رویداد

واکنش وزیر ارتباطات به اختلال در بازی کلش

● **شرق:** وزیر ارتباطات و فناوری اطلاعات گفت: اعتراضاتی به اختلال بازی کلش از سوی دنبال‌کنندگان صفحه اجتماعی بنده مطرح شده که این مطالب را به اطلاع کمیته تعیین مصادیق محتوای مجرمانه خواهم رساند. اواسط هفته گذشته دسترسی به بازی کلش‌آوکلنز با مشکل مواجه و سپس رفع شد. عبدالصمد خرم‌آبادی، معاون قضائی دادستان کل کشور، درباره اختلال ایجادشده در بازی «کلش‌آوکلنز» از اعمال محدودیت برای دسترسی به این بازی خبر داد و گفت: اکثریت قریب‌به‌اتفاق اعضای کارگروه تعیین مصادیق محتوای مجرمانه با اعمال محدودیت برای دسترسی به این بازی موافقت کردند. محمود واعظی نیز با حذف برخی اظهارنظر کاربران اینترنت از صفحه شبکه اجتماعی خود که ادبیات مناسبی نداشتند، بیان کرد: در چند پست اخیر اعتراضاتی به اختلال بازی کلش از سوی دنبال‌کنندگان صفحه اجتماعی من مطرح شده که این مطالب را به اطلاع کمیته تعیین مصادیق محتوای مجرمانه خواهم رساند. او ادامه داد: مطالب مطرح‌شده را پیگیری خواهم کرد اگرچه در بعضی موارد به دلیل استفاده از ادبیات نامناسب مجبور به حذف آنها شدم.

بی‌ارزش‌بودن ۷۵ درصد صفحات وب فارسی

● **ایسنا:** به گفته مدیر اجرائی موتور جست‌وجوگر پارسی‌جو در میان چهار میلیارد صفحه فارسی شناسایی‌شده به وسیله جست‌وجوگر پارسی‌جو، نزدیک به یک میلیارد آن، یعنی چیزی در حدود ۲۵ درصد، ارزشمند بوده و بقیه صفحات تکراری یا اسپم بوده است که نشان از ضعف تولید محتوا در زبان فارسی دارد. امیرعلی خیراندیش دراین‌باره بیان کرد: حجم بالای صفحات بی‌ارزش، دو چالش بزرگ را پیش‌روی پارسی‌جو در پوشش صفحات وب فارسی قرار داده است، این جست‌وجوگر ملی برای کشف صفحات وب مفید فارسی باید تعداد زیادی از صفحات را شناسایی کند درحالی‌که تنها ۲۵ درصد آنها قابل استفاده برای کاربران است که همین عامل علاوه بر اتلاف زمان، فشار زیادی بر سرورها وارد می‌کند، ضمن اینکه پارسی‌جو برای حفظ و ارتقای کیفیت خود، ملزم به ارتقای مداوم هوش مصنوعی خود در بخش خزش، نمایه‌سازی و رتبه‌بندی است. او ادامه داد: جویشگر پارسی‌جو به کمک نسخه جدید فنی خود، توانسته است به رکورد تحت پوشش قراردادن چهار میلیارد صفحه وب فارسی برسد که در مقایسه با رقم دو میلیارد در مدت مشابه سال پیش، نشان از افزایش صددرصدی میزان پوشش نسخه جدید این جست‌وجوگر است. او گفت: استفاده بیش از ۱۵ سرویس متنوع برای ارتقای کیفیت نتایج جست‌وجو، پوشش چهار میلیارد سند فارسی، قدرت پاسخ‌گویی به میلیون‌ها پرس‌وجو در روز، استفاده از خزشگر هوشمند با پوشش میلیاردها سند از جمله ویژگی‌های جست‌وجوگر ملی پارسی‌جو است.

