A Method for FIDO Management through Biometric Technology in IOT

Azamsadat Parei
MA in Information Technology Engineering - electronic Commerce;
K. N. Toosi University of Technology as.parei@gmail.com

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

Iranian Journal of Information Processing and Management

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

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 33 | No. 2 | pp. 793-828
Winter 2018
https://doi.org/10.35050/JIPM010.2018.082

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. Furthermore, the authentication of individuals is a more accurate and faster process. 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

ارائهٔ رویکردی برای مدیریت تشخیص سریع برخط با استفاده از فناوری بیومتریک در اینترنت اشیا

اعظم‌السادات پرئی
کارشناسی ارشد؛ گروه فنّاوری اطلاعات؛
دانشکدهٔ مهندسی صنایع؛ دانشگاه صنعتی خواجه نصیرالدین طوسی as.parei@gmail.com

حجت‌اله حمیدی
دکتری کامپیوتر؛ استادیار؛ گروه فنّاوری اطلاعات؛
دانشکدهٔ مهندسی صنایع؛
دانشگاه صنعتی خواجه نصیرالدین طوسی؛
پدیدآور رابط h_hamidi@kntu.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۳۹۵/۱۱/۱۰ **پذیرش:** ۱۳۹۵/۱۲/۲۴ مقاله برای اصلاح به مدت ۷ روز نزد پدیدآوران بوده است.

فصلنامه | علمی پژوهشی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۳ | شمارهٔ ۲ | ص‌ص ۷۹۳-۸۲۸
زمستان ۱۳۹۶
https://doi.org/10.35050/JIPM010.2018.082

چکیده: اینترنتِ اشیا مفهومی جدید در دنیای فنّاوری و ارتباطات است که قابلیت ارسال داده‌های فنّاوری برای تمام اشیا را از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌آورد. فنّاوری زیست‌سنجی کاربردهای فراوانی دارد که هدف اصلی آن تهیهٔ یک جانشین مناسب برای سیستم‌های کنترل دسترسی سنتی است و برای حفاظت شخصی یا دارایی‌های سازمانی استفاده می‌شود. استفادهٔ همزمان از فنّاوری زیست‌سنجی و تشخیص سریع برخط می‌تواند تفاوت‌های مؤثری در برقراری ارتباط با اشیا و احراز هویت افراد برای دسترسی به داده‌های مهم ایجاد کند. همچنین، تشخیص هویت فرد از افراد مختلف بسیار سریع‌تر و با دقتی بالاتر صورت می‌پذیرد. این در حالی است که این بررسی در روش‌های قدیمی بسیار زمان‌بر و پرهزینه است. در این مقاله برای مدیریت تشخیص سریع برخط در اینترنت اشیا، به معرفی رویکردی جدید جهت استفاده از زیست‌سنجی در اینترنت اشیا پرداخته شده است. با توجه به نتایج به‌دست‌آمده مشاهده می‌شود که زیست‌سنجی اثر انگشت دارای بالاترین اولویت نسبت به سایر تکنیک‌های زیست‌سنجی برای استفاده در اینترنت اشیا بوده و دارای پایین‌ترین هزینه برای پیاده‌سازی است. به‌علاوهٔ این‌که زیست‌سنجی اثر انگشت سطح امنیت بالایی را برای مدیریت سیستم برقرار می‌کند.

کلیدواژه‌ها: اینترنت اشیا، فنّاوری بیومتریک (زیست‌سنجی)، تشخیص سریع برخط، مدیریت اطلاعات

۱. مقدمه

اینترنت اشیا[1] این‌گونه تعریف می‌شود: زیرساختار شبکهٔ جهانی پویا که دارای قابلیت‌های خودپیکربندی بر اساس پروتکل‌های ارتباطی استاندارد و هم‌کنش‌پذیر است؛ جایی که در آن «اشیا» فیزیکی و مجازی دارای هویت، مشخصهٔ فیزیکی و شخصیت مجازی هستند، از واسط‌های هوشمند استفاده می‌کنند، و به‌طور بی‌نقص با شبکهٔ اطلاعات ادغام می‌شوند. زیرساخت اینترنت اشیا بر اساس تکنولوژی‌های متعدد تشکیل شده است. از آن جمله می‌توان به موارد زیر اشاره کرد: هوش محدوده‌ای، پروتکل اینترنتی، تکنولوژی‌های ارتباطی (وای‌فای، بلوتوث، زیگ‌بی)، دستگاه‌های تعبیه‌شده (یا حسگر شبکه‌های بی‌سیم)[2] و برنامه‌های کاربردی. سیستم‌های زیست‌سنجی[3]، گروهی از تکنولوژی‌ها و تکنیک‌هایی هستند که با استفاده از ویژگی‌های فیزیولوژی و رفتاری آن‌ها برای تشخیص هویت و شناخت انسان به‌کار می‌روند. یکی از مهم‌ترین مزایای زیست‌سنجی این است که ویژگی‌های بیومتریک را که به‌عنوان شناسه استفاده می‌شود، نمی‌توان امانت داد یا خریداری کرد و خیلی دشوار است که بتوان آن‌ها را جعل نمود. بر خلاف سایر فنّاوری‌های کنترل دسترسی، زیست‌سنجی را نمی‌توان فراموش کرد یا دزدید. به‌عنوان مثال، گذرواژه‌ها به‌راحتی فراموش می‌شوند و کلیدها و کارت‌ها به راحتی ممکن است گم شده یا به زور از ما گرفته شوند، در حالی که با استفاده از ویژگی‌های زیست‌سنجی ارتباط ما با اینترنت اشیا می‌تواند به سهولت و با امنیت بالا برقرار شود. در ادامه، به این مطلب می‌پردازیم. ابتکارات «بنیاد اینترنت اشیا»[4] توسط «فنگ و یانگ»[5] در مورد ساختار هوشمند اینترنت اشیا مورد بررسی قرار گرفته است. علاوه بر این ابتکارات، در مواردی تلاش بر سنجش فعالیت برچسب‌های مجاز با استفاده از RFID[6] همواره مطرح بوده است (Zhang et al. 2014). همچنین، نظریهٔ شواهد (Zhang et al. 2014) و شبکه‌های اجتماعی موقت موبایل (Zhang et al. 2014) ما را به سمت پیشرفت در اینترنت اشیا سوق می‌دهند.

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)

اینترنت اشیا مفهومی جدید در دنیای فنّاوری و ارتباطات بوده و به‌طور خلاصه، فنّاوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیا) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت فراهم می‌شود. بستر اینترنت اشیا بر امواج رادیویی بی‌سیمی قرار دارد که به دستگاه‌های مختلف این امکان را می‌دهد که از طریق اینترنت با یکدیگر ارتباط برقرار کنند.

اینترنت اشیا دامنه و اندازه‌اش را افزایش خواهد داد به شرطی که راه جدیدی از فرصت‌ها پیش روی چالش‌ها باشد (Zeng et al. 2011). بیشتر کشورها برای پیاده‌سازی اینترنت اشیا در سطح خدمات ملی، راهبردهای بلندمدتی ارائه کرده‌اند. به‌عنوان مثال، دسترسی به پهنای باند ژاپن تسهیلاتی را برای ارتباط بین مردم، مردم و اشیا، و اشیا و اشیا فراهم آورده است (Srivastava 2004). به‌طور مشابه، خانه‌های هوشمند در کرهٔ جنوبی مردم را قادر می‌سازد به اشیا از دوردست دسترسی داشته باشند (Giroux and Pigot 2005).

از طرف دیگر، اینترنت اشیا می‌تواند به داده‌ها نیز مرتبط شود. همان‌طور که می‌دانیم انسان همیشه به‌دلیل تمایل برای بهبود وضعیت خود، برای رسیدن به اطلاعات موجود و به‌دست آوردن داده‌های جدید تلاش می‌کند. تجزیه و تحلیل ترافیک داده‌ها شدیداً تحت تأثیر اطلاعات موقعیتی و سپس، تحت تأثیر حریم خصوصی موقعیت هستند (Alur et al. 2016). تولید اطلاعات از داده‌ها برای تنظیم و تعدیل زندگی بسیار مهم و حیاتی است، به‌ویژه این‌که شرکت‌ها نیاز دارند داده‌ها را ذخیره کرده و آن‌ها را تبدیل کنند تا بتوانند با سرعت در جهت رسیدن به اهدافی مانند مزیت رقابتی، تولید محصولات جدید و پیشرفت شرکت گامی به جلو بردارند (Dijkman et al. 2015). با استفاده از داده‌ها می‌توان مقدار زیادی از اطلاعات را در محدودهٔ وسیعی ذخیره، مدیریت و پردازش کرد. علاوه بر این، استفاده از داده‌ها و آنالیز آن‌ها می‌تواند مزایا و تسهیلاتی را برای شرکت‌ها، محققان و مصرف‌کنندگان ارائه کند. در نتیجه، اینترنت اشیا می‌تواند در حفاظت از دسترسی به داده‌های مهم نیز کارایی داشته باشد. علاوه بر این‌ها، امروزه شناسه و رمز کارت‌هایی که به‌کار می‌روند، دسترسی را محدود می‌کنند. اما این روش‌ها به‌راحتی می‌توانند شکسته شوند. پس، غیرقابل اطمینان هستند. تکنولوژی زیست‌سنجی کاربردهای فراوانی دارد که هدف اصلی آن تهیهٔ جانشینی مناسب برای سیستم‌های کنترل دسترسی سنتی است و برای حفاظت شخصی یا دارایی‌های سازمانی استفاده می‌شود.

در ادامه، این مقاله به‌صورت زیر بخش‌بندی شده است. در بخش دوم، دیدگاه‌های

مختلف الگوی اینترنت اشیا به‌صورت جدولی از مقالاتِ بازبینی‌شده ارائه و باهم مقایسه شده‌اند. در بخش سوم، تکنولوژی‌های اصلی و توانمند اینترنت اشیا معرفی شده است و در بخش چهارم، داده‌ها و اینترنت اشیا توضیح داده می‌شود. در بخش پنجم، چالش‌های امنیتی اینترنت اشیا بررسی می‌شود و در بخش ششم، به معرفی تکنولوژی زیست‌سنجی و تشخیص سریع برخط[1] می‌پردازیم. در بخش هفتم، روش پیشنهادی در جهت رفع چالش‌های امنیتی ارائه می‌گردد. در بخش هشتم، یافته‌های مقاله بسط داده شده و در بخش نهم، نتیجه‌گیری ارائه شده است.

۲. مروری بر پیشینهٔ پژوهش

بررسی‌های «مؤسسهٔ تحقیقاتی گارتنر»[2] نشان می‌دهد که تا سال ۲۰۲۰، بیش از ۲۵ میلیارد وسیلهٔ مختلف در جهان از طریق خدمات مبتنی بر اینترنت اشیا به اینترنت یا دیگر شبکه‌های اطلاع‌رسانی متصل خواهند شد. بررسی‌های «شرکت سیسکو»[3] نیز حاکی از آن است که تا عمومیت یافتن پدیدهٔ اینترنت اشیا تنها سه سال زمان باقی است. بنابراین، در سال ۲۰۱۸ ماشین‌ها و سیستم‌های الکترونیکی می‌توانند از طریق اینترنت بدون نیاز به انسان‌ها و حتی بیشتر از آن‌ها با یکدیگر در ارتباط باشند.

۲-۱. زیست‌سنجی

هر خصیصه‌ای از انسان را می‌توان به‌عنوان یک ویژگی در زیست‌سنجی به‌کار برد، به شرطی که دارای ۴ ویژگی زیر باشد:

جهانی‌بودن[4]: همگانی باشد (عمومی‌بودن)؛

تمایز[5]: در دو فرد مشابه نباشد (متفاوت‌بودن)؛

دائمی‌بودن[6]: در طول زمان تغییر نیابد (دوام داشتن)؛

قابلیت جمع‌آوری[7]: یعنی به‌صورت کمی قابل اندازه‌گیری باشد.

