کنفرانس بین المللی تکنولوژی های پیشرفته محاسبه و کاربردهای آنها(ICACTA-2015)

امنیت افزایش یافته برای ماشین های ATM با امکانات OTP و تشخیص صورت

محسن کارووالیا، سیف علی کاردیا، شراد عزا، دکتر د.ر.کالبند

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی سردار پتل، بمبئی *400058* ، هند

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی سردار پتل، بمبئی *400058* ، هند

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی سردار پتل، بمبئی *400058* ، هند

استاد تمام، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی سردار پتل، بمبئی *400058* ، هند

چکیده

هدف این مقاله افزایش امنیت مدل های ATM معمولی است. ما یک مفهوم جدید را فرض کرده ایم که تجربه کلی، قابلیت استفاده و راحتی تراکنش را در ATM بهسازی می کند. امکاناتی مانند تشخیص چهره و رمز عبور یک بار مصرف (OTP) برای افزایش امنیت حسابها و حریم خصوصی کاربر استفاده شده است. تکنولوژی تشخیص چهره در تشخیص هر و همه ی کاربران به صورت یکتا به ماشین کمک می کند و بنابراین چهره را به یک کلید تبدیل می کند. این باعث حذف احتمال کلاهبرداری به دلیل سرقت و کپی از کارت های ATM می شود. علاوه بر این OTP تولید شده ی تصادفی کاربران را از یادآوری PIN ها راحت می کند زیرا خود به عنوان یک PIN عمل می کند.

کلیدواژه ها: PCA، OTP، eigenface، ATM، امنیت، کلاهبرداری، تشخیص صورت

1. معرفی

به دلیل توسعه سریع در علم و تکنولوژی، نوآوری های آینده بر اساس امنیت قدرتمند ساخته می شوند. اما از طرف دیگر، تهدیداتی هم برای تخریب این سطح امنیت خودنمایی می کنند. بنابراین بهسازی ها در اتوماسیون یک تاثیر کلی مثبت داشته است، اما موسسات مالی متعددی مانند بانکها و کابری هایی مانند ATM هنوز هم در معرض دزدی و کلاهبرداری قرار دارند. مدل های ATM موجود از یک کارت و یک پین استفاده می کنند که باعث افزایش حملات به صورت کارت های دزدیده شده ،یا پین های تخصیص داده شده ی ثابت، کپی کردن کارت و تهدیدات فراوان دیگر شده است. برای غلبه بر آن، مدل های مرکبی که شامل امکانات عادی همراه با امکانات اضافی مانند تشخیص صورت و رمز عبور یک بار مصرف(OTP) هستند استفاده می شود. پایگاه داده ها اطلاعات در مورد جزییات حساب یک کاربر، تصویر هایی از صورت او و یک شماره موبایل را نگهداری می کنند که امنیت را به مقدار زیادی افزایش می دهد.

در ابتدا کاربر کارت را می کشد. یک تصویر زنده به صورت اتوماتیک از طریق یک وب کم نصب شده بر ATM گرفته می شود، که با عکس ذخیره شده در پایگاه داده مقایسه می شود. اگر منطبق باشد، یک رمز عبور یک بار مصرف(OTP) به شماره موبایل ثبت شده ی منطبق فرستاده می شود. این کد ایجاد شده ی تصادفی باید در تکست باکس توسط کاربر وارد شود. اگر کاربر OTP را به درستی وارد کرد، تراکنش می تواند ادامه پیدا کند. بنابراین ترکیب الگوریتم تشخیص صورت و یک OTP به مقدار زیاد احتمال کلاهبرداری را کاهش می دهد به علاوه کاربر را از بار اضافی حفظ کردن رمز عبور های پیچیده رها می کند.

1. هدف و منافع استفاده از تشخیص صورت و OTP در ATM

تشخیص صورت کاربردش را در زمینه های متعددی مانند امنیت ملی، تشخیص مجرمین، تراکنش انسان-کامپیوتر، امنیت حریم خصوصی و غیره سافته است. امکانات تشخیص صورت دسترسی به حساب را از کارت های دزدیده شده یا جعلی منع می کند. کارت به تنهایی برای دسترسی به حساب کافی نیست زیرا به خود فرد نیز برای ادامه ی تراکنش نیاز است. روش eigenface پایه برای تشخیص صورت استفاده می شود. هرچند مشکل استفاده از روش eigenface پایه این است که می تواند توسط ماسک های تقلبی یا عکسهایی از صاحب حساب فریب داده شود. برای غلبه بر این مشکل روش های تشخیص صورت سه بعدی می تواند مورد استفاده قرار گیرد. هر چند هزینه محاسباتی آن بالاست و نیاز به فضای ذخیره بسیاری دارد که ذخیره اطلاعات در مورد تعداد زیادی از کابران را مشکل می کند و ماسک های سه بعدی می توانند برای فریب مدل تشخیص صورت سه بعدی پایه استفاده شوند. چاپ سه بعدی برای این حملات معمولا مورد استفاده قرار می گیرد. این مشکلات می توانند به راحتی با استفاده از رمزعبور یک بار مصرف کنار روند. OTP تضمین می کند که کاربر با فرستادن کد 6 رقمی ایجاد شده ی تصادفی به شماره موبایل ثبت شده ی صاحب حساب منطبق تایید اعتبار می شود. به علاوه کاربر مجبور نیست که پین را حفظ کند. این باعث چلوگیری از حملات کلاهبردارانه مانند:

2.1 استراق سمع

کارت ATM یا پین یک کاربر می تواند مورد جاسوسی قرار گیرد و می تواند به آسانی با به دست آوردن کارت با روش های خلاف مورد دستیابی قرار گیرد. این باعث نتایج بسیار جدی می شود.