۷۰ درصد اعتبارات در ردیف‌های متفرقه است

● **شرق:** بررسی لایحه بودجه ۱۳۹۶ در بخش ارتباطات و فناوری اطلاعات نشان می‌دهد بیش از ۷۰ درصد اعتبارات فاوای بودجه ۱۳۹۶ و بودجه ۱۳۹۵ در قالب ردیف‌های متفرقه و فاقد برنامه، فعالیت و کمیت‌های زمان شروع و پایان و نوع خروجی است که نظارت را سخت می‌کند. دفتر مطالعات فناوری‌های نوین مرکز پژوهش‌های مجلس شورای اسلامی گزارش بررسی لایحه بودجه سال ۱۳۹۶ کل کشور را با نگاهی اجمالی به فناوری اطلاعات و ارتباطات منتشر کرده است. در این گزارش آمده، جمع اعتبارات فناوری اطلاعات و ارتباطات در لایحه بودجه ۱۳۹۶ نسبت به قانون بودجه ۱۳۹۵ حدود دو درصد کاهش داشته و به رقم ۱۱۸،۴۸۵ میلیارد ریال رسیده است. این رقم ۳،۲ درصد از جمع کل اعتبارات عمومی کشور است. بیش از ۷۰ درصد اعتبارات فاوای لایحه بودجه ۱۳۹۶ و قانون بودجه ۱۳۹۵ در قالب ردیف‌های متفرقه است و فاقد هرگونه برنامه، فعالیت و کمیت‌های پایه‌ای نظیر زمان شروع و پایان، نوع خروجی و... است که نظارت بر آنها را سخت می‌کند. در راستای شفافیت بودجه‌ای، انتقال اعتبارات متفرقه به ردیف‌های برنامه‌ای متناظر مثبت خواهد بود. از آنجا که اعتبارات وزارت ارتباطات و فناوری اطلاعات عموما بالای ۵۰ درصد محقق می‌شوند و سابقه چندساله دارند، قابلیت برنامه‌ریزی و انتقال آنها به بخش اعتبارات برنامه‌ای کاملا امکان‌پذیر است.

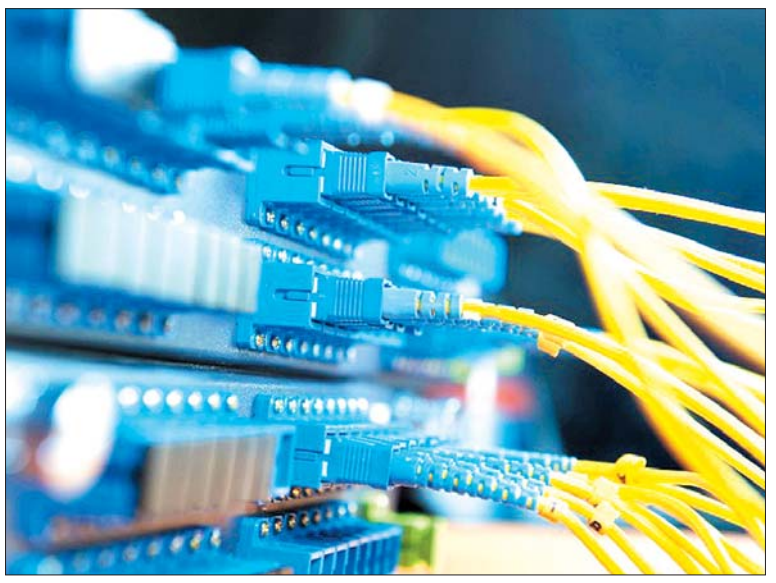
احراز هویت دارندگان کانال‌های شبکه‌های اجتماعی

● **فارس:** با اضافه‌شدن بخش کانال تلگرام و صفحه شخصی در رسانه کاربرمحور (مانند صفحات اینستاگرام و پروفایل‌های کلوب) به سامانه ساماندهی وزارت ارشاد به آدرس samandehi.ir احراز هویت فعالان فضای مجازی بیش از پنج هزار عضو پیرو مصوبه شورای عالی فضای مجازی آغاز شده است. دارندگان این شبکه‌ها برای ثبت‌نام و احراز هویت یک ماه فرصت دارند.

مخابرات تکذیب و رگولاتوری تلویحا تأیید کرد

قطع سرویس تلفن ثابت یک شرکت اینترنتی

حامد شفیعی



براساس ادعای یکی از شرکت‌های دارنده پروانه ارتباطات ثابت (FCP)، تنها دو روز پس از ارائه تلفن ثابت از سوی شرکت شاتل، شرکت مخابرات ایران در یک اقدام غیرقانونی اتصال متقابل مابین را قطع کرد.