در کاربردهای زندگی روزمره سه فاکتور دیگر نیز باید رعایت شود: کارایی (از

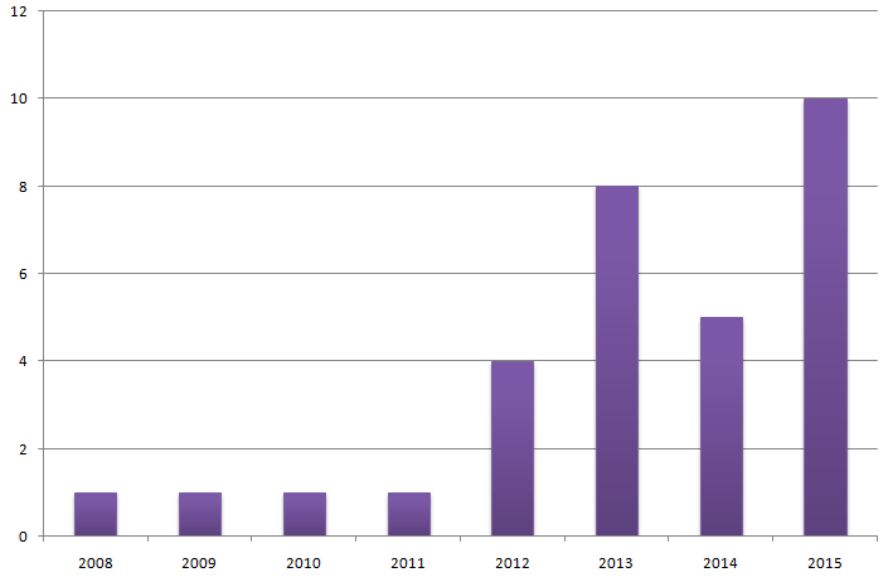
1. Fast Identity Online (FIDO)
2. Gartner Inc.
3. Cisco
4. universality
5. distinctiveness
6. permanence
7. collectability

لحاظ دقت، سرعت)، دسترسی و امنیت بالا (Jain, Nandakumar and Ross 2005). با توجه به این‌که تشخیص سریع و امنیت در حوزهٔ اینترنت اشیا مطرح است، در جدول ۱ و شکل ۱، به بررسی مقالاتی که در مورد کاربرد زیست‌سنجی مطالعه شده، می‌پردازیم.

جدول ۱. مقالات مطالعه‌شده در زمینهٔ زیست‌سنجی

نویسندگان	نام ژورنال	عنوان مقاله	توضیحات
Sharma and Lenka (2013)	International Journal of Engineering and Technology	احراز هویت در سیستم بانکداری برخط از طریق رمزنگاری کوانتومی	در این مقاله یک مدل احراز هویت در سیستم بانکی برخط با رمزنگاری کوانتومی پیشنهادشده است.
Fenker, Ortiz, and Bowyer (2013)	Access, IEEE	پدیدهٔ پیری الگو در تشخیص عنبیه	بررسی اثرات پیری الگوی عنبیه با استفاده از الگوریتم VeriEye و دوربین LG 4000 با ۶۴۴ نمونه
Dedeepya, Swetha, and Raju (2013)	International Journal of Scientific Research in Computer Science	بانکداری تلفن همراه ایمن در دستگاه‌های تلفن همراه هوشمند- رویکرد احراز هویت مبتنی بر الگو	ارائهٔ روش جدید مبتنی بر تجزیه و تحلیل الگوهای ورودی از کاربران بانکداری تلفن همراه مانند طول مدت‌زمان برای ورود داده‌ها، سطح فشار انگشت و ابعاد فیزیکی لمس در هنگام استفاده از یک صفحهٔ لمسی برای مقابله با تهدیدات موجود
Baker et al. (2013)	Handbook of Iris Recognition	پیری الگو در زیست‌سنجی عنبیه	بررسی اثرات پیری الگوی عنبیه با استفاده از سه الگوریتم IrisBEE، VeriEye و Cam-2 و دوربین LG 2200 با ۴۶ نمونه
Masamila (2013)	International Journal of Network Security and Its Applications	پروتکل احراز هویت محلی قوی نظیر به نظیر (P2PSLAP) یک نیاز در بانکداری تلفن همراه	ارائهٔ پروتکل احراز هویت محلی قدرتمند نظیر به نظیر P2PSLAP
Yıldırım and Varol (2014)	International Symposium on Digital Forensics and Security	سیستم‌های امنیتی زیست‌سنجی موبایل برای امروز و آینده	بحث در مورد سیستم‌های زیست‌سنجی موجود برای دستگاه تلفن همراه، سیستم‌عامل و توسعهٔ برنامه‌های کاربردی برای امنیت زیست‌سنجی
Marsico et al. (2014)	Image and Vision Computing	FIRME: تشخیص چهره و عنبیه برای تعامل با موبایل	توضیح تشخیص عنبیه و صورت برای تعامل با موبایل

نویسندگان	نام ژورنال	عنوان مقاله	توضیحات
Czajka (2015)	Biomedical Engineering Systems and Technologies	اثر پیری الگوی عنبیه بر قابلیت اطمینان تشخیص	بررسی اثرات پیری الگوی عنبیه با استفاده از سه الگوریتم VeriEyeMIRLIN ,IRIS – OSIRIS ،BiomIrisSDK و دوربین IrisCUBE با ۵۸ نمونه
Indu and Jain (2015)	Computing for Sustainable Global Development	سیستم امنیتی زیست‌سنجی: بررسی تکنیک‌های زیست‌سنجی ترکیبی برای تولید کلید رمزی	این مقاله بر این‌که زیست‌سنجی چگونه می‌تواند به امنیت بیشتر ابزار کمک کند، تمرکز دارد.
Mohammadi (2015)	Computers in Human Behavior	مطالعه‌ای از وفاداری بانکداری همراه در ایران	بررسی موانع، نقش واسطه از قابلیت‌ها و اثرات تعدیل نوآوری‌های شخصی و هنجارهای ذهنی بر نگرش مصرف‌کنندگان نسبت به استفاده از بانکداری تلفن همراه در ایران
Hamid (2015)	Biometric Technology Today	فنّاوری زیست‌سنجی: جایگزین رمز عبور نیست اما یک مکمل است	بررسی معایب ذاتی در رمز عبور و فنّاوری زیست‌سنجی و نمایش توانایی آن‌ها در ارتباط با استفادهٔ همزمان به‌منظور تقویت امنیت برنامه‌های کاربردی
(Jung and Hong 2015)	Journal of Systems and Information Technology	احراز هویت زیست‌سنجی مبتنی بر تصاویر پروفایل صورت برای امنیت موبایل	احراز هویت زیست‌سنجی مبتنی بر تصاویر پروفایل صورت برای امنیت موبایل



شکل ۱. تعداد مقالات بررسی‌شده بر اساس سال انتشار

۲-۲. اینترنت اشیا

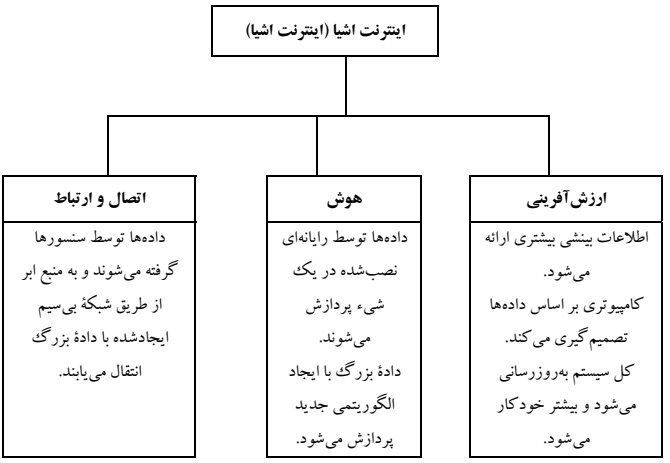
اینترنت اشیا سیستمی است که در آن می‌توان اشیاء امروزی را به قابلیت‌های شناسایی، سنجش، شبکه و پردازش مجهز نمود. از این طریق هر دستگاه می‌تواند با دستگاه‌های دیگر ارتباط برقرار کرده و از طریق اینترنت برای رسیدن به هدفی خاص ارائهٔ خدمت کند. در نهایت، دستگاه‌هایی که از اینترنت اشیا استفاده می‌کنند در همه جا حاضر خواهند بود. در واقع، بسیاری از موضوعات چالش‌برانگیز هنوز باید مورد بررسی قرار گیرند و گره‌های اجتماعی و تکنولوژی قبل از پذیرش گستردهٔ اینترنت اشیا با هم یکی شوند. قوانین اصلی به‌دنبال این هستند که تقابل بین وسایل متصل به هم را تا آنجا که لازم است، امکان‌پذیر ساخته و از طریق توانمندسازی سازش‌پذیری و رفتار مستقل‌شان آن‌ها را همواره در درجهٔ بالایی از هوشمندی نگه دارند و در عین حال، اعتماد، امنیت، و حریم خصوصی را تضمین کنند. در جدول ۲، طبقه‌بندی در مورد مقالات مطالعه‌شده در این زمینه انجام شده است.

جدول ۲. فنّاوری‌های مورد استفاده در اینترنت اشیا

فناوری	مراجع
RFID	(Dominikus 2010; Khoo 2010; Schmidt 2009; Welbourne 2009; Sheng 2010)
NFC	(Broll 2009; Garrido 2010)
شبکهٔ سنسورها	(Hong 2010; Tozlu 2011; Zhu 2010; Li 2013)
میان‌افزار	(Aberer 2006; Bandyopadhyay 2011; Blackstock 2010; De 2011; Dong 2010; Gómez-Goiri and López-de-Ipiña 2010; Huang and Li 2010a; Katasonov 2008; Kiritsis 2011; Puliafito. 2010; Roalter 2010; Song 2010; He and Xu 2014)
معماری جستجوگرها	(Garcia-Macias 2011; Ostermaier 2010)
معماری نرم‌افزار	Castellani 2010, 2011; Gronbaek 2008; Guinard 2011; James 2009; Michael and Darianian 2010; Spiess 2009; Wang 2012
معماری فرایند	(Giner 2010; Kawsar 2010)
عمومی	(Främling and Nyman 2008; Kortuem 2010; Ning and Wang 2011; Xiaocong and Jidong 2010)
زیرساخت‌های هوشمند	(Darianian and Michael 2008; Heil 2007; Li 2011; Liu 2011; Schaffers 2011; Vicini 2012; Fang 2013)
بهداشت و درمان	(Bui and Zorzi 2011; Dohr 2010; Domingo 2012; Jara 2010a, b; Luo 2009; Rohokale 2011)
امنیت و چالش‌ها	(Alcaraz 2010; Babar 2010; Dlamini 2009; Hancke 2010; Mahalle)
حریم خصوصی	(Medaglia and Serbanati 2010; Oleshchuk 2009; Sarma and Girão 2009)
قوانین	(Weber 2009, 2011)
عمومی	(Bandyopadhyay and Sen 2011; Christin 2009; Coetzee and Eksteen 2011; Ma 2011; Mattern and Floerkemeier 2010; Mayordomo 2011; Shen and Liu 2011; Zhang 2011)
مدل کسب‌وکار	(Bohli 2009; Haller 2009; Fu 2011; Li 2012)
آینده‌نگری	(Akyildiz and Jornet 2010; Guinard and Trifa 2009)

فنّاوری شبکه به سمت فنّاوری ارتباط بی‌سیم حرکت می‌کند و به برنامه‌های دستگاه به دستگاه اجازه می‌دهد که با انعطاف بیشتری گسترش یابد. فنّاوری شبکه از سوی شبکه‌ای مستقل که به زمینه آگاه است، استنتاج می‌شود. اشیا به نرم‌افزار تکیه دارند تا با یکدیگر ارتباط مؤثری داشته باشند. نرم‌افزار باید با قابلیت همکاری، اتصال، حریم خصوصی و الزامات امنیتی گسترش یابد. تمرکز توسعهٔ نرم‌افزار بر تغییرات کاربرمحور، اطلاعات انتشاریافته و همکاری ماشین به ماشین و ماشین به انسان است (Farooq et al. 2015). در ایدهٔ اولیهٔ اینترنت اشیا تصور این است که هر روز وسایلی مثل وسایل نقلیه،

یخچال، یخ‌زن، لوازم پزشکی و به‌طور کلی، کالاهای مصرفی به قابلیت سنجش از راه دور و ردیابی مجهز شوند. هنگامی‌که این ایده کاملاً واقعی شد، اینترنت اشیا مانند هر سیستم اطلاعاتی بر ترکیبی از نرم‌افزار و سخت‌افزار و معماری تأکید می‌کند. توابع اصلی اینترنت اشیا در شکل ۲ به تصویر کشیده شده است (Alur et al. 2015).



شکل ۲. توابع اصلی اینترنت اشیا

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

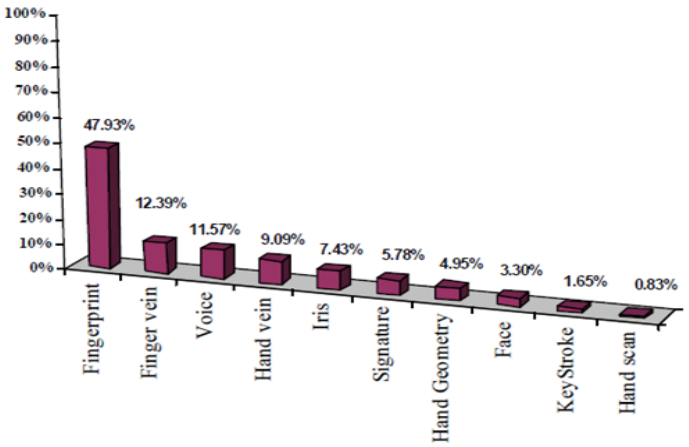
۱. هر چیزی ارتباط برقرار می‌کند: اشیا هوشمند قادر به برقراری ارتباط به‌صورت بی‌سیم در میان خودشان هستند و شبکه‌های تک‌کاره اشیاء متصل را شکل می‌دهند.
۲. هر چیزی شناسایی می‌شود: اشیاء هوشمند با یک نام دیجیتالی شناخته می‌شوند. ارتباطات بین اشیا می‌تواند در قلمرو دیجیتالی، هر زمانی که اتصال فیزیکی را نتوان ایجاد کرد، تعیین شود.
۳. هر چیزی تعامل دارد: اشیاء هوشمند می‌توانند با محیط محلی طی دریافت و به‌کاراندازی قابلیت‌ها در هر زمانی که ارائه می‌شوند، تعامل کنند.

