بیومتریک یک باره برای بانکداری آنلاین و تأیید اعتبار پرداخت الکترونیکی

چکیده

بانکداری آنلاین و سیستم‌های پرداخت الکترونیکی در اینترنت به‌طور فزاینده‌ای پیشرفت می‌کنند. در سطح ماشین، تراکنش‌های بین مشتری و سرور میزبان از طریق یک کانال امن محافظت شده با SSL / TLS انجام می‌شود. احراز هویت کاربر معمولا براساس دو یا چند عامل است. با این وجود، توسعه malwares مختلف و حمله‌های مهندسی اجتماعی کاربران کامپیوتر را به یک وسیله مورد اعتماد تبدیل می‌کند در نتیجه احراز هویت کاربر آسیب‌پذیر است. این مقاله به بررسی نحوه احراز هویت کاربر با بیومتریک در بانکداری آنلاین با استفاده از یک وسیله خاص به نام OffPAD می‌پردازد. این مقاله نیاز دارد تا تأیید اعتبار نه تنها توسط کاربر (یا دستگاه شخصی) بلکه توسط بانک برخلاف استاندارد سیستم‌های بانکداری انجام شود. بنا به بیانی دقیق‌تر، یک پروتکل جدید برای تولید رمز عبور یک‌بار مصرف از داده‌های بیومتریک ارائه شده است، تا اطمینان حاصل شود امنیت و حریم خصوصی حفظ شده است. نتایج نشان می‌دهد با توجه به مثبت کاذب بودن نتایج عملکرد عالی بوده است. تجزیه و تحلیل امنیتی پروتکل نیز مزایای مربوط به تقویت امنیت را نشان می‌دهد.

کلمات کلیدی: پرداخت الکترونیکی، بیومتریک، امنیت بانکداری آنلاین، احراز هویت

1. مقدمه

تجارت الکترونیک در اینترنت بیشتر برای پرداخت آنلاین و بانکداری آنلاین استفاده می‌شود. بنابراین، تقلب در تراکنش‌ها یک مشکل عمده برای موسسات مالی است [11]، [3]. در واقع، اگرچه پرداخت آنلاین تنها نشان‌دهنده درصد کوچکی از معاملات است تمرکز کمی بر روی بانک‌ها دارد [19]. بسیاری از دستورالعمل‌ها مربوط به پرداخت‌های آنلاین است، به‌عنوان مثال، دستورالعمل 31/2000 / EC اروپا در مورد امنیت تجارت الکترونیک [6]، درحالی‌که دستورالعمل‌ها در مورد خدمات پرداخت [7]، عرصه‌ی گسترده‌ی اروپایی برای پرداخت و پلت‌فرم قانونی SEPA فراهم می‌کند (واحد پرداخت یورو، [8]). پروتکل D-Secure3 یک پروتکل پرداخت پیشنهاد شده توسط صنعت است که برای کاهش تقلب در پرداخت آنلاین توسعه یافته است.

در تجارت الکترونیک معمول، مشتری می‌خواهد یک سرویس آنلاین را با یک کارت اعتباری از سایت اینترنتی خریداری کند. در سطح بالا، تراکنش به‌طورکلی با احراز هویت و اتصال امن بین میزبان سرویس‌گیرنده مشتری و میزبان خدمات (SP) با استفاده از یک پروتکل مانند SSL / TLS شروع می‌شود. بار دوم، کاربر به وسیله میزبان SP خود به بانک SP اطلاعات بانکی می‌فرستد: شماره هویت شخصی (PAN)، شماره تایید کارت (CVX2) و تاریخ انقضا. پروتکل‌های SSL / TLS تأمین تراکنش بین میزبان سرویس‌گیرنده و میزبان SP را امکان‌پذیر می‌کنند. با این وجود، احراز هویت مستقیم کاربر در این طرح وجود ندارد.

چالش‌های امنیتی در تجارت الکترونیک بسیار زیاد است و به خصوص با احراز هویت کاربر مرتبط است، زیرا ارائه دهنده و صاحب کارت در طول تراکنش در یک مکان قرار نگرفته‌اند. احراز هویت به اصطلاح قوی معمولا براساس دو عامل احراز هویت است. به‌عنوان مثال، امنیت اضافی، ارسال شده توسط تلفن‌همراه، به‌عنوان پروتکل D-Secure3 [27] یا یک دستگاه اضافی مانند خواننده CAP [12]، [10] برای پرداخت الکترونیکی و بانکداری آنلاین موردنیاز است. سیستم تأیید هویت کاربر به طور سنتی توسط بانک کاربر انجام می‌شود (از آنجا که ریسک مالی در بانک اتفاق می‌افتد). احراز هویت باید جزوء حملات man-in-the-middle قرار گیرد (همانگونه که در [3] شرح داده شده است). بااین‌حال، این مقاله بر احراز هویت کاربر تمرکز دارد و چنین حملاتی خارج از اهداف مطالعاتی این مقاله است.

این مقاله یک روش جایگزین برای احراز هویت کاربر بر اساس بیومتریک ارائه می‌کند. سیستم پیشنهادی رمزهای عبور یک بار مصرف از اثر انگشت را تولید می‌کند. این داده‌های بیومتریک به‌طور مستقیم در دستگاه ذخیره نمی‌شوند و رمز عبور تولید شده برای هر تراکنش برای جلوگیری از حمله مجدد متفاوت است.

ادامه مقاله بصورت زیر سازماندهی شده است. بخش 2 به‌طور خلاصه به ارائه‌ی راه‌حل‌های احراز هویت پیشرفته برای پرداخت الکترونیکی می‌پردازد. در بخش 3 امنیت و حریم خصوصی را تعریف می‌کنیم که مسائل مربوط به راه‌حل پیشنهادی را ارائه می‌کند. در بخش 4، مفهوم OffPAD، یک دستگاه امن برای اطمینان از تراکنش‌های ماشین به ماشین (M2M) را ارائه می‌کنیم. در حال حاضر در بخش‌های این مقاله پروتکل احراز هویت پیشنهاد شده است. برخی نتایج تجربی و تجزیه و تحلیل امنیتی در بخش 6 ارائه شده است. در نهایت، نتیجه‌گیری و دیدگاه‌های مختلف در مورد این مقاله بیان شده است.

2. معماری پرداخت الکترونیکی

پروتکل پرداخت‌های ایمن الکترونیکی (SET، 24]]) که توسط VISA [1]، و MasterCard [2] توسعه یافته است، یک پروتکل برای تأمین پرداخت‌های الکترونیکی با کارت اعتباری است. کاربر احراز هویت در SET براساس یک گواهی کلید عمومی است که بر روی کامپیوتر مشتری نصب شده است. VISA و MasterCard تشخیص دادند که مدیریت گواهی‌ها برای مشتریان بسیار پیچیده بود، بنابراین پروتکل ساده D-Secure3 توسط VISA در سال 2001 به‌عنوان یک راه‌حل جایگزین برای SET پیشنهاد شد.