چند روز پیش، این شرکت اقدام به ارائه تلفن ثابت به مشترکان ADSL خود و بر بستر اینترنت کرد. این تلفن با پیش‌شماره ۹۱۰۰ در تهران شروع می‌شد و تنها در جایی کار می‌کرد که مشترک به اینترنت شاتل دسترسی داشته و اپلیکیشن مخصوص را روی گوشی همراه نصب کرده باشد. به گفته مدیران این شرکت اما مخابرات ایران در یک اقدام یک‌طرفه، اتصال متقابل را قطع کرد؛ به‌طوری‌که درحال‌حاضر از طریق خطوط تلفن ثابت نمی‌توان با این شماره‌ها تماس گرفت و تماس از سوی این شماره‌ها با تلفن ثابت نیز امکان‌پذیر نیست.

تماس از طریق این شماره‌ها بین مشترکان و با تلفن ثابت و موبایل ارزان‌تر از استفاده از تلفن ثابت شرکت مخابرات ایران بود.

این شرکت در پیامی به کاربران خود اعلام کرده بود: «بی‌گمان شما کاربر عزیز اطلاع دارید به‌تازگی خدمات تلفن روی اپلیکیشن ShatelTalk را ارائه کرده که خوشبختانه با استقبال اعضای خانواده شاتل روبه‌رو شده است. ضمن آنکه این فعالیت براساس پروانه قانونی صادر شده و با حمایت وزارت ارتباطات و فناوری اطلاعات آغاز شده است، شرکت مخابرات ایران (و مخابرات استان‌ها) در پی اقدامی غیررقابتی طی روزهای گذشته ارتباطات این شرکت را قطع کرده‌اند. براین‌اساس، این موضوع در حال پیگیری توسط مقامات محترم وزارت ارتباطات و فناوری اطلاعات و سازمان تنظیم مقررات و ارتباطات رادیویی است و انتظار داریم ظرف روزهای آینده این مشکل و رفتار غیررقابتی صورت گرفته، برطرف شود. با توجه به این موضوع، واگذاری سرویس تا حل این مشکل متوقف خواهد بود. چه آنکه عزیزانی که تاکنون این سرویس را تهیه کرده‌اند، شاهد مشکلاتی در تماس‌های خود خواهند بود».

درهمین‌حال، حسین فلاح‌جوشقانی، معاون نظارت و اعمال مقررات سازمان تنظیم مقررات و ارتباطات رادیویی، در گفت‌وگو با رسانه دولت گفته است: «این اتفاق در حال بررسی است و هنوز مشخص نیست چرا مخابرات این کار را انجام داده است. ما از مخابرات درخواست کرده‌ایم دلایل خود را برای قطع اینترکانکشن (اتصال متقابل) این شرکت اینترنتی که به‌تازگی اقدام به ارائه خدمات تلفن ثابت کرده بود، اعلام کند. این شرکت تمامی مستندات خود برای این اقدام را تحویل رگولاتوری داده و ما باید براساس روال، بررسی‌های خود را بر این مستندات را انجام دهیم؛ اما در نهایت تا شنبه نتیجه بررسی‌های خود را اعلام خواهیم کرد». شرکت مخابرات ایران نیز در واکنش به ادعای شاتل، اطلاعیه‌ای صادر کرد. شرکت مخابرات ایران در اطلاعیه خود مدعی شده شرکت شاتل قرارداد اتصال متقابل را امضا نکرده است. در اطلاعیه شرکت مخابرات ایران آمده است: «برای برقراری ارتباطات بین شبکه تلفنی ثابت شرکت شاتل با شبکه‌های موجود سایر اپراتورها، نیازمند قرارداد اتصال متقابل است که این شرکت اقدامی برای امضای این قرارداد نکرده است. در نتیجه مشخص نیست هزینه‌های مربوط به دولت، شرکت ارتباطات زیرساخت و شرکت مخابرات ایران که قرار است تأمین‌کننده زیرساخت ارتباطی باشند، چگونه باید پرداخت شود. بنابراین این شرکت باید در اسرع وقت مانند سایر اپراتورها (همراه و ثابت) نسبت به امضای قرارداد براساس هزینه‌های تمام‌شده اقدام کند تا بتواند از مزایای ارتباط متقابل برخوردار شود. همچنین شرکت شاتل نه‌تنها با شرکت مخابرات ایران بلکه با اپراتورهای تلفن همراه هم قرارداد اتصال متقابل امضا نکرده است و بنابراین مشترکان احتمالی این شرکت، قادر به ارتباط اینترنتی فقط با مشترکان اپراتور مذکور خواهند بود. از طرفی برقراری ارتباط متقابل توسط این شرکت در شش استان به طور آزمایشی بوده و با وجود امضانکردن قرارداد اتصال متقابل، در دو استان که چند مشترک دارد، ارتباط این شرکت برقرار است. آنچه تاکنون توسط شرکت شاتل اعلام شده، تست تلفن ثابت بر بستر اینترنت برای توسعه آتی بوده است.