۳. فنّاوری زیست‌سنجی و تشخیص سریع برخط

عملکرد اساسی مورد نیاز در زیست‌سنجی توسط چهار معیار دقت[1]، مقیاس[2]، امنیت[3] و حریم خصوصی[4] اندازه‌گیری می‌شود. برای تمام دستگاه‌های زیست‌سنجی پنج عنصر مشترک وجود دارد. این عناصر عبارت‌اند از ثبت‌نام[5]، الگوی زیست‌سنجی[6]، مقایسه[7]، شبکه[8] و ویژگی‌های زیست‌سنجی شخصی[9].

آقای «منگ» و همکاران طی مطالعه‌ای در سال ۲۰۱۵ تکنیک‌های مختلف زیست‌سنجی را بر اساس هفت ویژگی در حالات مشترک به‌صورت تجربی ارزیابی کرده‌اند. عمومیت، منحصربه‌فردبودن، پایداری، جمع‌آوری، عملکرد، مقبولیت، و عبور از آن ۷ ویژگی بیان‌شده در این مطالعه هستند. این ارزیابی در دو زمینهٔ زیست‌سنجی فیزیولوژیکی و زیست‌سنجی رفتاری انجام شده است. تشخیص اثر انگشت، تشخیص چهره، تشخیص عنبیه، تشخیص هندسهٔ دست و تشخیص کف دست از زیست‌سنجی‌های فیزیولوژیکی بررسی‌شده است و تشخیص صدا، تشخیص امضا، تشخیص راه رفتن، پروفایل رفتار، ضربه‌زدن به کلید دینامیک و لمس دینامیک از زیست‌سنجی‌های رفتاری ارزیابی شده است. در مقایسه با روش‌های سنتی تشخیص هویت، مانند رمز عبور و کارت شناسایی می‌توان به مزایای زیست‌سنجی اشاره کرد که امانت داده نمی‌شوند، دزدیده نمی‌شوند، گم و یا فراموش نمی‌شوند، خراب نمی‌شوند، غیرقابل حدس زدن و غیرقابل فراموشی هستند. با توجه به شکل ۳، حدود ۴۸ درصد از بانک‌های جهان از زیست‌سنجی اثر انگشت در عملیات بانکی خود استفاده می‌کنند، بنابراین، می‌توان با امنیت بیشتر و استفاده از استاندارد تشخیص سریع برخط در اینترنت اشیا نیز از آن استفاده کرد.

1. accuracy
2. scale
3. security
4. privacy
5. enrollment
6. biometric reference
7. comparison
8. networking
9. personal biometric criteria



شکل ۳. نقاط ضعف و قوت انواع تکنیک‌های بیومتریک

پس از مراحل مربوط به استفاده از این فنّاوری، ارزیابی دیگری در مورد عملکرد و مقبولیت ویژگی‌های دیگر زیست‌سنجی نیز انجام گردید که در قالب جدول ۳، به نمایش گذاشته شده است. در این بخش نقاط قوت و ضعف تکنیک‌های زیست‌سنجی را بیان می‌کنیم. پس از بررسی‌های به‌عمل آمده معلوم شد که یکی از زیست‌سنجی‌های مهم اثر انگشت است که با تکنیک‌های دیگر مقایسه شده است.

جدول ۳. مقایسهٔ تکنیک‌های زیست‌سنجی

تکنیک زیست‌سنجی	نقاط قوت	نقاط ضعف
تشخیص اثر انگشت	استفاده و پذیرش وسیع، هزینهٔ پایین، دقت خوب	نیازمند به سخت‌افزار اضافی، سخت‌بودن دریافت تصاویر باکیفیت، عدم کارایی در شرایط خاص
تشخیص چهره	استفاده و پذیرش وسیع، دقت خوب و غیرقابل تقلب	نیازمند به سخت‌افزار اضافی، عدم کارایی در شرایط خاص
تشخیص عنبیه	دقت بالا، غیرقابل تقلب	نیازمند به سخت‌افزار اضافی، هزینهٔ بالا، زمان بالای احراز هویت
تشخیص هندسهٔ دست	سادگی استفاده، کمتر قابل تقلب	نیازمند به سخت‌افزار اضافی، دقت متوسط
تشخیص کف دست	پذیرش عمومی، دقت بالا	نیازمند به سخت‌افزار اضافی، هزینهٔ بالا
تشخیص صدا	پذیرش گسترده، راحتی استفاده، احراز هویت از راه دور	دقت نسبتاً پایین، عدم کارایی در شرایط خاص

تکنیک زیست‌سنجی	نقاط قوت	نقاط ضعف
تشخیص امضا	پذیرش گسترده، غیرقابل تقلب	دقت نسبتاً پایین
پروفایل رفتار	احراز هویت پیوسته	عدم کارایی تحت شرایط خاص
ضربه‌زدن به کلید دینامیک	احراز هویت پیوسته، عدم نیاز به سخت‌افزاری خاص	دقت متناقض، عدم کارایی تحت شرایط خاص
لمس دینامیک	احراز هویت پیوسته، عدم نیاز به سخت‌افزاری خاص	دقت متناقض، عدم کارایی تحت شرایط خاص

۳-۱. روش‌های اصلی اصالت‌سنجی (احراز هویت)

این روش‌ها جهت دسترسی افراد به سامانه‌های بزرگ در سازمان‌ها یا دسترسی به اطلاعات بیماران در سیستم‌های بیمارستانی و استفاده از اشیاء مرتبط با اینترنت همواره مورد استفاده قرار می‌گیرند. این روش‌ها به سه بخش زیر تقسیم می‌شوند:

- ◇ بر پایهٔ «دانش»، مانند پسوردها؛
- ◇ بر پایهٔ «مالکیت»، مانند استفاده از کارت هوشمند یا توکن[1] سخت‌افزاری؛
- ◇ بر پایهٔ «بودن»، مانند استفاده از ویژگی‌های رفتاری و ذاتی زیست‌سنجی (صدا، امضا، تایپ، عنبیه، شبکیه، اثر انگشت، هندسهٔ دست، تشخیص چهره). پس از بررسی‌های صورت‌گرفته معلوم شد که روش سوم از امنیت بالاتری برخوردار است.

احراز هویت زیست‌سنجی اثر انگشت با استفاده از نقاط مشخصه در برآمدگی‌های پوست مانند نقاط دوشاخه، برآمدگی کوتاه، و نقاط انتهایی در انگشت انجام می‌شود. دستگاه‌های ثبت اثر انگشت عمدتاً به‌صورت حرارتی، نوری، خازنی و فراصوتی هستند. در روش ابتدایی حرارت به ولتاژ تغییر می‌یابد. در روش بعدی از نور مرئی برای تهیهٔ اثر انگشت استفاده می‌شود و در روش خازنی پیکسل‌های خازنی وجود دارند که هر جزء وظیفهٔ ثبت یک پیکسل از تصویر نهایی را دارد (جدول ۴).

۳-۲. احراز هویت زیست‌سنجی با روش فراصوت

«شرکت کوالکام»[2] در سال ۱۹۸۵ میلادی در شهر «سن‌دیگو» ایالات متحده آمریکا

1. token
2. Qualcomm

تأسیس شد. در دههٔ ۱۹۹۰ میلادی اقدام به تولید تجهیزات مخابرات راه دور و تأسیسات شبکه‌های تلفن همراه کرد. این شرکت پردازنده‌های «اسکورپیون و کرایت» از سری «اسنپ دراگون» را عرضه کرده است. تکنولوژی تصویر سه‌بعدی اثر انگشت قابلیت سازگاری با سری ۴۰۰-۶۰۰-۸۰۰ را دارد. در این حسگر، ابتدا امواج مافوق صوت به سطح انگشت ارسال می‌شود و انرژی دریافتی این امواج از سطح انگشت اندازه‌گیری می‌شود. دقت آن در مقیاس ۰/۰۵ میلی‌متر است و این، از مزایای آن به حساب می‌آید. پویش سطح کامل انگشت در زمانی کوتاه با دقت ۱۰۰۰ نقطه در اینچ انجام می‌گیرد. این حسگر به چربی، خشکی یا بریدگی سطح پوست حساسیت ندارد. قابلیت تشخیص منافذ در زیر و سطح پوست را دارد و از همه مهم‌تر این‌که قابلیت سازگاری با سایر پایگاه داده‌های اثر انگشت را دارد.

جدول ٤. بررسی دستگاه‌های ثبت اثر انگشت

	نوری	خازنی	فراصوت
اندازه	نسبتاً بزرگ، استفاده از دوربین	قابل تعبیه در تجهیزات کوچک	قابل تعبیه در تجهیزات کوچک
هزینه	متوسط	کم	زیاد
دقت	حساسیت به لکه یا آب	حساسیت به لکه و یا آب	عدم حساسیت به لکه و آب

با توجه به این‌که فراوانی و فراموشی گذرواژه، سرقت گذرواژه، فیشینگ، حمله و جست‌وجوی کورکورانه از مشکلات اساسی گذرواژه‌هاست و از مسائل کاربردی نیز می‌توان سختی تایپ پسورد در تلفن‌های همراه را نام برد، بنابراین، وجود راه حلی جهت حفظ امنیت ضروری است.

همان‌طور که می‌دانید، امروزه برای حصول اطمینان در زمینهٔ امنیت در فنّاوری‌های مختلف استانداردهای مختلفی تدوین می‌گردد. این است که برای استخراج استاندارد بین‌المللی جهت استفاده در کاربردهای مختلف ممیزی صورت می‌گیرد تا روشی واحد با دقت بهینه و سرعت مناسب انتخاب شود. به‌عنوان مثال، استاندارد ISMS[1] سیستم مدیریت امنیت اطلاعات است که در سازمان‌ها مورد استفاده قرار می‌گیرد. در زمینهٔ استفاده از ویژگی‌های زیست‌سنجی نیز لزوم استفاده از استانداردهای یکپارچه با دقت بالا احساس

1. Information Security Management Systems

می‌شود. به همین منظور، فهرستی از استانداردهای مختلف جمع‌آوری شده که در جدول ۵ نمایش داده می‌شود.