پروتکل D-Secure3 [27] احراز هویت فعلی و معماری پرداخت برای کارت‌های اعتباری در وب است. ابتدا توسط VISA تصویب شد، سپس سایر سازمان‌های مالی پیاده‌سازی خود را از معماری VISA 3D-Secure مانند MasterCard با SecureCode MasterCard، American Express و SafeKey توسعه دادند. یک مقایسه بین 3D Secure و MasterCard SecureCode در [21] پیشنهاد شده است. پروتکل 3D-Secure از 9 مرحله بین پنج عامل تشکیل شده است (شکل 1):

الف) کاربر به قصد خرید اطلاعات بانک خود را به SP می‌فرستد: PAN(شماره حساب شخصی)، تاریخ انقضا، CVV2 (شماره تأیید کارت). این داده‌ها برای یک ماژول اختصاصی به نام MPI (Merchant Plug In) در وب‌سایت در نظر گرفته شده‌اند.

ب) MPI سرور دایرکتوری را با پیام VEReq می‌پرسد (درخواست تأیید).

پ) سرور دایرکتوری هویت SP، شماره کارت و بانک کاربر را بررسی می‌کند و مدیریت ACSکارت Access) Control Server) را بازیابی می‌کند.

ج) پیام VERes (نتیجه تأیید) حاوی پاسخ پیام است. اگر کاربران بانک در D-Secure3 شرکت کنند ACS چک می‌کند و تأیید هویت URL را به MPI ارسال می‌کند.

د) MPI پیام PAReq (درخواست احراز هویت پرداخت‌کننده) را به URL داده شده می‌فرستد. این پیام شامل جزئیات خرید مجاز است. همچنین MPI بر روی کامپیوتر کاربر یک پنجره پاپ آپ در ACS باز می‌کند.

ه) کاربر اطلاعات لازم را برای تأیید اعتبار از بانک ارائه می‌کند.

و) ACS تأیید احراز هویت کاربر را برای MPI از طریق پیام PARes ارسال می‌کند.

ن) MPI پیام PARes را به‌عنوان تأیید هویت کاربر توسط ACS ثبت می‌کند.

ی) SP برای بانک تایید می‌کند. بانک ماهیت تراکنش از بانک کاربر را تایید می‌کند و پرداخت از SP را تایید می‌کند. SP می‌تواند پرداخت خود و کاربران را دریافت کند و کاربران بانکی اطلاعات پرداخت را برای اطمینان از تسویه حساب نگه می‌دارند.

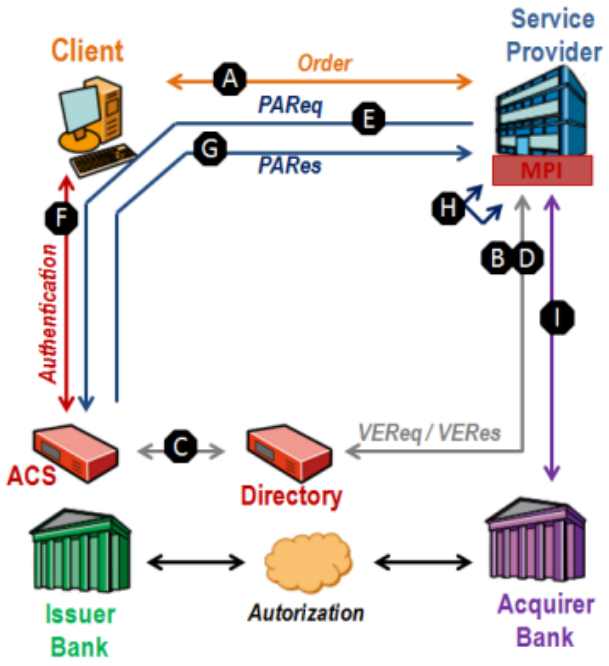

Figure 1. The 3D-Secure protocol

نقص اصلی امنیتی پیاده‌سازی‌های 3D-Secure، که در [19] تأکید شده است، مربوط به تأیید هویت کاربر (مرحله ه) است. برخی از بانک‌ها در گذشته از تاریخ تولد یا دیگر موارد استفاده می‌کردند. بسیاری از بانک‌ها این راه‌حل‌ها را با یک مکانیزم احراز هویت قوی جایگزین کرده‌اند (به‌عنوان مثال پیامی به تلفن همراه کاربر فرستاده می‌شود) و سپس دو عامل تأیید اعتبار (براساس داشتن مالکیت) تلفن‌همراه و دانستن کد PIN برای دسترسی منطقی به آن) مطرح می‌شود. با این حال ما استدلال می‌کنیم که طرح تأیید اعتبار کاربر آسیب‌پذیری قابل توجهی دارد. بنابراین یک رویکرد جدید مبتنی بر بیومتریک پیشنهاد می‌کنیم که این آسیب‌پذیری‌ها را از بین ببرد.

راه‌حل‌های تأیید هویت کاربر، که به‌عنوان خوانندگان CAP، تولیدکنندگان TAN یا سیستم سبک وزن در [17] پیشنهاد شده‌اند، رویکردهای مبتنی بر دانش هستند. بنابراین استدلال می‌کنیم که فقط بیومتریک می‌تواند کاربران را تصدیق کند، درحالی‌که راه‌حل‌های مبتنی بر دانش و اختیار، تنها تأیید اعتبار غیرمستقیم کاربران را برعهده دارند. دلیل اصلی مربوط به ارتباط خاص بین کاربر و تأییدکننده است البته مشکلات خاص مربوط به بیومتریک، در زیر ذکر شده است:

• داده‌های بیومتریک بسیار حساس هستند زیرا نمی‌توانند به طور کلی لغو شوند. رمزگذاری آن ضروری است اما کافی نیست (همانگونه که داده‌ها باید برای تطبیق فرآیند در حالت کلی رمزگشایی شوند و طول عمر داده بسیار بالا است). به همین دلیل استفاده از مرکز ذخیره‌سازی داده‌های بیومتریک مشکل‌ساز است.

فرآیند تطبیق می‌تواند اشتباهات واقعی به هنگام راهنمایی کاربران ایجاد کند و افراد متخلف می‌توانند به اشتباه پذیرفته شوند. این مسئله برای تأیید رمز عبور تا زمانی که رمز صحیح تایپ شده است درست نیست (اما هیچ اثباتی وجود ندارد که توسط کاربر واقعی تایپ شده است).