معاون نظارت و اعمال مقررات سازمان تنظیم مقررات و ارتباطات رادیویی، در گفت‌وگو با رسانه دولت گفته است: این اتفاق در حال بررسی است و هنوز مشخص نیست چرا مخابرات این کار را انجام داده است. ما از مخابرات درخواست کرده‌ایم دلایل خود را برای قطع اینترکانکشن (اتصال متقابل) این شرکت اینترنتی که به‌تازگی اقدام به ارائه خدمات تلفن ثابت کرده بود، اعلام کند

دراین‌باره شرکت مخابرات ایران هم نسبت به هرگونه همکاری در چهارچوب قوانین و مقررات استقبال کرده و آماده همکاری خواهد بود. مصداق ادعای شرکت مخابرات ایران در ادعای بند فوق، اجرای مصوبه ۲۳۰ ابلاغ‌شده از سوی سازمان تنظیم مقررات و ارتباطات رادیویی درخصوص ارائه امکانات مورد نیاز شرکت‌های FCP و PAP است که این شرکت طی سال جاری با راه‌اندازی سامانه ثبت مکانیزه درخواست‌های شرکت‌های دارنده پروانه، نیازهای شرکت‌های فوق را در اختیار آنان قرار داده است و در این میان، شرکت شاتل تمامی امکانات مورد درخواست خود را دریافت کرده است.

گفتنی است این خدمات از طریق همین سامانه به صورت برخط (آنلاین) توسط سازمان تنظیم مقررات و ارتباطات رادیویی پایش و نظارت کامل شده و ضمنا تمامی خدمات درخواستی شرکت‌های دارنده پروانه و ارائه‌شده به آنها در سراسر کشور، توسط شرکت مخابرات ایران کنترل و بررسی می‌شود. در پایان انتظار می‌رود مسئولان شرکت شاتل ضمن رعایت اخلاق حرفه‌ای و احتراز از فرافکنی، مقید به رعایت مقررات تعاملی و مناسب با دیگر بازیگران این عرصه باشد و با تعامل و براساس مجوزها و مقررات، اهداف خود را پیگیری کنند». با وجود ادعای طرفین، دو نکته شایان توجه است؛ اول آنکه به نظر می‌رسد براساس مصوبه ۲۳۴ کمیسیون، هیچ طرفی، ولو با فسخ قرارداد، حق قطع اتصال متقابل را ندارد.

همچنین براساس ادعای مدیرعامل شرکت مخابرات ایران، مخابرات فقط مسئول واگذاری خط‌های جدید تلفن ثابت نیست.

درواقع بنابر اظهارات سرایان، در حوزه تلفن ثابت، اکنون با ایجاد ۱۷ شرکت FCP، دیگر فقط مخابرات مسئولیت تأمین تلفن ثابت را برعهده نداشته و مانند تلفن همراه که می‌توان سیم‌کارت آن را از سوی سه اپراتور دریافت کرد، درباره تلفن ثابت نیز مردم می‌توانند از این شرکت‌ها خرید داشته باشند.

بازتاب

حملات سایبری ۲۰۱۶

● سال گذشته میلادی را می‌توان سال ثروتمندشدن هکرها در سطح جهان نامید. حملات گسترده‌ای که با موفقیت‌های چشمگیری همراه بوده و دولت‌ها را به فکر تقویت توانمندی‌های آفندی و پدافندی سایبری خود انداخته است. حوزه اقتصاد و سلامت دو حوزه اصلی تهاجمات سایبری در سال گذشته هستند که بیشترین خبرهای حملات هکری را به خود اختصاص داده‌اند.

حملات DDOS: به گزارش سایبربان، حمله اخیر به زیرساخت‌های اینترنتی جهان در شرکت DynDNS نشان داد که هنوز هم اینترنت برابر حملات دیداس ناتوان است و حملات گسترده این‌چنینی می‌تواند شرکت‌های بزرگ اینترنتی و به تبع آن شرکت‌های تجاری بزرگ را فلج کند.