جدول ۵. بررسی استانداردهای معتبر جهانی

صنعت	نام استاندارد	شرح
اتحادیهٔ اروپا	دستورالعمل حفاظت داده‌های اتحادیهٔ اروپا (EUDPD)	نیاز به همهٔ اعضای اتحادیهٔ اروپا برای اتخاذ دستور امنیتی
مالی/ بانکی	دستورالعمل‌های امنیتی برای حسابرسان (آمریکا)	تعریف نیازهای امنیتی بانکداری برخط
مالی/ بانکی و خدمات	گرم- صافی- قانون Bliliey (GLB/ GLBA)	مجموعهٔ نیازها برای امنیت و محرمانگی اطلاعات مالی جمع‌آوری‌شده
مالی و فرایند پرداخت خرد	استاندارد امنیت اطلاعات صنعت کارت پرداخت (PCIDSS)	چارچوب برای پردازش امنیتی داده‌های کارت پرداخت: احراز هویت، تشخیص تقلب، پیشگیری
مراقبت‌های بهداشتی مدارک دارویی	اطلاعات سلامت قابل‌حمل‌بودن و پاسخگو به قانون (HIPAA)	کنترل دسترسی، حسابرسی، یکپارچگی داده‌ها، استانداردهای رمزنگاری برای داده‌های سلامت
ادارهٔ آموزش و پرورش آمریکا	حقوق آموزشی خانواده‌ها و قانون حریم خصوصی (FERPA)	استانداردهای محرمانگی برای داده‌های دانش‌آموز شامل نمرات، ثبت‌نام، صدور صورت‌حساب
دولت آمریکا	استاندارد پردازش اطلاعات فدرال (FIPS) از مؤسسهٔ ملی استاندارد و تکنولوژی (NIST)	تعریف احراز هویت، مدیریت کلید رمزنگاری و امنیت فیزیکی در سازمان‌های آمریکا

۳-۳. تشخیص سریع برخط و حذف پسوردها

در سال ۲۰۱۳، «مایکل بارت»[1] مدیر امنیت اطلاعات «پی پال»[2]، در نمایشگاه «اینتراوپ»[3] در آمریکا با نمایش سنگ قبری منقش به واژگان بیان داشت که استفاده از گذرواژه‌ها در اینترنت به شکست منجر می‌شود و نشان داد که عمر گذرواژه‌ها به پایان رسیده است. ائتلاف تشخیص سریع برخط یک سازمان غیرانتفاعی است که در تابستان سال ۲۰۱۲، توسط شرکت‌های بزرگ و عمدهٔ فعال در زمینهٔ احراز هویت در فضای مجازی

1. Michael Barrett 2. Paypal 3. Interop

تشکیل و در فوریهٔ سال ۲۰۱۳، رسماً به‌طور عام معرفی شد. با پیوستن شرکت‌هایی مانند «گوگل»، «مایکروسافت»، «آراِس‌اِی»[1] و برخی شرکت‌های معتبر و صاحب‌نام دیگر که در حال حاضر عضو هیئت مدیرهٔ ائتلاف هستند، به سرعت رشد کرد. این اتحادیه با هدف جایگزینی گذرواژه با یک پروتکل امن و سازگار با صنایع شکل گرفته است که استفاده از آن نیز آسان باشد. تشخیص سریع برخط در حال بررسی فنّاوری‌هایی چون پویشگرهای اثر انگشت، تشخیص صدا و چهره در کنار راه‌حل‌های موجود مانند NFC و گذرواژهٔ یک‌بار مصرف است. شرکت‌های ارائه‌دهندهٔ خدمات برخط با ابداع استاندارد تشخیص سریع برخط ضمن تأمین امنیت لازم در بالاترین حد آن، روشی ساده و آسان در اختیار کاربران قرار می‌دهند. ایدهٔ اصلی سرویس مرکزی جهت استانداردسازی، لایه‌های مشتریان و پروتکل‌های تغییرِ داده است. این اقدام منجر به استفاده از روش‌های احراز هویت زیست‌سنجی می‌شود که با سرویس‌های متعدد برخط قابلیت سازگاری دارند. همچنین، ترکیب روش زیست‌سنجی و استاندارد رمزنگاری کلید عمومی برای تسهیل روند احراز هویت کاربران به فرایند جایگزینی کلمات عبور در سامانه‌های کاربردی کمک خواهد کرد.

۳-٤. مزایای استفاده از تکنولوژی بدون پسورد

- ◇ تکنولوژی به‌روز برای احراز هویت کاربران بدون نیاز به رمز عبور؛
- ◇ عدم نیاز به تحویل اطلاعات حساس و محرمانه به فراهم‌کنندگان سرویس‌ها؛
- ◇ مقاومت بالا در برابر حملهٔ Phishing/ man-in-the-middle؛
- ◇ سهولت استفاده برای کاربران بانک‌ها و مؤسسات مالی؛
- ◇ ارائهٔ آسان خدمات دولت الکترونیک و تجارت الکترونیک؛
- ◇ توسعهٔ سامانه‌های اینترنت اشیا در برنامه‌های کاربردی موبایل.

٤. روش پیشنهادی استفاده از تکنولوژی تشخیص سریع برخط

با توجه به افزایش استفاده از اینترنت در عصر حاضر و ارائهٔ خدمات الکترونیکی توسط بنگاه‌های اقتصادی و تجاری اهمیت تأمین امنیت تبادل اطلاعات در این فضا مطرح

1. RSA

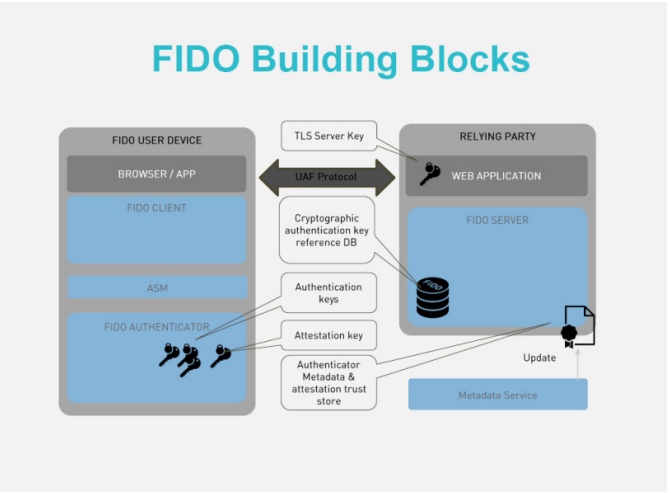
بوده و یکی از چالش‌های بزرگ آن استفاده از ابزار متصل به اینترنت و دسترسی به دادگان در شرکت‌ها و ... است. با توجه به این‌که همزمان با گسترش اینترنت و ارائهٔ انواع خدمات الکترونیکی، نفوذ افراد غیرمجاز و سوءاستفاده‌کنندگان گسترده‌تر شده است، ارائهٔ راهکارهای جدید و با قدرت جهت تأمین امنیت تبادل اطلاعات نیاز اساسی این بحث است. امروزه، استفاده از کلمات عبور و گذرواژه‌ها برای این امر در نظر گرفته شده است که خود، با چالش‌های فراوانی روبه‌روست. یکی از مشکلات اساسی گذرواژه‌ها فراوانی و فراموشی گذرواژه و سرقت گذرواژه، تکراری‌بودن آن‌ها به جهت یادآوری آسان‌تر، استفاده از موارد معمول و قابل دسترس مانند شمارهٔ شناسنامه یا تاریخ تولد، حملهٔ فیشینگ، حملهٔ جست‌وجوی کورکورانه است. از مسائل کاربردی نیز، سختی تایپ پسورد در تلفن‌های همراه، استفاده از اینترنت اشیا و دسترسی به اطلاعات حجیم قابل ذکر است (شکل ۶).

با توجه به موارد ذکرشده استفاده از راهکاری جهت حفظ امنیت، احراز هویت یا اصالت‌سنجی که شامل تأیید هویت یک شخص، یا اطمینان از اصالت یک نرم‌افزار است، ضروری احساس می‌شود.

٤-١. استاندارد تشخیص سریع برخط

- ◇ داده‌ها در بانکداری برخط: یکی از مؤلفه‌های کلیدی در بحث اعتماد مشتریان به بانکداری اینترنتی مسئلهٔ احراز هویت و تأیید هویت است که عموماً بر شناسه و رمز عبور مبتنی است. استفاده از شیوه‌های زیست‌سنجی در این حوزه ضروری است. انتخاب درست یک یا 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 NFC خرید با استفاده از برنامه‌های کاربردی موبایل، نقل و انتقال پول P2P تجارت الکترونیک بدون کارت؛
- ◇ سایر خدمات تجارت الکترونیک: تجارت در بازارهای جهانی نیازمند امنیت و اجرای بدون افشای اطلاعات است و از آنجا که تعاملات الکترونیکی رودررو نیستند، لذا بحث احراز هویت به‌عنوان یکی از موارد امنیت الکترونیک محسوب می‌شود. اگر بتوان با روشی مطمئن ثابت کرد که طرفین تجاری همان کسانی هستند که ادعا می‌کنند،

مسلماً یکی از چالش‌های موجود در تعاملات الکترونیک برطرف خواهد شد.



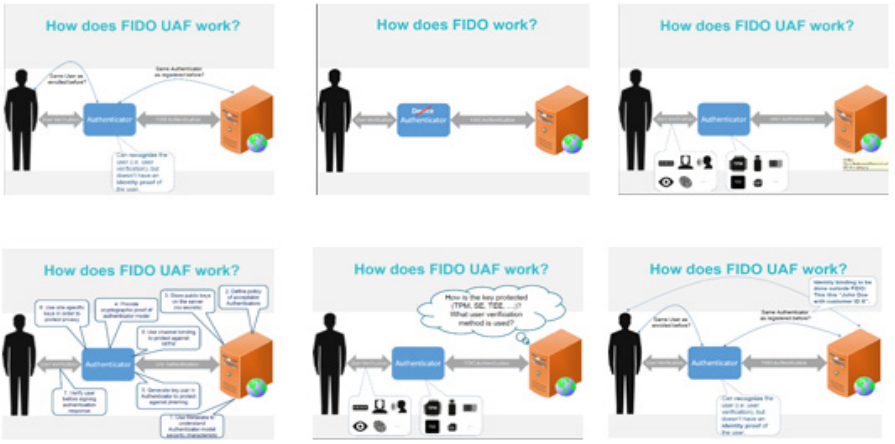
شکل ٦. بلوک دیاگرام استاندارد تشخیص سریع برخط

مأموریت اصلی ائتلاف تشخیص سریع برخط تغییر روش‌های احراز هویت برخط تعیین شد. نسخهٔ اول پروتکل‌های تشخیص سریع برخط در ۹ دسامبر سال ۲۰۱۴ میلادی منتشر شد. این ائتلاف برای رسیدگی به طیف گستردهٔ 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 با اهمیت سازمان‌هاست. دو پروتکل مهم مورد استفاده در آن UAF و U2F هستند که در ادامه به توضیحات آن‌ها می‌پردازیم.

UAF[1]: پروتکل فاقد کلمهٔ عبور که از ویژگی‌های زیست‌سنجی کاربران برای احراز هویت استفاده می‌کند. این پروتکل اجازهٔ ثبت یک دستگاه فعال مثل تلفن همراه هوشمند یا تبلت در یک سرور یا وب‌سایت پشتیبانی‌کنندهٔ تشخیص سریع برخط را به کاربر می‌دهد. کاربر دستگاه و سرویس‌گیرنده با قابلیت UAF را حمل می‌کند یا یک pin یا زیست‌سنجی محلی ارائه می‌دهد. در این راهکار کاربر دستگاه خود را از طریق انتخاب یک مکانیسم احراز هویت محلی مانند اثر انگشت، نگاه به دوربین، صحبت با میکروفن، واردکردن Pin و ... ثبت می‌کند. پروتکل UAF به سرویس این امکان را

1. Universal Authentication Framework (UAF)

می‌دهد که مکانیسم‌های ارائه‌شده به کاربر را انتخاب کند. پس از ثبت نام اولیه، کاربر به سادگی می‌تواند عملیات احراز هویت محلی را در هر زمان و مکان انجام دهد. این پروتکل همچنین، امکان ترکیب مکانیسم‌های تأیید هویت چندگانه مانند اثر انگشت به همراه pin را نیز فراهم می‌کند. پروتکل UAF شامل عملیات ثبت‌نام، احراز هویت، تأیید تراکنش، و لغو ثبت‌نام است (شکل ۷).



شکل ۷. بلوک دیاگرام نحوهٔ کارکرد پروتکل UAF

U2F[1]: پروتکلی است که با استفاده از یک توکن سخت‌افزاری احراز هویت انجام می‌دهد.

این پروتکل به‌منظور احراز هویت کاربر با استفاده از یک فاکتور ثانویهٔ قوی یک کلید لمسی[2] بر روی ابزار USB طراحی شده است. کاربر، دستگاه U2F را که قابلیت شناسایی توسط مرورگرهای وب را دارد، همراه خود دارد. این راهکار اجازه می‌دهد که خدمات برخط امنیت زیرساخت رمز عبور موجود خود را با اضافه‌کردن یک عامل دوم قوی برای ورود کاربر به سیستم تقویت کند. کاربر به‌سادگی با فشار دادن یک دکمه بر روی دستگاه USB و یا با تکنولوژی NFC ارتباط برقرار می‌کند.