• داده‌های بیومتریک را می‌توان در حین انتقال آن متوقف کرد. این امر می‌تواند به مشکلات امنیتی منجر شود، مانند حملات پاسخ و حملات حریم خصوصی براساس قابلیت اتصال. به همین علت، داده‌های بیومتریک باید قابل لغو و پویا باشمد (تغییر در هر تراکنش).

در این مقاله، یک راه‌حل جدید را پیشنهاد می‌کنیم که این مشکلات را حل می‌کند. برای دستیابی به یک راه‌حل استاندارد امنیتی و حفظ حریم خصوصی، دو عنصر را ترکیب می‌کنیم: یکی از آنها یک دستگاه خاص متعلق به کاربر به نام OffPAD است و دومی پروتکل استفاده از بیومتریک و الگوریتم‌های قابل لغو است. در بخش بعدی، لیستی از نیازمندی‌های امنیتی و حریم خصوصی را از راه‌حل پیشنهادی بیان می‌کنیم.

3. الزامات امنیتی و حفظ حریم خصوصی

در پرداخت الکترونیکی، چهار عامل اصلی حضور دارند: کاربر C، که دارای OffPAD است، می‌خواهد یک سرویس آنلاین با یک کارت اعتباری، از طریق وب سایت ارائه دهنده خدمات SP خریداری کند. کاربر دارای یک بانک صادرکننده و SP یک بانک خریدار دارد. در این مقاله ارائه‌دهندگان پرداخت را بانک کاربر و بانک SP می‌نامیم. عامل پنجم اغلب درگیر است. این عامل به عنوان شخص ثالث صندوقدار یا دایرکتوری مورد استفاده در D-Secure3 مورداعتماد است. نقش عامل پنجم متفاوت است، اما به طورکلی امکان تایید هویت بانک‌ها را فراهم می‌کند. پروتکل پیشنهادی بر روی احراز هویت کاربر و ثبت نام کاربر با SP تمرکز دارد.

در طول پرداخت آنلاین، اطلاعات شخصی متعددی درگیر هستند و باید در برابر چندین تهدید محافظت شوند [4]. برای حفظ خصوصیات امنیتی و خصوصی، یک لیست از ده مورد الزامات RI تعریف شده است. این الزامات باید در طول احراز هویت / ثبت نام کاربر در معماری پرداخت الکترونیکی در نظر گرفته شوند:

• R1: محرمانه بودن تراکنش‌ها نیازمند آن است که هر کدام از داده‌های مبادله به منظور حفاظت در برابر نهادهای خارجی رمزگذاری شوند.

• R2: یکپارچگی اطلاعات منتقل شده، دقت محتوا و به همین ترتیب تغییر داده‌ها در حین انتقال یا ذخیره‌سازی را ممکن می‌کنند.

• R3: احراز هویت کاربر توسط یک شخص مورد اعتماد، هویت مشتری بسته به وضعیت را تضمین می‌کند، احراز هویت می‌تواند به لطف داده‌های بیومتریک تحقق یابد.

• R4: تأیید اعتبار دستگاه کاربر، معتبر بودن دستگاه در نرم افزار را تایید می‌کند. این احراز هویت می‌تواند به لطف یک شناسه دستگاه تحقق یابد.

• R5: ثابت می‌کند که دستگاه متعلق به کاربر تضمین می‌کند دستگاه را از حملات جایگزینی دستگاه حفظ می‌کند.

• R6: تأیید هویت SP توسط کاربر یا توسط یک بخش مورد اعتماد، هویت SP را تضمین می‌کند.

• R7: تأیید اعتبار بانک توسط یک شخص مورد اعتماد هویت بانک SP و بانک مشتری را تضمین می‌کند.

• R8: عدم پیوند تراکنش‌ها مانع پیوند تراکنش‌های مختلف از همان مشتری می‌شود.

• R9: محرمانه بودن اطلاعات مشتری CI (اصل کمینه سازی داده) تنها دسترسی افراد مجاز به این اطلاعات را تضمین می‌کند. این مورد به بیومتریک داده‌های کاربر نیاز دارد که برای بانک‌ها و SP مشخص نیست.

• R10: حاکمیت اطلاعات بدین معنی است که اطلاعات شخصی مرتبط با مشتری می‌تواند تنها با کنترل پردازش و رضایت او انجام شود.

در بخش بعد، مفهوم OffPAD را به عنوان دستگاهی امن برای تضمین امنیت عملیات حساس معرفی می‌کنیم.

4. مفهوم OFFPAD

PAD (دستگاه تایید شخصی) توسط Jøsang و Pope [13] به‌عنوان یک دستگاه امن خارجی برای پلت‌فرم کامپیوتر مشتری شرح داده شده است. PAD مفهومی پیشین از OffPADاست. OffPAD (دستگاه تأیید هویت آفلاین شخصی) توسط Klevjer و همکارانش [16] و Varmedal و همکارانش توصیف شده است. [26] که یک نسخه پیشرفته از PAD است و یک ویژگی اساسی برای تضمین امنیت آفلاین (ارتباطات ماشین به ماشین) است. OffPAD نشان‌دهنده مدیریت محلی هویت کاربر محور است زیرا امکان مدیریت امن و کاربرپسند را برای هویت‌های دیجیتالی و اعتبارات محلی بر روی کاربر فراهم می‌کند. OffPAD تأیید اعتبار هویت کاربر و ارائه‌دهنده خدمات (به‌عنوان مثال احراز هویت متقابل) را برعهده دارد و علاوه بر این می‌تواند تأیید اعتبار داده را نیز پشتیبانی کند. برای دسترسی به OffPAD، کاربر باید دستگاه را با استفاده از به عنوان مثال، یک پین، رمز عبور، بیومتریک یا سایر کافی اعتبارات احراز هویت باز کند. طراحی OffPAD در شکل 2 نشان داده شده است.

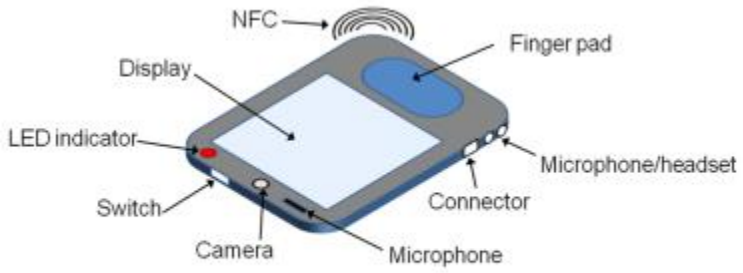

Figure 2. OffPAD concept [26].

