به آن‌ها برای درک و فهم پتانسیل بزرگ اینترنت اشیا و دسترسی از طریق روش پیشنهادی کمک کند. نا را حل‌های فنی نوآورانه‌ای را تدبیر کنند و در آینده‌های نزدیک شاهد آن باشیم که اینترنت اشیا از یک دیدگاه پژوهشی به یک هدایت کاربردی تبدیل شود.

فهرست منابع