1. Universal 2nd Factor (U2F)
2. finger touch

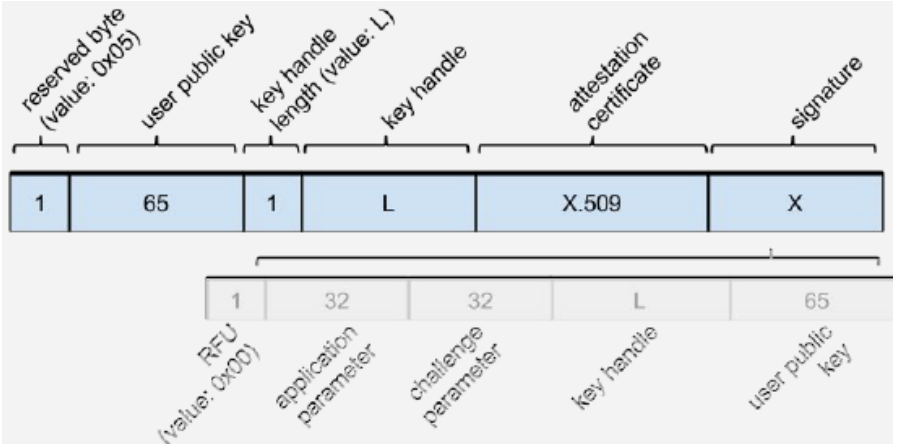
```
u2f.register([{
    'version' : 'U2F_V2',
    'challenge': 'KSDJsdASAS-AIS_AsS',
    'appId': 'https://www.google.com/facets.json'
  }], callback);

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

حال برای کاربر برنامهٔ زیر ارائه می‌شود:

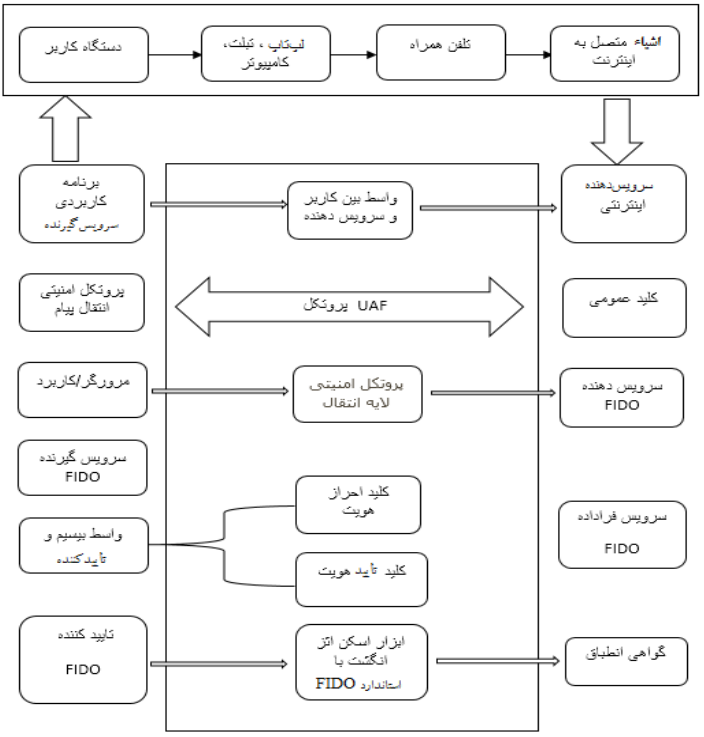
```
{
  "typ":"register",
  "challenge":"KSDJsdASAS-AIS_AsS",
  "cid_pubkey": {
    "kty":"EC",
    "crv":"P-256",
    "x":"HzQwlfXX7Q4S5MtCRMzPO9tOyWjBqRl4tJ8",
    "y":"XVguGFLIZx1fXg375hi4-7-BxhMljw42Ht4"
  },
  "origin":"https://accounts.google.com"
}
```

و در ادامه، برای ثبت نام کاربر با استفاده از شمای کلی زیر، اطلاعات اسکن‌شده کدگذاری می‌شود (شکل ۸).



شکل ۸. کدگذاری در FIDO

٤-۲. ساختار جدید و استفاده از FIDO در اینترنت اشیا:



شکل ۹. ساختار جدید استفاده از FIDO در اینترنت اشیا

ساختار پیشنهادی شکل ۹، می‌تواند تحول عظیمی در امنیت اینترنت اشیا به‌وجود آورد. در این ساختار در مرحلهٔ اول، ویژگی زیست‌سنجی در دستگاه کاربر ثبت می‌گردد. این دستگاه می‌تواند وسایل الکترونیکی شخصی مانند تلفن همراه، تبلت و لپ‌تاپ یا سیستم‌های هوشمند خانگی و اشیا متصل به اینترنت باشند. از طرف دیگر، در سمت کاربر یا سرویس‌گیرنده یک برنامهٔ کاربردی که با استاندارد FIDO سازگاری دارد، نصب می‌گردد. این برنامه با پروتکل انتقال در سمت سرویس‌گیرنده از یک‌سو و با ابزار تحت پوشش از سوی دیگر در ارتباط است، پس از این‌که اسکن اثر انگشت ثبت گردید، کلید عمومی در سطح کاربر تولید می‌شود که کلید احراز هویت و تأیید هویت است. سپس، تأییدکنندهٔ FIDO به جای ارسال عکس، اسکن اثر انگشت یا تبدیل آن به کد را با استفاده از زیرساخت کلید عمومی آن به‌صورت محرمانه ارسال می‌کند. در مرحلهٔ بعد، در سمت سرویس‌دهنده گواهی انطباق اثر انگشت بررسی می‌شود و در صورت درستی آن، سرویس‌دهندهٔ FIDO دسترسی به اطلاعات یا برقراری ارتباط را از طریق برنامهٔ کاربردی خود فراهم می‌کند. با استفاده از ابزار ثبت اثر انگشت و استاندارد FIDO تمامی شرکت‌های فعال در زمینهٔ فنّاوری زیست‌سنجی می‌توانند با یک پروتکل مشترک و امنیت بالا به پیاده‌سازی نرم‌افزار و سخت‌افزار مرتبط بپردازند. این امکان می‌تواند جهت دسترسی به داده‌ها در یک سازمان، در بانکداری الکترونیکی و شرکت‌های سازندهٔ تلفن همراه استفاده شود یا جهت ارائهٔ برنامه‌های کاربردی در زمینهٔ اینترنت اشیا و نرم‌افزارهای تلفن همراه ارائه گردد. در صورتی‌که این ابزارها مجهز به این استاندارد باشند، امنیت برقراری ارتباط آن‌ها با استفاده از یک زبان مشترک تضمین می‌گردد.

همان‌طور که در مقالات متعددی در زمینهٔ زیست‌سنجی بحث شده، در پژوهش‌های پیشین با استفاده از اسکن اثر انگشت می‌توانستیم با ابزارهای مختلف ارتباط برقرار کنیم. به این صورت که الگویی از اثر انگشت افراد استخراج شده و برای سرویس‌گیرنده ارسال می‌شد که متأسفانه احتمال خطر ربوده‌شدن و دسترسی توسط افراد غیرمجاز و هکرها وجود داشت، در حالی که در مدل جدید الگوی ذخیره‌شده از زیست‌سنجی افراد به زیرساخت کلید عمومی تبدیل شده و جابه‌جا می‌شود. در این حالت چالش حفظ حریم خصوصی نیز برطرف می‌شود، چرا که اطلاعات کلید عمومی روی سرور قرار می‌گیرد و حتی هک‌شدن سرور باعث از بین رفتن اطلاعات زیست‌سنجی افراد نمی‌شود. بنابراین، استاندارد FIDO می‌تواند تفاوت‌های مؤثری در برقراری ارتباط با اشیا

و احراز هویت افراد برای دسترسی به داده‌های مهم ایجاد کند. همچنین، تشخیص هویت فرد از افراد مختلف بسیار سریع‌تر و با دقت بالاتری صورت می‌پذیرد. این در حالی است که در شیوه‌های قدیمی این بررسی بسیار زمان‌بر و پرهزینه بوده است. با استفادهٔ ترکیبی از پروتکل دیگری با نام TLS تأیید هویت یک‌طرفه یا دوطرفه برای دسترسی رمزشده به شبکه‌ها فراهم می‌شود و بخش‌هایی مانند حفاظت از بستهٔ داده، محدودنمودن و بهینه‌نمودن اندازهٔ بسته و انتخاب یک الگوریتم سریع هم با استاندارد TLS امکان‌پذیر می‌شود. در نهایت، می‌توان نتیجه گرفت که امنیت و کیفیت ارتباط بین دو طرف بستگی به نوع الگوریتم‌های توافق‌شدهٔ بین آن‌ها دارد. استاندارد FIDO به همراه پروتکل امن ارتباط در شبکه می‌تواند تحول بزرگی در زمینهٔ استفادهٔ مؤثر از اینترنت اشیا به‌وجود آورد. در راهکار ارائه‌شده هزینه و پیچیدگی احراز هویت به طرزی چشمگیر کاهش می‌یابد و کاربران به جای به‌کارگیری کلمات عبور می‌توانند با استفاده از روش‌های کاربرپسند نظیر اثر انگشت، تشخیص چهره و ... احراز هویت شوند.

از مهم‌ترین مزایای استفاده از راهکار تحت استاندارد FIDO می‌توان به موارد زیر اشاره کرد:

۱. پشتیبانی از همهٔ سناریوهای احراز هویت (اثرانگشت، تشخیص چهره، صدا و ...)؛
۲. کاهش پیچیدگی و هزینهٔ احراز هویت؛
۳. امکان استفاده از قابلیت‌های امنیتی دستگاه‌های موجود نظیر تلفن همراه هوشمند، تبلت‌ها و ...؛
۴. کاهش خطر افشاء اطلاعات کاربران در اثر نفوذ به سرور؛
۵. کاهش نیاز کاربران برای به خاطر سپردن کلمات عبور.

تعاریف مهمی در این زمینه وجود دارد که به اهمّ آن‌ها می‌پردازیم.

دستگاه احراز هویت‌کننده: دستگاهی که به‌واسطهٔ آن احراز هویت زیست‌سنجی صورت می‌گیرد.

طرف اعتمادکننده: به برنامهٔ کاربردی گفته می‌شود که به سرور اعتماد می‌کند و جهت احراز هویت کاربران خود از این سرور استفاده می‌کند.

سرویس‌دهنده: واحدی که وظیفهٔ اجرای فرایند احراز هویت و نگهداری اطلاعات کاربران را بر عهده دارد.

سـرویس‌گیرنده: بخشـی از برنامـهٔ کاربـر کـه بـه روی دسـتگاه کاربـران اجـرا می‌شـود و جهـت احـراز هویـت ارتبـاط لازم را بـا سـرویس‌دهنده برقـرار می‌کنـد.

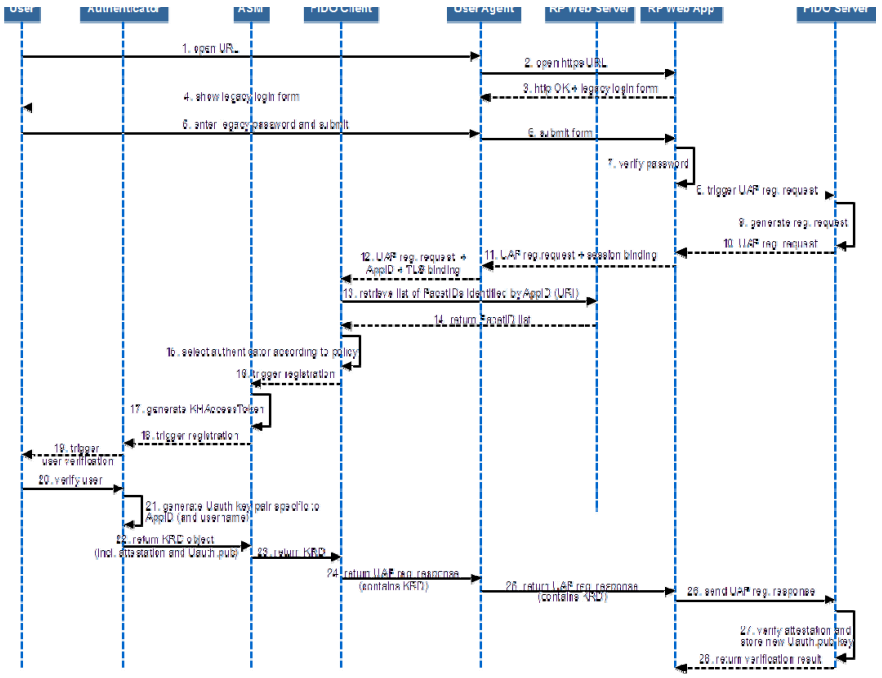
۵. یافته‌ها

اینترنـت اشـیا بـه چنـد دلیـل نسـبت بـه خطـرات، ضعیـف عمـل می‌کنـد و شـکننده اسـت. اول این‌کـه اغلـب، از عناصـر آن مراقبـت نمی‌شـود و ممکـن اسـت به‌طـور فیزیکـی در معـرض خطـر باشـند. از طـرف دیگـر، بـا توجـه بـه این‌کـه ارتباطـات بیشـتر از طریـق بی‌سـیم اسـت، اسـتراق سـمع بـه سـاده‌ترین شـکل ممکـن خواهـد شـد. در نهایـت این‌کـه، بیشـتر عناصـر اینترنـت اشـیا چـه از نظـر انـرژی و چـه از لحـاظ منابـع رایانـه از توانایـی پایینـی برخوردارنـد و بنابرایـن، نمی‌تواننـد الگوهـای پیچیـدهٔ پشـتیبانی امنیتـی را اجـرا کننـد.

به‌طـور خـاص، مشـکلات بـزرگ بیشـتر مربـوط بـه تصدیـق و یکپارچه‌سـازی داده‌هاسـت. تصدیـق هویـت کاربـران، بسـیار سـخت اسـت، چـرا کـه نیازمنـد زیرسـاخت‌ها و سـرورهایی اسـت کـه از طریـق انتقـال پیام‌هـای مناسـب بـا دیگـر گره‌هـا بـه اهـداف خـود دسـت پیـدا می‌کنـد. در اینترنـت اشـیا چنیـن رویکردهایـی امکان‌پذیـر نیسـتند، زیـرا برچسـب‌های RFID تعـداد بسـیار بـالای پیـام را نمی‌تواننـد بـه سـرورها انتقـال دهنـد و البتـه، ایـن مسـئله در مـورد گره‌هـای حسـگر نیـز صـادق اسـت. طـی سـال‌های اخیـر، راه‌حل‌هـای بسـیاری بـرای سیسـتم‌های RFID پیشـنهاد شـده اسـت. اگرچـه هنـوز مشـکل، آن‌گونـه کـه بایـد حـل نشـده اسـت و بـا مسـائل جدّی روبه‌روسـت، امـا در ایـن مقالـه راه‌حـل جدیـدی بـرای حـل ایـن مشـکل به‌وجـود می‌آیـد. در واقـع، هیچ‌کـدام از راه‌حل‌هـای موجـود نمی‌تواننـد در حـل مشـکل خطـر پراکسـی[1] کـه بـه man-in-middle attack هـم معـروف هسـتند، کمـک کننـد. راه‌حل‌هـای مربـوط بـه یکپارچه‌سـازی اطلاعـات بایـد ایـن ضمانـت را داشـته باشـد کـه یـک مخالـف نتوانـد اطلاعـات را در مسـیر بـدون تغییـر انتقـال دهـد. مسـائل و مشـکلات جدیـدی ممکـن اسـت پیـش بیایـد. وقتـی سیسـتم‌های RFID بـا اینترنـت ادغـام می‌شـوند، در بیشـتر مـوارد آن‌هـا به‌درسـتی کنتـرل نمی‌شـوند. داده‌هـا ممکـن اسـت در زمانـی کـه ذخیـره می‌شـوند و یـا از شـبکه عبـور می‌کننـد، توسـط حمله‌کننده‌هـا تغییـر یابنـد. بـرای حفاظـت از داده‌هـا و اطلاعـات در برابـر اولیـن نـوع حملـه در بسـیاری از تکنولوژی‌هـای دارای برچسـب، حافظـه محافظـت می‌شـود و

1. Proxy