OffPAD یک دستگاه قابل اعتماد است، به این معنی که طوری در نظر گرفته شده که در مقابل حملات مربوطه به اندازه کافی محافظت شده است. OffPAD اتصال محدودی به سیستم عامل مشتری دارد. بنابراین این کانال ارتباطات باید با دقت کنترل شوند، برای مثال با پاکسازی داده‌های دریافت شده. حفاظت در مقابل حملات به دنبال سرقت فیزیکی است که کنترل دسترسی سنتی بر اساس پین و بیومتریک، همراه با سطحی از مقاومت در برابر تهاجم فیزیکی دارد.

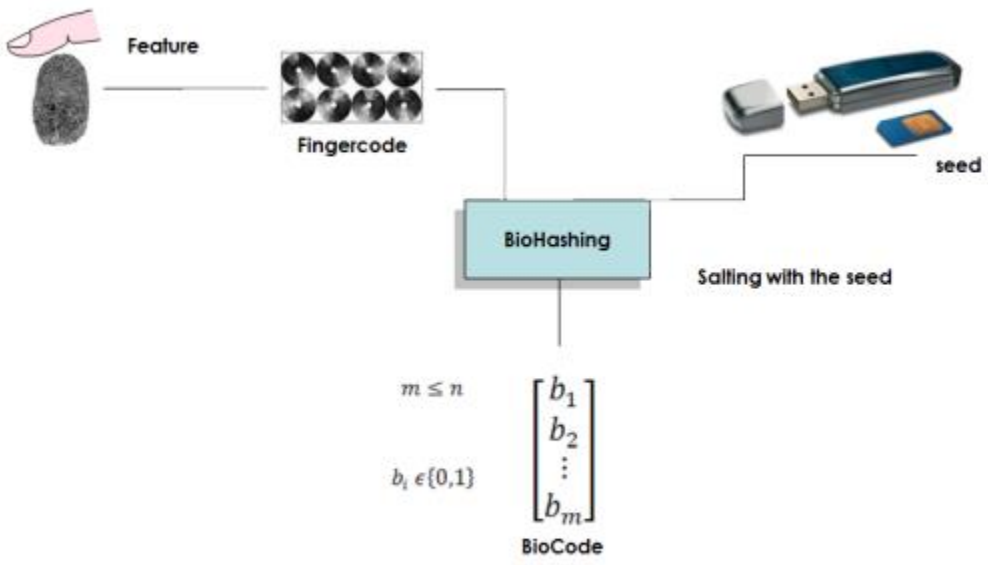

Figure 3. BioHashing scheme

بااین‌حال، لازم نیست که سیستم عامل OffPAD و برنامه‌های کاربردی از آسیب‌پذیری‌هایی که به طور معمول در سیستم‌های آنلاین یافت می‌شود در امان باشند، زیرا فرض می‌شود که مهاجمان قادر به بهره‌برداری از چنین آسیب‌پذیری از OffPAD در اکثر موارد آفلاین هستند. بدین معنا که، باگ‌های خاص نرم‌افزاری که آسیب‌پذیری در یک سیستم آنلاین ایجاد می‌کنند به سختی در مورد آسیب‌پذیری در OffPAD صحبت می‌کنند زیرا نمی‌توانند مورد سوء استفاده قرار گیرند. OffPAD ممکن است دارای چندین رابط برای ارتباطات باشد. میکروفون و دوربین ممکن است برای تشخیص صدا و چهره استفاده شود تشخیصگر اثر انگشت می‌تواند برای تأیید هویت استفاده شود. الزامات آفلاین بودن با ارتباط الکترونیکی با OffPAD همراه نیست، اما به این معنی است که ارتباط فرمت‌ها کنترل شده و در مدت زمان کوتاه است. جدا شدن از شبکه‌ها امنیت دستگاه را بهبود می‌بخشد تا کمتر در مقابل حملات خارجی آسیب‌پذیر باشد.

هرگونه ارتباط الکترونیکی خاص باید به طور معمول قطع شود و فقط باید زمانی وصل شود که نیاز به احراز هویت یا مدیریت برای دستگاه NFC با اتصال USB پشتیبان مناسب برای اتصال OffPAD است. در اولین استفاده، هیچ روش رمزنگاری برای تأیید اتصال بین دستگاه و پلت فرم مشتری وجود ندارد، اعتماد باید به‌سادگی براساس تنظیم مشاهده

شده باشد. در اولین اتصال، نوعی جفت شدن بین دستگاه و کامپیوتر اتفاق می‌افتد، به‌طوری‌که اتصالات بعدی می‌تواند تأیید شوند که بین دستگاه و رایانه مشابه باشند.

ما از این دستگاه امن برای بانکداری آنلاین و پرداخت الکترونیکی به همراه یک پروتکل اصلی با بیومتریک استفاده می‌کنیم. بخش زیر الگوریتم Biohashing مورد استفاده در پروتکل پیشنهاد شده را توضیح می‌دهد. سپس بخش 6 جزئیات این پروتکل اصلی و جدید را بیان می‌کند.

5. الگوریتم Biohashing

الگوریتم BioHashing بردار مقدار واقعی با طول n را (به عنوان مثال FingerCode، حاصل از یک روش استخراج ویژگی) به یک بردار دوتایی به طول $m \leq n$(به عنوان مثال BioCode)، همانطور که توسط Teoh و همکارانش بیان شده است تبدیل می‌کند [25].

این مسئله شامل طرح کردن FingerCode با یک پایه تعریف شده توسط یک seed تصادفی برای تولید BioCode است. تبدیل قالب از الگوریتم زیر استفاده می‌کند، که در آن ورودی‌ها تصادفی هستند و FingerCode F و خروجی BioCode B است:

1) برای $m \leq n \quad i = 1, \ldots, m$ بردارهای شبه تصادفی v_i با طول n تولید می‌شود (از seed تصادفی) و در یک ماتریس شبه تصادفی جمع می‌شوند.

2) الگوریتم Gram-Schmidt بر روی m بردار vi از ماتریس، برای تولید n بردار $V_1, \ldots, V_n$ اعمال می‌شود.

3) برای $m، \quad i = 1, \ldots, m$ ضرب اسکالر $p_i =< F, V_i >$ با استفاده از FingerCode F و m محاسبه می‌شود.

4) در نهایت کد m بیتی (B_0؛...؛ B_m)، با استفاده از فرآیند quantization زیر به دست می‌آید:

$$B_i = \begin{cases} 0 & \text{if} \quad p_i < t \\ 1 & \text{if} \quad p_i \geq t, \end{cases}$$

که در آن t یک آستانه داده شده است که، به طور کلی برابر با 0 است.