بدافزارها و باج‌افزارها: تقریبا گزارش‌های منتشرشده از سوی تمامی شرکت‌های امنیتی حاکی از آن است که میزان فعالیت باج‌افزارها به‌شدت رو به رشد است و بازار هکری را از نظر اقتصادی بسیار جذاب‌تر می‌کند. این رشد فعالیت‌های هکری بیشتر حوزه‌هایی مانند سلامت و اقتصاد را نشانه رفته که میزان تخصص امنیتی در آنها کمتر است.

حملات نرم‌افزارهای خاص: هکرها نرم‌افزارهای خاصی را در رایانه و موبایل هدف قرار می‌دهند که امکان دسترسی به اطلاعات کامل کاربر را فراهم می‌کنند. کاربران نیز به خاطر اطلاع‌نداشتن از دسترسی‌های گسترده‌ای که نرم‌افزارها به اطلاعاتشان دارند، اغلب در مقابله با این حملات ناتوان هستند. از هر پنج حمله سایبری که در ۲۰۱۶ صورت گرفته، یکی از آنها با استفاده از حملات نرم‌افزاری انجام شده است.

حملات وب‌ابزارها: حملات وب‌ابزارها به گزارش مردمی، بیشترین و آسان‌ترین راه حمله به کاربران را به خود اختصاص داده است. هکرها با استفاده از روش‌هایی مانند SQL injections، cross-site scripting می‌توانند به رایانه‌های کاربران نفوذ کرده و به اطلاعات حساس دسترسی داشته باشند. این نوع حملات باعث شده طراحان نرم‌افزارها با چالشی اساسی در زمینه امنیت روبه‌رو شوند. در این بازی همیشه هکرها یک قدم جلوتر از طراحان نرم‌افزارها حرکت می‌کنند که کار شناسایی و مقابله با راه‌های نفوذ را سخت‌تر می‌کند. برگزاری کمپین‌های عیب‌یابی داوطلبانه و استفاده از هکرهای کلاه‌سفید می‌تواند در این زمینه به شرکت‌ها کمک کند.