راه‌حلی برای شبکه‌های حسگر بی‌سیم ارائه نشده است. برای حفاظت از داده‌ها در مقابل دومین نوع حمله‌ها، پیام‌ها بر اساس الگوی HMAC محافظت می‌شوند. این حفاظت بر اساس یک کلید رمز مشترک بین برچسب و مقصد پیام است که با یک عملکرد ادغامی به‌کار می‌رود تا امنیت لازم را به‌وجود بیاورد. بدون اطمینان از خصوصی‌بودن در دنیای حسگرهای متصل به هم و دستگاه‌ها، کاربران تمایل ندارند که این تکنولوژی‌ها را بپذیرند. گزارش واحد ارتباطات مخابراتی بین‌المللی در مورد پیشرفت و ارتباط اینترنت بیان می‌کند که نگرانی‌ها در مورد حریم خصوصی و حفاظت داده‌ها گسترده شده است؛ به‌ویژه این‌که حسگرها و برچسب‌های هوشمند می‌توانند حرکات کاربر، عادات او را ردیابی کند. در نتیجه، استفاده از استانداردهای مناسب در این زمینه بسیار ضروری است. در حالت کلی، برای پیاده‌سازی و استفاده از فنّاوری FIDO ابتدا باید طبق مراحل شکل ۱۰، ثبت‌نام کاربر انجام شود. در این ساختار شناسایی و تشخیص هویت ابتدایی در ۲۸ مرحله صورت می‌پذیرد که از این کاربرد می‌توان در کاربردهای بانکداری الکترونیکی برای دسترسی به داده‌ها و اینترنت اشیا بهره برد.



شکل ۱۰. ساختار کلی فرایند ثبت زیست‌سنجی در تکنولوژی FIDO

۵. فرایند ثبت[1]

در طول عملیات ثبت نام در سمت کاربر، به کاربران اجازه داده می‌شود که خود را به یک یا چند شاخصهٔ احراز هویت‌کننده‌های قابل پذیرش توسط سرور ثبت نام کنند. در این مرحله در سمت کاربر یک زوج کلید تولید می‌شود که برای کاربر احراز هویت‌کننده و طرف اعتمادکننده منحصربه‌فرد است. کلید عمومی به سرور ارسال و کلید خصوصی به‌طور امن در سمت کاربر ذخیره می‌شود. سرور با استفاده از کلید احراز هویتی که قبلاً منتشر شده است، اصل‌بودن احراز هویت‌کننده را بررسی می‌کند و بدین‌ترتیب، خطر جعل عنوان یا تغییر هویت[2] به حداقل می‌رسد. آغاز فرایند ثبت‌نام به این صورت است که درخواست ثبت نام کاربر جدید به سرور ارسال می‌شود. سپس، سرور لیست احراز هویت‌کننده‌های قابل پذیرش و سیاست قابل پشتیبان را به کلاینت ارسال می‌کند. ثبت‌نام کردن کاربران انتخاب شده و منطبق بر تولید زوج کلید است. کلید عمومی به سرور ارسال می‌شود و در آخر تأیید اعتبار احراز هویت‌کننده با استفاده از کلید تأیید انجام می‌گردد (جدول ۶).

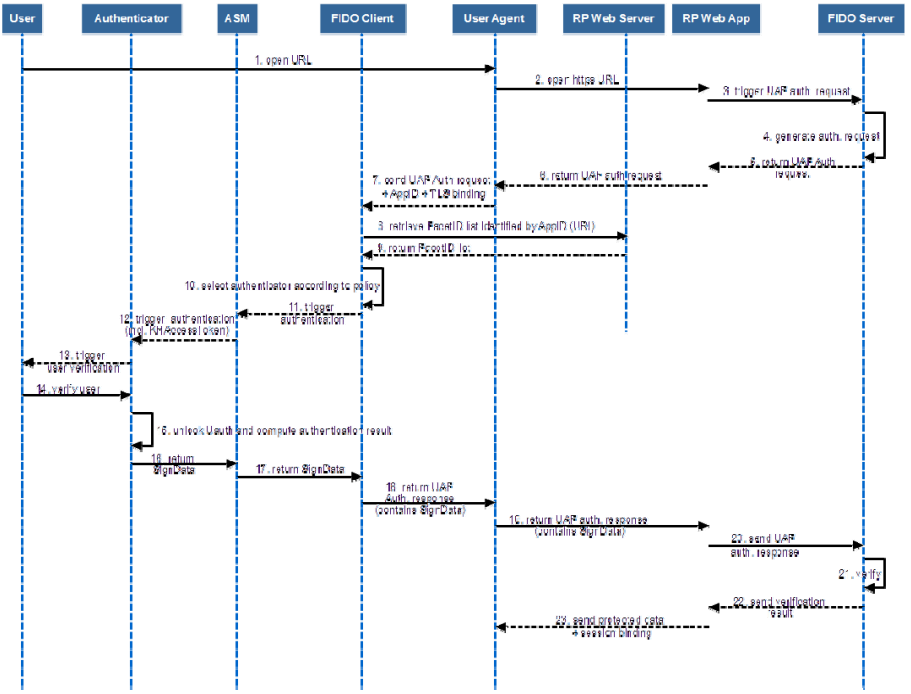
جدول ٦. ساختار کلی فرایند ثبت

ردیف		شرح فرایند ثبت‌نام
۱	Open URL	ابتدا درخواست کاربر در مرورگر وارد می‌شود.
۲	Open https URL	درخواست به relying party یا RP که می‌تواند برنامه کاربردی یا سرویس‌دهنده باشد، ارسال می‌شود.
۳	http OK + legacy login form	صفحهٔ ورود به سیستم به مرورگر نشان داده می‌شود.
۴	Show legacy login form	فرم ورود به سیستم برای کاربر نمایش داده می‌شود.
۵	Enter legacy password and submit	نام کاربری و رمز عبور در این بخش وارد می‌شود.
۶	Submit form	فرم ورود به سیستم ثبت می‌گردد.
۷	Verify password	در این مرحله درستی نام کاربری و رمز عبور بررسی می‌شود.
۸	Trigger UAF reg. request	پیام آماده‌سازی فرایند ثبت نام به سرویس‌دهنده ارسال می‌شود.
۹	Generate reg. request	درخواست ثبت را تولید می‌کند.
۱۰	UAF reg. request	درخواست ثبت برای RP ارسال می‌شود.

1. provisioning

ردیف		شرح فرایند ثبت‌نام
۱۱	UAF reg. request + session binding	RP پیام ثبت را به کاربر نشان می‌دهد.
۱۲	UAF reg. request + App ID + TLS binding	مرورگر درخواست ثبت را دریافت می‌کند.
۱۳	Retrieve list of Facet IDs identified by app ID (URL)	فرایند TLS را بررسی می‌کند. کلاینت هم گواهینامه دارد. برای این‌که اگر کسی در حین برقراری ارتباط شنود کند موفق نشود و برای کاربر واقعی دسترسی ایجاد شود.
۱۴	Return facet ID list	بررسی می‌شود از کدام وب‌سایت یا برنامهٔ کاربردی ارتباط برقرار شده است.
۱۵	Select authenticator according to policy	در سمت سرویس‌گیرنده FIDO قوانین و دسترسی‌ها را استخراج و فراخوانی می‌کند (برای مثال، این‌که چه ویژگی زیست‌سنجی را باید شناسایی کند مثل اثر انگشت.)
۱۶	Trigger registration	سرویس‌گیرنده پیغام را به رابط می‌فرستد.
۱۷	Generate KHAccess Token	رابط یک توکن دسترسی تولید می‌کند و به همراه پیغام آن را به ابزار ثبت زیست‌سنجی ارسال می‌کند.
۱۸	Trigger registration	دسترسی ارسال می‌شود.
۱۹	Trigger user verification	فرایند ثبت اثر انگشت انجام می‌شود.
۲۰	Verify user	عملیات ثبت صورت می‌گیرد.
۲۱	Generate Uauth key pair specific to App ID (and username)	کلید عمومی و خصوصی تولید می‌شود. این عمل با مشخصهٔ برنامهٔ کاربردی و نام کاربری انجام می‌شود.
۲۲	Return KRD object (incl. attestation and Uauth.pub)	کلید عمومی در پیام درج و ارسال می‌گردد.
۲۳	Return KRD	کلید عمومی و نام کاربری و مشخصهٔ برنامهٔ کاربردی برای سرویس‌گیرنده ارسال می‌شود.
۲۴	Return UAF reg. response (contains KRD)	سرویس‌دهنده پیام ثبت را تولید می‌کند.
۲۵	Return UAF reg. response (contatains KRD)	پیام به مرورگر ارسال می‌شود و به RP می‌رسد.
۲۶	Send UAF reg. response	RP نیز پیام را به سرویس‌دهنده ارسال می‌کند.
۲۷	Verify attestation and store new Uauth. publickey	RP نیز پیام را احراز هویت می‌کند.
۲۸	Return verification result	نتیجهٔ تصدیق هویت مشخص می‌گردد.

در مرحلهٔ بعد، هویت گوینده تصدیق و مطابقت با اطلاعات ثبت‌شده از کاربران در ۲۳ مرحله انجام می‌شود. دیاگرام تصدیق هویت گوینده در پروتکل UAF مرحله به مرحله در شکل ۱۱، نشان داده شده است.



شکل ۱۱. ساختار کلی فرایند احراز هویت با استفاده از اثر انگشت و تکنولوژی FIDO

فرایند 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 چالش تولید می‌کند و به کلاینت می‌فرستد. سرور همچنین، یک یا چند احراز هویت‌کنندهٔ قابل پذیرش را اعلام می‌کند و کلاینت نیز از بین احراز هویت‌کننده‌ها انتخاب می‌کند و از کاربر می‌خواهد اقدام مورد نیاز با روش مشخص را اجرا نماید (جدول ۷). در نتیجه، این فرایند دارای مراحل زیر است:

۱. آغاز مرحلهٔ احراز هویت و ارسال شناسهٔ برنامهٔ کاربردی و نام کاربردی به سرور؛
۲. ارسال چالش و سیاست به کلاینت توسط سرور؛
۳. احراز هویت کاربر با استفاده از احراز هویت‌کنندهٔ انتخاب‌شده منطبق بر سیاست سرور مانند اثر انگشت؛
۴. ارسال پاسخ احراز هویت به WEB APP؛

۵. تأیید اعتبار پاسخ احراز هویت با کلید عمومی.

جدول ۷. ساختار کلی فرایند ثبت زیست‌سنجی در تکنولوژی FIDO

ردیف		شرح فرایند ثبت‌نام
۱	Open URL	ابتدا درخواست کاربر در مرورگر وارد می‌شود
۲	Open https URL	درخواست به relying party یا RP، که می‌تواند برنامهٔ کاربردی یا سرویس‌دهنده باشد، ارسال می‌شود.
۳	http OK + legacy login form	صفحهٔ ورود به سیستم به مرورگر نشان داده می‌شود.
۴	Show legacy login form	فرم ورود به سیستم برای کاربر نمایش داده می‌شود.
۵	Enter legacy password and submit	نام کاربری و رمز عبور در این بخش وارد می‌شود.
۶	Submit form	فرم ورود به سیستم ثبت می‌گردد.
۷	Verify password	در این مرحله درستی نام کاربری و رمز عبور بررسی می‌شود.
۸	Trigger UAF reg. request	پیام آماده‌سازی فرایند ثبت‌نام به سرویس‌دهنده ارسال می‌شود.
۹	Generate reg. request	درخواست ثبت را تولید می‌کند.
۱۰	UAF reg. request	درخواست ثبت برای RP ارسال می‌شود.
۱۱	UAF reg. request + session binding	RP پیام ثبت را به کاربر نشان می‌دهد.
۱۲	UAF reg. request + App ID + TLS binding	مرورگر درخواست ثبت را دریافت می‌کند.
۱۳	Retrieve list of Facet IDs identified by app ID (URL)	فرایند TLS را بررسی می‌کند. کلاینت هم گواهینامه دارد. برای این‌که اگر کسی در حین برقراری ارتباط شنود کند، نتواند و برای کاربر واقعی دسترسی ایجاد شود.
۱۴	Return facet ID list	بررسی می‌شود از کدام وب‌سایت یا برنامهٔ کاربردی ارتباط برقرار شده است.
۱۵	Select authenticator according to policy	در سمت سرویس‌گیرنده FIDO قوانین و دسترسی‌ها را استخراج و فراخوانی می‌کند (برای مثال، این‌که چه ویژگی زیست‌سنجی را باید شناسایی کند، مثل اثر انگشت.)
۱۶	Trigger registration	سرویس‌گیرنده پیغام را به رابط می‌فرستد.
۱۷	Generate KHAccess Token	رابط یک توکن دسترسی تولید می‌کند و به همراه پیغام آن را به ابزار ثبت زیست‌سنجی ارسال می‌کند.
۱۸	Trigger registration	دسترسی ارسال می‌شود.
۱۹	Trigger user verification	فرایند ثبت اثر انگشت انجام می‌شود.

ردیف		شرح فرایند ثبت‌نام
۲۰	Verify user	عملیات ثبت صورت می‌پذیرد.
۲۱	Generate Uauth key pair specific to App ID (and username)	کلید عمومی و خصوصی تولید می‌شود. این عمل با مشخصهٔ برنامهٔ کاربردی و نام کاربری انجام می‌شود.
۲۲	Return KRD object (incl. attestation and Uauth.pub)	کلید عمومی در پیام درج شده و ارسال می‌گردد.
۲۳	Return KRD	کلید عمومی و نام کاربری و مشخصهٔ برنامهٔ کاربردی برای سرویس‌گیرنده ارسال می‌شود.
۲۴	Return UAF reg. response (contains KRD)	سرویس‌دهنده پیام ثبت را تولید می‌کند.
۲۵	Return UAF reg. response (contatains KRD)	پیام به مرورگر ارسال می‌شود و به RP می‌رسد.
۲۶	Send UAF reg. response	RP نیز پیام را به سرویس‌دهنده ارسال می‌کند.
۲۷	Verify attestation and store new U auth.publickey	RP نیز پیام را احراز می‌کند.