هنگامی که برای احراز هویت BioCode مرجع استفاده می‌شود (محاسبه شده از FingerCode پس از ثبت‌نام و پس از نمایش مخفی) با BioCode ثبت شده (محاسبه شده از FingerCode محاسبه شده پس از ثبت جدید) با فاصله همینگ مقایسه می‌شود. اگر این مقدار پایین‌تر از آستانه تعیین شده توسط مدیر سیستم باشد، هویت کاربر تایید شده است. به‌طورکلی، بخش اول الگوریتم، شامل ضرب اسکالر با بردارهای orthonormal است که بنا به الزامات عملکرد و آخرین مرحله از الگوریتم برای الزامات غیرقابل انعطاف از الگوریتم BioHashing استفاده می‌شود. همانطور که قبلا ذکر شد، seed تصادفی خواص تنوع و لغوپذیری را تضمین می‌کند.

پروتکل احراز هویت کاربر چندین بار الگوریتم BioHashing را که در بخش بعدی آن را شرح داده‌ایم به کار می‌برد.

6. پروتکل احراز هویت پیشنهادی

پروتکل احراز هویت پیشنهادی از داده‌های بیومتریک استفاده می‌کند که باید از طریق ثبت با دستگاه OffPAD و الگوریتم حفاظت از الگو محافظت شود. طرح‌های حفاظت از الگو بیومتریک یک گروه از فن‌آوری ها هستند، که شامل فن‌آوری‌های قابل ارتقاء حریم خصوصی هستند و برای ارتقاء حریم خصوصی و امنیت اطلاعات بیومتریک مورد استفاده می‌شوند. از این رو، هر روش حفاظت از قالب باید اجازه لغو داده‌های بیومتریک را بدهد و باید با دقت طراحی شده باشد و تجزیه و تحلیل امنیتی قوی داشته باشد. در میان راه‌حل‌های مختلف در کارهای پیشین، حفاظت از الگو می‌تواند با استفاده از رمزنگاری‌های بیومتریک [15]، [14]، [9]، [20] یا با تبدیل داده‌های ویژگی بیومتریک به دست آید [22]، [5]، [25]، [23]. همانطور که در بخش بعدی بیان شده، BioHashing یک طرح محبوب است که متعلق به رده دوم است و اجازه لغو یک قالب بیومتریک را می‌دهد.

پروتکل پیشنهادی با اثر انگشت دقیق است اما می‌تواند برای هر روش دیگر بیومتریکی (چهره،...) استفاده شود. هنگامی که از بیومتریک استفاده می‌کنیم، دو مرحله اصلی مورد نیاز است: ثبت‌نام و احراز هویت

1) ثبت‌نام: این مرحله برای جمع‌آوری قالب مرجع Alice استفاده می‌شود. در طرح پیشنهادی، قالب داده شده توسط یک BioCode با نام Reference Biocode از یک FingerCode (بردار ویژگی محاسبه شده از اثر انگشت) و

یک رمز (رمز کاربر با شماره سریال دستگاه OffPAD همراه است) شناخته شده است. رمز کاربر می‌تواند یک رمز عبور یا یک مقدار تصادفی ذخیره شده در دستگاه OffPAD باشد (البته، توسط تایید بیومتریک دستگاه محافظت می‌شود). هنگامی که Reference BioCode محاسبه شده است، به بانک صادرکننده Alice از طریق یک کانال SSL فرستاده می‌شود. بنا به به یک دیدگاه سازمانی، این مرحله می‌تواند در یک شاخه پس از بررسی هویت فیزیکی توسط فرد انجام شود. شکل 4 پروسه ثبت‌نام را شرح می‌دهد. هیچ حریم خصوصی برای ذخیره Reference BioCode توسط بانک صادرکننده به‌عنوان این الگو قابل لغو و به‌عنوان فرآیند معکوس BioHashing وجود ندارد.

2) احراز هویت: در طول پرداخت الکترونیکی، بانک صادرکننده باید Alice را تأیید کند (به‌عنوان مثال روند 3D-Secure). یک چالش به Alice فرستاده می‌شود (شماره نمایش داده شده در کامپیوتر یا شماره‌ای که به طور مستقیم به OffPAD فرستاده می‌شود). Alice مجبور است اثر انگشت و رمز عبور خود را (که توسط بانک صادرکننده شناخته شده نیست) ارائه کند. BioCode ثبت شده FingerCode را در داده‌های بیومتریک، رمز عبور و شماره سریال OffPAD محاسبه می‌کند. چالش ثبت Biocode با استفاده از الگوریتم BioHashing در Capture BioCode با چالش ارسال شده توسط بانک صادرکننده به عنوان رمز محاسبه می‌شود. بانک صادرکننده نیز با استفاده از BioHashing، Biocode مرجع را با به چالش کشیدن الگوریتم در BioCode مرجع محاسبه می‌کند. فاصله همینگ برای مقایسه دو چالش BioCodes استفاده می‌شود و اگر فاصله کمتر از آستانه از پیش تعریف شده باشد، Alice تأیید شده است. شکل 5 جزئیات کل روند را توضیح می‌دهد.

3) بحث: چالش ارسال شده توسط بانک صادرکننده اجازه می‌دهد تا یک راه‌حل احراز هویت بیومتریک یک‌باره تعریف کنیم. در این راه‌حل فرض می‌کنیم که OffPAD یک دستگاه امن است. در این راه‌حل، بانک صادرکننده تصمیم‌گیری در مورد احراز هویت Alice را کنترل می‌کند.

7. تجزیه و تحلیل روش پیشنهادی

در این بخش، پروتکل احراز هویت پیشنهاد شده را با توجه به دو جنبه تجزیه و تحلیل می‌کنیم: تجزیه و تحلیل عملکرد (با توجه به اشتباهات بیومتریک) و مسائل امنیت و حریم خصوصی

A. تجزیه و تحلیل عملکرد

در این بخش، عملکرد پروتکل را برای جلوگیری از رد اشتباه و نادرست تجزیه و تحلیل می‌کنیم. با تعریف تجربی پروتکل شروع می‌کنیم.

1) پروتکل تجربی: در این مطالعه، از سه پایگاه داده اثر انگشت استفاده شده است که، هر کدام از 800 عکس از 100 نفر با 8 نمونه از هر کاربر تشکیل شده است:

• پایگاه داده معیار FVC2002 DB2: وضوح تصویر 296 × 560 پیکسل با حسگر نوری "FX2000" توسط Biometrika؛

• پایگاه داده معیار FVC2004 DB1: وضوح تصویر 640 × 480 پیکسل با سنسور نوری "V300" توسط CrossMatch؛

• پایگاه داده معیار FVC2004 DB3: وضوح تصویر 300 تا 480 پیکسل با سنسور حرارتی فراخوانی است "FingerChip FCD4B14CB" توسط Atmel.

شکل 6 یک تصویر از هر پایگاه داده ارائه می‌دهد. ما می‌توانیم ببینیم که اثرانگشت‌ها کاملا متفاوت و نمایشی از انواع مختلف اثرانگشت (به دست آمده از سنسورها با استفاده از فن‌آوری‌های مختلف) است.