بازار

بازار ۷۸۰ میلیارد دلاری پرداخت موبایلی در ۲۰۱۷

طبق گزارش جدید منتشرشده از مؤسسه تحقیقاتی TrendForce حجم بازار پرداخت موبایلی در سال آینده باز هم ارتقا یافته و به رقم بی‌سابقه ۷۸۰ میلیارد دلار تا پایان سال ۲۰۱۷ می‌رسد. بنا بر این گزارش نوآوری و تنوع دو عامل ایجاد تقاضا و فرصت‌های جدید در این بازار رو به رشد به حساب می‌آیند. Kelly Hsieh مدیر ارشد تحقیقاتی در مؤسسه TrendForce در این رابطه می‌گوید: «در میان سازندگان اسمارت‌فون که همچنین در حال توسعه کسب و کار پرداخت موبایلی خود نیز هستند، اپل و سامسونگ دو برندی هستند که بر رقبای خود برتری دارند. گوگل نیز با توجه به اینکه اندروید در سطح جهانی از سهم بازار بیش از ۵۰درصدی برخوردار است، از شانسی برای ساخت یک اکوسیستم گسترده پرداخت موبایلی برخوردار است. گوگل اخیرا توسعه جهانی پلتفرم کیف پول دیجیتالی خود Android Pay را تسریع کرده و در ماه دسامبر با اعلام همکاری با کمپانی بزرگ اینترنتی و e-commerce ژاپنی راکوتن، گام بزرگی را رو به جلو برداشته است». به گفته Hsieh بازار پرداخت موبایلی کشور ژاپن تقریبا به‌طورکامل به وسیله شرکت‌های بومی داخلی احاطه شده و شرایط دشواری برای حضور رقبای خارجی در مقایسه با چین یا آمریکا در این بازار به چشم می‌خورد؛ از همین رو پشتیبانی شرکت ژاپنی Rakuten از Android Pay اهمیت استراتژیک بسیار بالایی برای گوگل خواهد داشت. به این ترتیب کاربران Android Pay در ژاپن از این پس به پلتفرم پول مجازی (e-money) راکوتن موسوم به Edy (که در بسیاری از رستوران‌ها و فروشگاه‌های زنجیره‌ای ژاپن استفاده می‌شود)، دسترسی خواهند داشت. براساس گزارش وب‌سایت mobile، گوگل همچنین در حال رایزنی با شرکت سونی برای جای‌دادن فناوری FeliCa این شرکت درون یک کارت مجهز به IC دارای NFC با قابلیت کارکرد با گوشی‌های هوشمند است. FeliCa راه‌حل پرداخت هوشمند شرکت سونی به حساب می‌آید که براساس RFID عمل می‌کند. فعالیت گوگل برای استحکام اکوسیستم Android Pay این شرکت در ژاپن در سال آینده نیز ادامه یافته و سرویس‌های پرداخت و مؤسسات مالی دیگر به فهرست پشتیبانی گوگل افزوده می‌شوند. در گزارش TrendForce همچنین به پیشرفت‌های بزرگ در سال آینده در مقوله امنیت پرداخت موبایلی اشاره شده است؛ در این زمینه علاوه بر پیشرفت مستمر در به‌کارگیری فناوری‌های سخت‌افزاری مختلف در طراحی چیپ‌های رمزنگاری‌شده، متدهای تعیین هویت چندمرحله‌ای و الگوریتم‌های رمزگذاری نرم‌افزاری نیز نقش مهمی را در پروسه پرداخت و تبادل امن اطلاعات بر عهده می‌گیرند. NFC یا ارتباطات برد نزدیک نقشی اساسی در ارتقا و پیشرفت پروسه پرداخت موبایلی ایفا می‌کند. طبق گزارش TrendForce بیش از ۶۰ درصد اسمارت‌فون‌هایی که در سال ۲۰۱۷ به بازار ارائه می‌شوند، به این امکان ارتباطی مجهز بوده و با حضور روزافزودن این فناوری در تولیدات شرکت‌های چینی نظیر هوآوی، شائومی و Meizu این روند رو به گسترش خواهد بود. امنیت تبادل دیتا بر مبنای NFC نکته مهم دیگری است که به گفته Hsieh ارتباط مستقیمی با مقوله کنترل دسترسی یا access control دارد؛ این تحلیلگر TrendForce به اهمیت کنترل دسترسی در دو مقوله نرم‌افزاری و سخت‌افزاری اشاره می‌کند که در بخش اول درنظرداشتن شرایط اپلیکیشن پرداخت هنگام ساخت ماژول NFC و در بخش دوم تلفیق انواع مختلف آی‌سی‌های امنیتی در کنترلر چیپ ضروری خواهد بود. به عنوان نمونه ماژول‌های NFC می‌توانند به سنسورهایی برای تشخیص اثر انگشت، عنبیه چشم یا حتی رگ‌های خونی (که همانند چشم و اثر انگشت از ترکیب منحصربه‌فردی برای هر شخص برخوردارند) مجهز شده و با به‌کارگیری فناوری‌های بیومتریک مختلف، مکانیسم تشخیص هویت چندمرحله‌ای امنی را برای سیستم‌های پرداخت مبتنی بر NFC فراهم کنند. از میان این فناوری‌ها درحال‌حاضر تنها سنسورهای اثر انگشت برای پرداخت از طریق موبایل استفاده می‌شوند که با توجه به حضور این نوع از حسگرها از قبل در اسمارت‌فون‌ها شرایط مطلوبی برای فراگیرشدن این فناوری از این طریق وجود دارد. طبق پیش‌بینی TrendForce بیش از ۵۰ درصد از گوشی‌های هوشمند وارد بازار شده در سال ۲۰۱۷ به سنسور اثر انگشت مجهز خواهند بود. اسکنرهای تشخیص عنبیه چشم (iris scanner) فناوری بیومتریک دیگری هستند که شرکت‌های بزرگ سازنده اسمارت‌فون سرمایه‌گذاری‌های گسترده‌ای را برای حضور آنها در نسل بعدی گوشی‌های هوشمند به کار گرفته‌اند؛ این شیوه تشخیص هویت در مقایسه با مکانیسم تشخیص صدا و حتی اثر انگشت از دقت و امنیت بسیار بالاتری برخوردارند و پتانسیل بالایی را برای حضور در مکانیسم پرداخت موبایلی ارائه می‌کند.