۲۸	Return verification result	نتیجهٔ تصدیق هویت مشخص می‌گردد

در نهایت، سرویس‌دهنده بر روی زیرساخت طرف اصلی- متکی[1] اجرا می‌شود. سرویس‌گیرنده بخشی از برنامهٔ کاربر است که بر روی دستگاه کاربر اجرا می‌شود. احراز هویت‌کننده با دستگاه کاربر یکپارچه است و پس از طی‌شدن این مراحل کاربر می‌تواند به‌راحتی به سیستم متصل شود.

همچنین، ایدهٔ دیگری که می‌توان مورد ارزیابی قرار داد، استفاده از چندین روش احراز هویت به‌صورت همزمان است که دقت و امنیت بسیار بالا را تضمین خواهد کرد.

٦. بحث

با توجه به نتایج به‌دست‌آمده، هر سیستم زیست‌سنجی شامل موارد زیر است:

۱. ابزار اندازه‌گیری: ابزار اندازه‌گیری واسط کاربر را تشکیل می‌دهد. راحتی استفاده، یک فاکتور مهم دیگر برای زیست‌سنجی است. ابزار باید مطابق با غریزه باشد و فضای کمی برای خطا ایجاد کند. این ابزار همچنین، باید قابل استفاده برای دامنهٔ وسیعی از مردم و به‌ویژه برای افراد ناتوان باشد.

1. relying party

۲. نرم‌افزار عامل: نرم‌افزار عامل شامل الگوریتم‌های ریاضی است که پارامترهای سنجش‌شده را با الگوی مرجع مقایسه می‌کنند. جدیدترین الگوریتم‌ها به مدل‌سازی آماری وابستگی کمی دارند و بیشتر بر پایهٔ برنامه‌ریزی دینامیک، شبکه‌های عصبی، و منطق فازی هستند که انعطاف‌پذیری را افزایش می‌دهند (Jain, Nandakumar and Ross 2005).

۳. سخت‌افزار و سیستم‌های بیرونی: قابلیت استفاده، قابلیت اطمینان و هزینهٔ سیستم اغلب، حداقل به همان اندازه که به ابزار سنجش بستگی دارد، به سخت‌افزار نیز بستگی دارد. بعضی سیستم‌ها (مانند آزمون اثر انگشت) فی‌نفسه برای استفاده در سیستم‌های توزیع‌شده مناسب هستند؛ در حالی که بقیه (مانند تشخیص صدا) برای سیستم‌های متمرکز مناسب هستند. لازم به توضیح است که از بیومتریک در دو فیلد مجزا می‌توان استفاده کرد:

◇ تشخیص هویت[1]:

سامانه، فرد را از طریق جست‌وجو و مقایسهٔ الگوی همهٔ کاربران در پایگاه داده‌ها تشخیص می‌دهد. در این فیلد سعی می‌شود که هویت شخص دقیقاً مشخص گردد. تشخیص شامل مقایسهٔ اطلاعات کسب‌شده در قالبی خاص با تمام کاربران در پایگاه داده است. بنابراین، سامانه، مقایسهٔ یک به چند را برای معین‌کردن هویت فرد اجرا می‌کند. تشخیص هویت عنصر مهمی در کاربردهای تشخیص منفی است که در آن سامانهٔ زیست‌سنجی بیان می‌کند که آیا این فرد کسی است که هویت خود را انکار کرده است؟ هدف از تشخیص منفی جلوگیری از استفاده از چندین هویت توسط یک فرد است. این فیلد را همچنین می‌توان برای سهولت در تشخیص مثبت استفاده کرد (لازم نیست کاربر هویت خود را مشخص نماید). در حالی که روش‌های سنتی تشخیص فرد مانند رمز عبور، شمارهٔ شناسایی، و کلید تنها برای تشخیص مثبت قابل استفاده‌اند، تشخیص منفی تنها از طریق زیست‌سنجی قابل انجام است (DiNardo 2008).

◇ تأیید هویت[2]:

در این فیلد، بررسی می‌کنند که آیا فرد با هویت ادعاشده مطابق است یا خیر؟ تأیید فقط شامل مقایسه با یک قالب خاصی است که ادعا شده است. بنابراین، لازم

1. identification 2. verification

است که به این دو مسئله به‌صورت جدا پرداخته شود. تأیید هویت برای تشخیص مثبت استفاده می‌شود که هدف از آن جلوگیری از استفاده از یک هویت توسط افراد متعدد است (DiNardo 2008). دستگاه‌های زیست‌سنجی همواره به روش‌های مختلف مورد هجوم قرار می‌گیرند. این نوع حملات شامل حمله به پایگاه داده، حمله به پورت‌های ورودی سیستم، و حمله به سیستم تشخیص هویت از طریق زیست‌سنجی‌های جعلی است. سارقان معمولاً جهت فریب سیستم‌های تشخیص هویت از روش‌های مختلفی بهره می‌برند؛ از جمله: استفاده از عکس چهره یا عنبیهٔ فرد مقابل دوربین، ضبط باکیفیت صدای شخص در سیستم‌های زیست‌سنجی صوتی، استفاده از اثر انگشت ژلاتینی و حتی استفاده از لاشهٔ انگشت توسط سارقان جهت ورود به سیستم. فرایند تشخیص هویت می‌تواند هم از طریق نرم‌افزاری (خواندن و پردازش اطلاعات زیست‌سنجی) باشد و هم از طریق سخت‌افزارهایی که در امر تشخیص به ما کمک می‌کنند. یک روش برای جلوگیری از حمله به سیستم تشخیص هویت (جلوگیری از ورود زیست‌سنجی‌های جعلی)، استفاده از سیستم زیست‌سنجی‌های ترکیبی و افزایش تعداد زیست‌سنجی‌های سنجش هویت است. هرچند این روش ممکن است افزایش هزینه و صرف وقت بیشتری را در پی داشته باشد، اما بسیار مفید است (Jain, Kumar & Ross 2015). راه‌حل نهایی جهت فائق‌آمدن بر مشکلاتی که بعضی از فنّاوری زیست‌سنجی به همراه دارد، استفادهٔ همزمان از چند زیست‌سنجی مختلف در یک سیستم است. به این روش اصطلاحاً سیستم چندلایه[1] گفته می‌شود. در بعضی از سیستم‌های فوق امنیتی، متخصصان از روش لایه‌ای استفاده می‌کنند. سیستمی چندوجهی[2] است که چند روش شناسایی از طریق زیست‌سنجی را با هم ترکیب می‌کند؛ مثل اسکن عنبیه و الگوی صدا. و بدین‌ترتیب ضریب امنیت را افزایش می‌دهند. برای این کار باید به محاسبهٔ اولویت‌ها بپردازیم و بر اساس بیشترین امتیاز، تکنیک را انتخاب کنیم. در این مرحله به این صورت عمل می‌کنیم که «بردار ویژگی مربوط به هر تکنیک بر اساس معیار خاص» را در وزن همان معیار ضرب کرده و با هم جمع می‌کنیم. به این ترتیب، اولویت هر تکنیک محاسبه می‌شود:

1. layered
2. multimodal

شکل ۱۲. نتایج نهایی اولویت زیست‌سنجی‌ها

با توجه به نتایج به‌دست‌آمده در نمودار شکل ۱۲، مشاهده می‌شود که زیست‌سنجی اثر انگشت دارای بالاترین اولویت نسبت به دیگر زیست‌سنجی‌هاست. پس از آن ضربه به کلید بالاترین اولویت را دارد. بنابراین، ترکیب این دو زیست‌سنجی دارای بالاترین بهینگی است و پیشنهاد می‌شود برای استفاده در اینترنت اشیا و دسترسی به پایگاه‌های داده بزرگ از این ترکیب استفاده شود، زیرا این ترکیب پایین‌ترین هزینه را برای پیاده‌سازی دارد و سطح امنیت بالایی را برای سیستم برقرار می‌کند.

جدول ۸. نتیجهٔ ارزیابی تجربی تکنیک‌های زیست‌سنجی بر اساس ۷ ویژگی

زیست‌سنجی	عمومیت	منحصربه‌فرد بودن	پایداری	جمع‌آوری	عملکرد	مقبولیت	عبور از آن
تشخیص اثرانگشت	متوسط	بالا	متوسط	متوسط	بالا	بالا	متوسط
تشخیص چهره	بالا	پایین	متوسط	بالا	پایین	بالا	پایین
تشخیص عنبیه	بالا	بالا	متوسط/ بالا	متوسط/ پایین	بالا	پایین	بالا
تشخیص هندسهٔ دست	متوسط	متوسط	متوسط	بالا	متوسط	متوسط	متوسط
تشخیص کف دست	متوسط	بالا	بالا	متوسط	بالا	پایین	بالا
تشخیص صدا	متوسط	پایین	پایین	بالا	پایین	بالا	پایین
تشخیص امضا	پایین	پایین	پایین	بالا	پایین	بالا	پایین
تشخیص راه رفتن	متوسط	متوسط	پایین	متوسط	پایین	پایین	متوسط
پروفایل رفتار	بالا	پایین	پایین	بالا	پایین	متوسط	متوسط
ضربه به کلید دینامیک	بالا	متوسط	پایین	بالا	پایین	بالا	متوسط
لمس دینامیک	بالا	متوسط	پایین	بالا	پایین	متوسط	متوسط

با یک بررسی اجمالی در نتایج ارائه‌شده در جدول ۸، می‌توان به این نتیجه رسید که تکنیک‌های زیست‌سنجی فیزیولوژیکی دارای نتایج بهتری نسبت به تکنیک‌های زیست‌سنجی رفتاری هستند. بنابراین، احتمال موفقیت در استفاده از زیست‌سنجی فیزیولوژیکی در کاربردهای مختلف بالاتر از تکنیک‌های رفتاری است.

۷. نتیجه‌گیری

امروزه استفادهٔ روزافزون از اینترنت توسط عموم جامعه و ارائهٔ خدمات الکترونیکی توسط بنگاه‌های اقتصادی و تجاری از طرفی و گسترش ابزار و تجهیزات ورود به فضای سایبر از طرف دیگر، اهمیت تأمین امنیت تبادل اطلاعات در فضای مجازی را روز به روز پررنگ‌تر می‌کند؛ چرا که همزمان با گسترش اینترنت و ارائهٔ انواع خدمات با این فنّاوری، نفوذ افراد غیرمجاز و سوء استفاده‌کنندگان به‌طوری فزاینده پیچیده و گسترده شده است. لذا، ابداع و تدوین راهکارهای جدید و پیشرفتهٔ تأمین امنیت تبادل اطلاعات، به‌طور مداوم مورد نیاز بوده و در حال انجام است. در این مقاله به تعریف ویژگی‌های اساسی اینترنت اشیا، توصیف فنّاوری‌های مورد نیاز آن و همچنین، پیش‌بینی برنامه‌های کاربردی برای دسترسی امن پرداختیم. علاوه بر این، دربارهٔ چالش عمده‌ای که در راه تحقق اینترنت اشیا با آن‌ها مواجه هستیم، بحث شد و روش پیشنهادی با استفاده از ویژگی‌های زیست‌سنجی شرح داده شد. با توجه به این‌که اینترنت به شکلی بسیار گسترده نحوهٔ زندگی ما را تغییر داده است، ارتباطات مردم در سطح مجازی را چه در حیطهٔ شغلی و در چه در روابط اجتماعی تحت تأثیر قرار داده است. اینترنت اشیا نیز این پتانسیل را دارد که بُعد دیگری را به این فرایند اضافه کند و ارتباط بین اشیاء هوشمند را با استفاده از روش‌های ایمن و جدید ممکن سازد و در نتیجه، به چشم‌انداز «هر زمان، هرکجا، هر رسانه، هر چیز» دنیای ارتباطات دست پیدا کند. گسترش نسل جدیدی از اشیاء مجهز به هوش مصنوعی به همراه توانایی برقراری ارتباط و حرکت باعث حرکت سریع برای تحقق اینترنت اشیا شده است. با توجه به این الگوی در حال ظهور همه‌چیز یکپارچه به یک زنجیرهٔ مجازی از اشیاء به‌هم‌پیوسته و دارای نشانی در دنیای پویای شبکه متصل خواهد شد. با توجه به اهمیت اتصال ایمن اشیا به اینترنت و دسترسی به آن‌ها، از ویژگی‌های زیست‌سنجی به‌عنوان شناسه استفاده می‌شود، زیرا آن‌ها را نمی‌توان امانت داد یا خرید یا فراموش کرد و خیلی دشوار است که بتوان آن‌ها را جعل نمود. در این مقاله با استفاده از ویژگی‌های