این پایگاه داده‌ها برای مسابقات (رقابت برای تایید اثر انگشت) در سال های 2002 و 2004 استفاده شده است. جدول 1 عملکرد بهترین الگوریتم‌ها بر روی این پایگاه داده‌ها را نشان می‌دهد. نرخ خطای برابر (EER) نرخ خطای سازش را زمانی که کاربران واقعی به اشتباه رد می‌شوند و فریبکارانه پذیرفته می‌شوند محاسبه می‌کند.

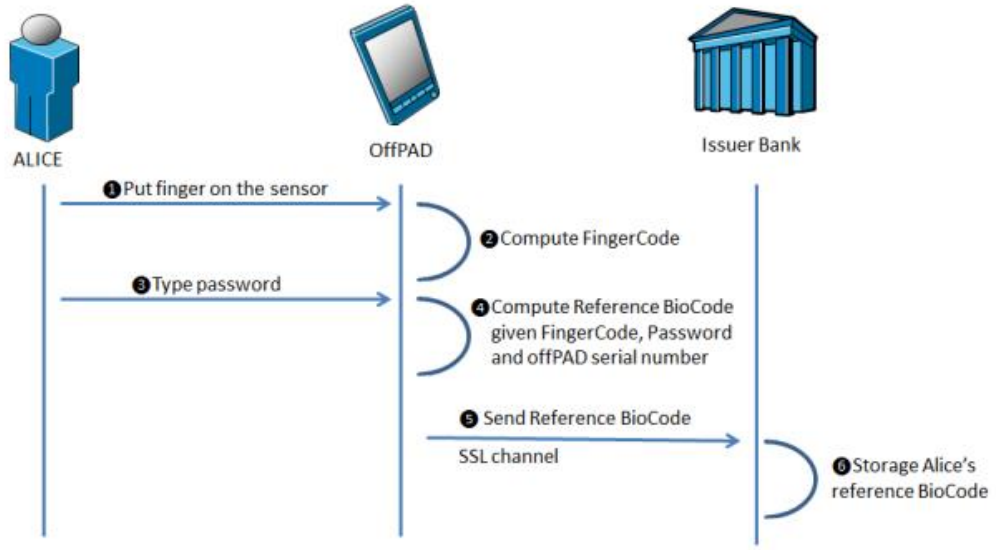

Figure 4. Enrollment step

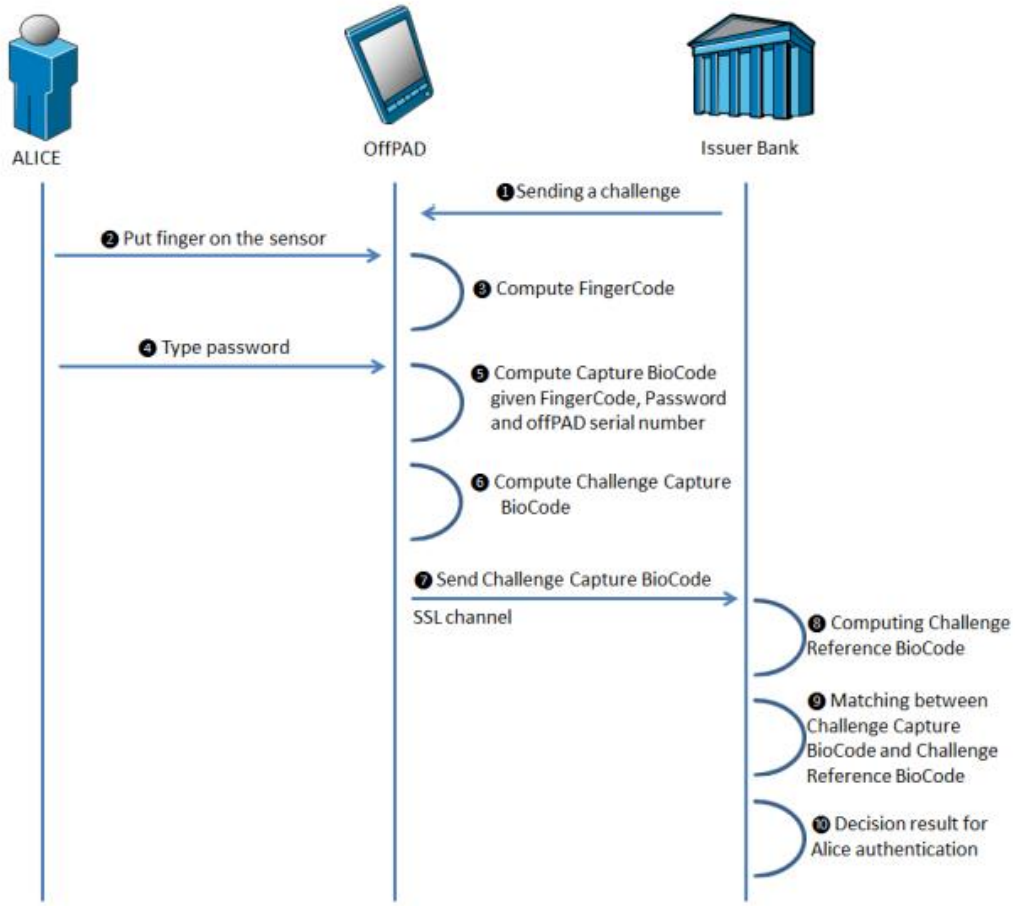

Figure 5. Authentication step

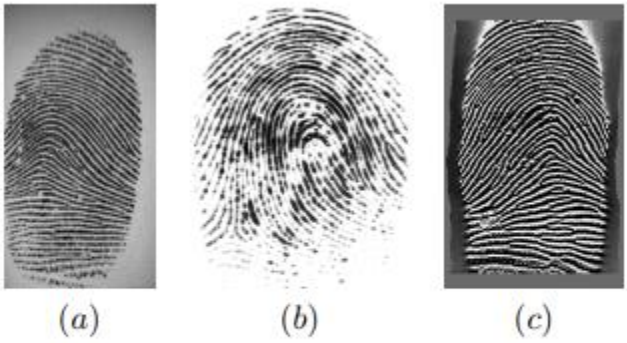

Figure 6. One fingerprint example from each database: (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3

ZeroFRM مقدار False Non Match Rate (FNMR) است هنگامی‌که هیچ موردی به‌صورت اشتباه پذیرفته نشده باشد. این مقادیر پیچیدگی هر پایگاه‌داده و برخی از عناصر عملکردی که می‌توانیم در این پایگاه‌داده‌ها انتظار داشته باشیم تعریف می‌کند.