زیست‌سنجی و استاندارد تشخیص سریع برخط، دسترسی ایمن‌تر 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 جاسازی‌شده و مورد استفاده برای تعاملات داخلی در داخل شبکه و برای تعاملات میان اشیا و محیط تشکیل می‌دهد. مثال‌هایی از این مورد شامل حسگرهای توکار مختلف، تکنولوژی خانه‌های هوشمند، روش‌های مدرن ارتباطات مانند برنامه‌های مدیریت کنترل وزن، وسیله‌های عکاسی و ویدیوئی، آژیرها، دیکشنری‌ها، پویشگرها، بازی‌ها و غیره هستند. این تنها یک‌سوی مفهوم اینترنت اشیا است که مادی یا فیزیکی بودن شیء را منعکس می‌سازد و می‌تواند با ترکیب مواد از نشانه‌ها مقایسه شود. قفل‌های هوشمند، ترموستات‌های هوشمند، خودروهای هوشمند، مطمئناً این‌ها واژه‌هایی هستند که بارها و بارها شنیده‌اید و البته، در سال‌های آتی بیشتر خواهید شنید. همهٔ دستگاه‌های یادشده در دسته‌ای به نام اینترنت اشیا یا به‌طور مخفف IOT قرار می‌گیرند. در سطح پایه‌ای، اینترنت اشیا در واقع، به ارتباط اشیاء مختلف از طریق اینترنت و برقراری ارتباط با یکدیگر می‌پردازد تا هدف آن یعنی فراهم‌کردن تجربهٔ کاراتر و هوشمندتر محقق شود. همانند دیگر فنّاوری‌های جدید، اینترنت اشیا نیز می‌تواند در ابتدا مفهومی سردرگم‌کننده به نظر برسد. همچنین، این واژه، به‌ویژه هنگامی‌که صحبت از استانداردهای مختلف و همچنین ایمنی و امنیت آن می‌شود، می‌تواند مفاهیم جدید و ویژه‌ای پیدا کند. از نظر دیگر، با توجه به چالش‌های امنیتی موجود برای برقراری ارتباط باید چاره‌ای اندیشید. برای برطرف‌نمودن چالش‌های امنیتی استفاده از زیست‌سنجی پیشنهاد می‌شود. البتهٔ باید در نظر داشت که سیستم‌های زیست‌سنجی هر کدام به‌تنهایی دارای ضعف‌هایی هستند که برای برطرف‌شدن این ضعف‌ها سیستم زیست‌سنجی ترکیبی پیشنهاد می‌شود. با توجه به این‌که در ترکیب‌کردن زیست‌سنجی‌ها محدودیت‌هایی از قبیل هزینه و پیچیدگی پیاده‌سازی وجود دارد، یک ترکیب بهینه برای سیستم اینترنت اشیا معرفی کردیم. با توجه به نتایج حاصل از تحلیل سلسله‌مراتبی ترکیب اثر انگشت بر اساس تکنولوژی FIDO و ضربه به کلید را به‌عنوان ترکیب بهینه معرفی می‌نماییم.

پیشنهادهایی برای آینده: اینترنت اشیا ممکن است جهش بزرگ رو به جلو بعدی در بخش ICT را موجب شود. احتمال ادغام یکپارچهٔ جهان واقعی و مجازی از طریق گسترش

عظیـم دسـتگاه‌های تعبیه‌شـده، مسـیرهایی مهیـج و جدیـد، هـم بـرای پژوهـش و هـم کسـب‌وکار ایجـاد می‌کنـد. بـا اجـرای ایـن شـیوه، در نهایـت ممکـن اسـت محیـط پیرامـون بشـر بـه چیـزی شـبیه آنچـه کـه در فیلم‌هـا و داسـتان‌های تخیلـی اشـاره می‌شـود، نزدیـک شـود. به‌عنـوان مثـال، بهره‌گیـری از ایـن روش باعـث می‌شـود کـه کلیـۀ وسـایل هوشـمند پیرامـون مـا بتواننـد در زمانـی مشـخص فعـال شـده، فعالیـت از قبـل تعیین‌شـده را انجـام داده و سـپس خامـوش شـوند. امیدواریـم کـه ایـن بررسـی بـرای پژوهشـگران و شـاغلان در ایـن زمینـه مفیـد واقـع شـود و بـه آن‌هـا بـرای درک و فهـم پتانسـیل بـزرگ اینترنـت اشـیا و دسترسـی از طریـق روش پیشـنهادی کمـک کنـد تـا راه‌حل‌هـای فنـی نوآورانـه‌ای را تدبیـر کننـد و در آینـده‌ای نزدیـک شـاهد آن باشـیم کـه اینترنـت اشـیا از یـک دیـدگاه پژوهشـی بـه یـک واقعیـت کاربـردی تبدیـل شـود.

فهرست منابع

Aggarwal, C. C., & Wang, H. 2011. Text mining in social networks. In Social network data analytics (pp. 353-378). Springer, Boston, MA.

Alur, R., E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, D. Lopresti, K. Nahrstedt, E. Mynatt, S. Patel, J. Rexford, J. A. Stankovic, and B. Zorn. 2016. Systems Computing Challenges in the Internet of Things. https://arxiv.org/abs/1604.02980 (accessed Sep. 22, 2017).

Daqiang, Z., G. Minyi, Z. Jingyu, K. Dazhou and C. Jiannong. 2010. Context reasoning using extended evidence theory in pervasive computing environments, *Future Generation Computer Systems* 26 (2): 207-216.

Dijkman, R. M., B. Sprenkels, T. Peeters, and A. Janssen. 2015. Business models for the Internet of Things. *International Journal of Information Management* 35 (6): 672-678.

Di Nardo, J. V. 2008. Biometric Technologies: Functionality, Emerging Trends, and Vulnerabilities. *Journal of Applied Security Research* 4 (1-2): 194-216.

Eleonora, E. 2014. The Internet of Things vision: Key features, applications and open issues. *Computer Communications* 54: 1-31.

Eunhwa, J., and K. Hong. 2015. Biometric verification based on facial profile images for mobile security. *Journal of Systems and Information Technology* 17 (1): 91-100.

Farooq, M. U., M. Waseem, A. Khairi, and S. Mazhar. 2015. A Critical Analysis on the Security, Concerns of Internet of Things (IoT). *International Journal of Computer Applications* 111 (7): 1-6.

Giroux, S., and H. Pigot. 2005. *From smart homes to smart care: ICOST 2005*. Washington: IOS Press.

Han, S. S. 2005. Global city making in Singapore: a real estate perspective. Progress in Planning, 64 (2), 69-175.

In, L., and L. Kyoochun. 2015. The Internet of things: Applications, investments, and challenges for enterprises. *Business Horizons* 58 (4): 431-440.

Jain, A., K. Nandakumar, and A. Ross. 2005. Score normalization in multimodal biometric systems. *Pattern Recognition* 38 (12): 2270-2285.

Nataliia, L., & Elena, F. (2015). Internet of things as a symbolic resource of power. *Procedia-Social and Behavioral Sciences*, *166*, 521-525.

O'droma, M., and I. Ganchev. 2010. The creation of a ubiquitous consumer wireless world through strategic ITU-T standardization, *IEEE Communications Magazine* 48 (10): 158–165.

Srivastava, L. 2004. Japan's ubiquitous mobile information society. *Info* 6 (4): 234–251.

Ulrich, G., G. Peter, J. Benjamin, and L. Dennis. 2012. *Multimedia content identification through smart meter power usage profiles.* Proceedings of the International Conference on Information and Knowledge Engineering (IKE). Athens: 1-8.

Venier, S. 2009. *Ethical aspects of biometric identification technologies in a multicultural society*. AECME annual meeting. Venice, 10–11 September.

Verma, I., & Jain, S. K. (2015, March). Biometrics security system: A review of multimodal biometrics based techniques for generating crypto-key. In Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on (pp. 1189-1192). IEEE

Villalbaa, A., J. L. Pe´reza, D. Carreraa, C. Pedrinacib, and L. Panzierab. 2015. servIoTicy and iServe: A Scalable Platform for Mining the IoT, *Procedia Computer Science* 52: 1022-1027.

Xia, F., L. T. Yang, L. Wang, and A. Vinel. 2012. Internet of things. *International Journal of Communication Systems* 25 (9): 1101–1102.

Zeng, D., S. Guo, and Z. Cheng. 2011. The web of things: a survey, *Journal of Communications* 6 (6): 424–438.

Zhang, D., Zhang, D., Xiong, H., Hsu, C. H., & Vasilakos, A. V. (2014). BASA: building mobile Ad-Hoc social networks on top of android. *IEEE Network*, *28* (1), 4-9.

Zhang, D., J. Zhou, M. Guo, J. Cao, and T. Li. 2011. tag-free activity sensing using RFID tag arrays. *IEEE Transactions on Parallel and Distributed Systems* 22 (4): 558–570.

اعظم‌السادات پرئی

دارای مدرک تحصیلی کارشناسی ارشد مهندسی فنّاوری اطلاعات گرایش تجارت الکترونیک از دانشگاه صنعتی خواجه نصیرالدین طوسی است.

زمینهٔ علاقه‌مندی وی تجارت الکترونیک و کسب‌وکار است.

حجت‌اله حمیدی

متولد سال ۱۳۵۵، دارای مدرک تحصیلی دکتری در رشتهٔ مهندسی کامپیوتر و فنّاوری اطلاعات و استادیار گروه فنّاوری اطلاعات دانشگاه صنعتی خواجه نصیرالدین طوسی است.

زمینهٔ علاقهٔ کاری ایشان تجارت الکترونیک، کسب‌وکار هوشمند، و محاسبات نرم است.