Databases	*EER*	*ZeroFMR*
FVC2002 DB2	0.14%	0.29%
FVC2004 DB1	0.61%	1.93%
FVC2004 DB3	1.18%	4.89%

Table I
PERFORMANCE OF THE BEST ALGORITHM FOR EACH DATABASE (SEE HTTP://BIAS.CSR.UNIBO.IT/FVC2002)

همانند FingerCode، از ویژگی‌های گابور (GABOR) [18] با اندازه n = 512 (16 مقیاس و 16 جهت) به‌عنوان الگو استفاده می‌کنیم. این ویژگی‌ها به خوبی شناخته شده هستند و اجازه می‌دهند تا تجزیه و تحلیل بافت یک اثر انگشت به خوبی انجام شود. برای هر کاربر از اولین نمونه FingerCode به‌عنوان قالب مرجع استفاده کردیم. اثرانگشت‌های دیگر برای تست طرح پیشنهاد شده استفاده می‌شوند. BioCodes به اندازه 256 بیت است. برای ارزیابی عملکرد روش بیومتریک یک‌باره، 1000 مقایسه را (با فاصله هامینگ) بین چالش BioCode مرجع و چالش ثبت BioCode برای هر کاربر محاسبه کردیم. 100.000 امتیاز بین کلاسی و درون کلاسی را برای تجزیه و تحلیل عملکرد طرح پیشنهادی به دست آوردیم.

2) نتایج تجربی: ما پروتکل قبلی را به راه‌حل پیشنهادی اعمال کردیم. در سه پایگاه‌داده، مقدار EER نزدیک به 0٪ رسید. که به منظور نشان دادن این کارایی، که در شکل 7 توزیع امتیازات درون کلاسی و بین کلاسی برای هر پایگاه داده نشان داده شده است. ما به وضوح می‌بینیم که هیچ همپوشانی بین آن دو توزیع و آستانه در نزدیکی 60 (بدین معنی که حداکثر 60 بیت متفاوت بین ثبت و مرجع BioCodes تحمل می‌شود) وجود ندارد و می‌تواند مورد استفاده قرار گیرد. در ستون آخر از جدول 2، ارزیابی مقدار EER را با در اختیار داشتن دستگاه OffPAD و رمز عبور کاربر (بدترین حالت) ارائه می‌دهیم. در این مورد، فریبکار می‌تواند با ارائه بیومتریک خود، تلاش کنید داده‌ها برای جعل هویت کاربر واقعی به کار ببرد. ما 100.000 حمله را برای هر پایگاه داده آزمایش کردیم و این حمله در 16٪ تا 25٪ موارد موفقیت آمیز بود. در رویکردهای کلاسیک (تأیید اعتبار با دو عامل)، این حمله همیشه موفق است.

Database	*EERwithoutattack*	*EERwithattack*
*FVC*2002 *DB*2	0%	25.85%
*FVC*2004 *DB*1	0.00093%	23.95%
*FVC*2004 *DB*3	0.00023%	16.12%

Table II
PERFORMANCE OF THE PROPOSED ALGORITHM FOR EACH DATABASE

B. تجزیه و تحلیل امنیت و حریم خصوصی

پروتکل پیشنهاد شده احترام بیشتری برای حریم خصوصی کاربران نسبت به پروتکل D-Secure3 قائل است. یک تجزیه و تحلیل از پروتکل پیشنهادی در این بخش پیشنهاد می‌کنیم.

1) امنیت داده‌ها و احراز هویت: کانال امن بین عوامل و طرح‌های رمزنگاری از محرمانه بودن اطلاعات مبادله شده و یکپارچگی داده‌ها در طول پروتکل اطمینان دارد. در نتیجه، الزامات R1 و R2 مورد اطمینان دارند. احراز هویت افراد نیز از طریق SSL برای SP (R6) و بانک‌ها (R7) تحقق یافته است، درحالی‌که تأیید هویت کاربر (R3) به واسطه قدرت قوی به دست آمده از تأیید اعتبار و از طریق الگوریتم Biohashing است. علاوه براین، با تشکر از چالش‌ها در هنگام تایید هویت کاربر، این احراز هویت یک تایید بیومتریک یک‌باره است. در نتیجه، تراکنش‌های مختلف یک کاربر را نمی‌توان پیوند داد. الزام R8 نیز تضمین شده است. این دستگاه توسط شماره سریال خود و مدرک مالکیت دستگاه

کاربر که ارائه شده است تأیید شده است، در نتیجه الزامات R4 و R5 تضمین شده هستند. علاوه براین، برای راه‌حل احراز هویت کاربر، کاربر تنها نیاز به تولید آنچه که او دارد (داده‌های بیومتریک) و آنچه شناخته شده است (رمز عبور) دارد.

2) تجزیه و تحلیل خصوصی: در طول فرآیند تأیید هویت ما، چندین آیتم اطلاعات حساس مانند داده‌های بیومتریک و رمز عبور مبادله و ذخیره می‌شوند. ذخیره‌سازی آنها نباید متمرکز باشد. با این حال، به لطف استفاده از الگوریتم BioHashing، قابل لغو می‌باشد. بدین ترتیب، دانش BioCode در مورد اطلاعات شخصی کاربر هیچ چیزی در دست ندارد. در مورد ما، دانش BioCode مرجع با دانش داده‌های بیومتریک مانند اثر انگشت همراه نیست. فقط داده‌های مرتبط و ضروری ارسال و ذخیره می‌شوند. بنابراین اصل کمینه‌سازی (R9) نیز مورد احترام است. علاوه براین، برای احراز هویت هر کاربر، کاربر باید اثر انگشت خود را ارائه دهد و رمز عبور خود را تحویل بگیرد. این اقدامات باعث می‌شود تا کاربر رضایت خود را برای استفاده از این اطلاعات که می‌تواند به لطف محاسبات Capture کنترل شود بیان کند. اصل حاکمیت داده (R10) مورد احترام است.

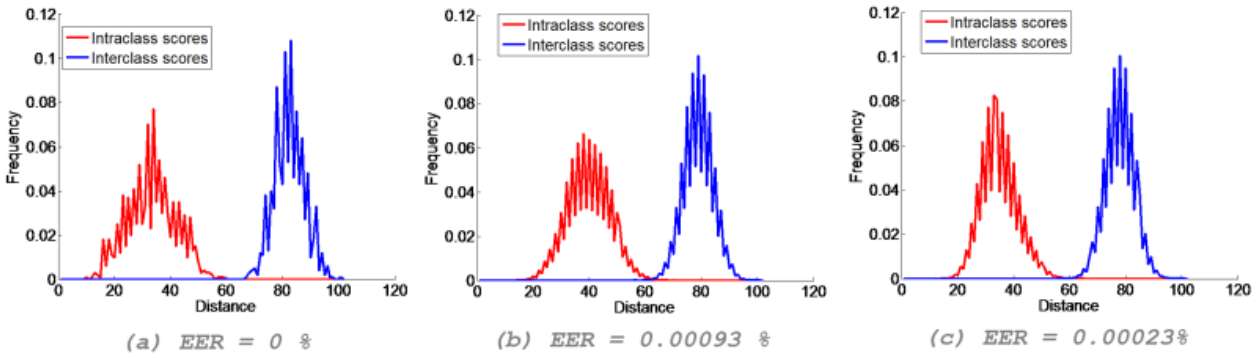

Figure 7. Distribution of intraclass and interclass scores for each database: (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3

8. نتیجه‌گیری و چشم‌اندازهای آینده

راه حل پیشنهادی از یک دستگاه اضافی، که دارای هزینه ناچیزی است استفاده می‌کند. با این وجود، ریسک مالی برای بانکداری و یا پرداخت مهم است و به شدت افزایش می‌یابد. در نتیجه، این دستگاه اضافی برای یک دنیای واقعی

مسئله‌ای نمی‌باشد. در این مقاله، یک پروتکل احراز هویت جدید "One Time Biometrics" برای بانکداری آنلاین و احراز هویت پرداخت الکترونیکی ارائه شده است. پروتکل شامل دو جزء اصلی است. اولین جزء یک دستگاه خاص به نام OffPAD است که بسیاری از مسائل امنیتی و حفظ حریم خصوصی را تضمین می‌کند. مولفه دوم استفاده از یک الگوریتم حفاظت از قالب بیومتریک برای ذخیره متمرکز داده‌های بیومتریک توسط بانک صادرکننده است. سپس یک پروتکل مبتنی بر چالش برای جلوگیری از حملات مجدد پیشنهاد شده است. طرح احراز هویت کاربر برای کاربران قابل استفاده است زیرا آنها مجبور هستند گذرواژه‌های مختلف را به یاد داشته باشند. پروتکل عملکرد بسیار خوبی در سه پایگاه داده اثر انگشت با توجه به مسائل امنیتی و حفظ حریم خصوصی از خود نشان داده است.

دیدگاه‌های آینده در مورد این مطالعه بسیار زیاد است. ما برنامه‌ریزی می‌کنیم تا از داده‌های بیومتریک چندگانه به منظور اجتناب از استفاده یک رمز عبور در پروتکل پیشنهادی استفاده کنیم و همچنین قصد داریم یک پروتکل معتبر برای داده‌های بیومتریک طراحی کنیم.

9. تقدیر و تشکر

نویسندگان می‌خواهند از برنامه یورواستار برای کمک به این پروژه و همچنین برای حمایت مالی تشکر کنند.

http://www.eurostars-eureka.eu

REFERENCES

[1] Visa corporate, 1958. http://corporate.visa.com/index.shtml.

[2] Mastercard worldwide, 1966. http://www.mastercard.com/.

[3] Manal Adham, Amir Azodi, Yvo Desmedt, and Ioannis Karaolis. How to attack two-factor authentication internet banking. In Financial Cryptography, 2013.

[4] G. Antoniou and L. Batten. E-commerce: protecting purchaser privacy to enforce trust. Electronic commerce research, 11(4):421–456, 2011.

[5] R.M. Bolle, J.H. Connell, and N.K. Ratha. Biometric perils and patches. Pattern Recognition, 35(12):2727–2738, 2002.

[6] European Commission. Directive 2000/31/ec of the european parliament and of the council of 8 june 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (’directive on electronic commerce’), 2000.

[7] European Commission. Directive 2007/64/ec of the european parliament and of the council of 13 november 2007 on payment services in the internal market amending directives 97/7/ec, 2002/65/ec, 2005/60/ec and 2006/48/ec and repealing directive 97/5/ec, 2007.

[8] European Payments Council. Sepa - single euro payment area, 2007. http://www.sepafrance.fr/.

[9] J. Daugman. New methods in iris recognition. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, 37(5):1167–1175, October 2007.

[10] S. Drimer, S. Murdoch, and R. Anderson R. Optimised to fail: Card readers for online banking. Financial Cryptography and Data Security, pages 184–200, 2009.

[11] Y. Espelid, L.H. Netland, A. Klingsheim, and K. Hole. A proof of concept attack against norwegian internet banking systems. Financial Cryptography and Data Security, pages 197–201, 2008.

[12] MasterCard International. Chip authentication program functional architecture, September, 2004.

[13] Audun Jøsang and Simon Pope. User centric identity management. In AusCERT Asia Pacific Information Technology Security Conference, page 77. Citeseer, 2005.

[14] A. Juels and M. Sudan. A fuzzy vault scheme. In ISIT, page 408, 2002.

[15] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In ACM Conference on Computer and Communications Security, pages 28–36, 1999.

[16] Henning Klevjer, Kent Are Varmedal, and Audun Jøsang. Extended http digest access authentication. In Policies and Research in Identity Management, pages 83–96. Springer, 2013.

[17] Shujun Li, Ahmad-Reza Sadeghi, Soeren Heisrath, Roland Schmitz, and Junaid Jameel Ahmad. hPIN/hTAN: A lightweight and low-cost e-banking solution against untrusted computers. In Financial Cryptography, 2011.

[18] B. S. Manjunath and W.Y. Ma. Texture features for browsing and retrieval of image data. IEEE Transactions on Pattern Analysis and Machine Intelligence, 18:37–42, 1996.

[19] S. Murdoch and R. Anderson. Verified by visa and mastercard securecode: or, how not to design authentication. Financial Cryptography and Data Security, pages 336–342, 2010.

[20] M. Osadchy, B. Pinkas, A. Jarrous, and B. Moskovich. Scifi - a system for secure face identification. In IEEE Symposium on Security and Privacy, 2010.

[21] V. Pasupathinathan, J. Pieprzyk, H. Wang, and J.Y. Cho. Formal analysis of card-based payment systems in mobile devices. In Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54, pages 213– 220. Australian Computer Society, Inc., 2006.

[22] N.K. Ratha, J.H. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication system. IBM Systems J., 37(11):2245–2255, 2001

. [23] C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. on Information Security, 3, 2011.

[24] S.E.T. Secure electronic transaction specification. Book 1: Business Description. Version, 1, 2002.

[25] A.B.J. Teoh, D. Ngo, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 40, 2004.

[26] Kent Are Varmedal, Henning Klevjer, Joakim Hovlandsvag, ˚ Audun Jøsang, Johann Vincent, and Laurent Miralabe. The ´ offpad: Requirements and usage. In Network and System Security, pages 80–93. Springer, 2013.

[27] Visa. 3D secure protocol specification, core functions, July 16, 2002.