2.2 فریب

این احتمال وجود دارد که هنگامی که کاربر پین را در طول یک فرایند تراکنش وارد می کند، یک هکر به عنوان یک سایت مجاز خود را جا بزند و از کاربر بخواهد که به دلیل اشکال سیستم پین را دوباره وارد کندو هنگامی که کاربر کار خود را با تراکنش پایان داد هکر داده را ذخیره می کند و برای نیات شوم آینده خود از آن استفاده کند. این حمله man-in-the-middle (فرد میانی = هکر) به دلیل تخصیص موقت رمز عبور برای هر تراکنش جدید ملغی می شود.

2.3 حمله *Brute-force*

استفاده از brute force، اگر بخواهیم که پین ثابت کنونی 4 رقمی را بشکنیم در 9999 تلاش انجام می شود، بنابراین امنیت را تضعیف می کند. در مدل ما یک کد 6 رقمی به یک شماره ثبت شده فرستاده می شود، بنابراین امنیت را افزایش می دهد و احتمال شکستن کد با استفاده از brute force را کاهش می دهد.

1. مقایسه ی بیومتریک
2. جدول 1 : مقایسه ی تکنولوژی های بیومتریک

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| شاخصه بیومتریک | هزینه | دقت | کارایی | اشکالات | پایداری |
| عنبیه | بالا | بالا | بالا | نوردهی | بالا |
| شبکیه | بالا | بالا | بالا | عینک | بالا |
| صورت | متوسط | متوسط | متوسط | ریش، عینک، سن | متوسط |
| اثرانگشت | پایین | متوسط | متوسط | کثیفی، خشکی | بالا |

تشخیص و شناسایی صورت

در این مرحله یک کاربر صرفا نیازمند نگاه کردن به دوربین نصب شده بر روی ATM است. اگر کاربر شناخته شد، سپس OTP به شماره موبایل کاربر فرستاده می شود. ما سرقت هایی را در ATM دیده ایم مانند هنگامی که مجرم وارد اتاق می شود و کاربر را مجبور به دستری به حسابش می کندو برای غلبه بر این مشکل ما یک راه حل ساده یافتیم: اگر بیشتر از یک صورت توسط ماشین تشخیص داده شد در آن صورت حساب به صورت موقت قفل می شود. این امکانات اضافی ساده ولی موثر است. بنابراین سیستم تضمین می کند که تراکنش تنها در صورتی ادامه پیدا می کند که کاربر به تنهایی با ماشین کار می کند.

در کل، تکنیک تشخیص صورت می تواند به دو گروه بر اساس نمایش صورتی که استفاده می کنند تقسیم شود:

1. بر اساس ظاهر

این روش از خواص جامع بافت استفاده می کند و یا به کل صورت یا فقط به بخش های خاصی از عکس آن اعمال می شود. تحلیل بخش اصلی(PCA)، تحلیل بخش مستقل(ICA) و تحلیل گسسته خطی(LDA) تحت این گروه قرار می گیرند.

1. بر اساس مشخصات

این روش از خواص هندسی صورت استفاده می کند(دهان، چشم،بینی و...) و ارتباط هندسی مابین آن ها.

مدل ما از تحلیل بخش اصلی استفاده می کند. برای ساخت eigenface، اطلاعات خوبی برای انطباق بخش ها لازم است. eigenface ها از بزرگترین به کوچترین مرتب می شوند، در حالی که eigenface ای که بزرگترین مقدار ویژه را دارد اختلاف بیشتری را در مقایسه با آن هایی که مقدار ویژه کمتری دارند تجربه می کند. از این مجموعه از eigenface ها تنها K تای اول آن ها انتحاب می شوند که نشان دهنده ی بیشتر خواص یکتا هستند. یک برتری PCA بر بقیه روش ها این است که 90% تنوع کل در 5-10 درصد ابعاد قرار می گیرند.

4.1 هدف استفاده از PCA

1. زمان صرف شده برای محاسبه بسیار کمتر است زیرا تنها بخش های اساسی از عکس ها را در نظر می گیرد
2. بر اساس چندین عکس صورت به عنوان ورودی انجام می شود به این معنی که چندین عکس ورودی از هر فرد را با ظواهر متفاوت و تحت شرایط نوری متفاوت در نظر می گیرد.
3. برای ذخیره دیتاست به فضای ذخیره کمتری نیازمند است
4. نمایش پایگاه داده کوچکتر زیرا فقط عکس های آموزش داده شده به صورت نمایششان در یک پایه کاهش یافته ذخیره می شود.
5. ابعاد کاهش یافته کارایی فرایند را افزایش می دهد.

4.2 کارکد تکنیک تشخیص صورت

4.2.1 ایجاد eigenface ها

این فرایند تنها توسط افراد مورد اعتماد در بانک انجام می شود. هنگامی که یک مشتری حسابی را ایجاد می کند او باید عکس هایی را ارایه دهد. این می تواند با گرفتن عکس های او توسط وبکم در بانک انجام شود. حسابدار تعدادی عکس می گیرد و آنها را در پایگاه داده که برچسبی با عنوان شماره حساب مرتبط با هرکدام از آنها دارد ذخیره می کند.

برای آموزش عکس ها در پایگاه داده، هر عکس در یک مجموعه داده به گونه ای تغییر اندازه داده می شود که هر کدام از آنها ابعاد مشخص داشته باشند برای مثال N×N. هر عکس به فرم بردار صورت تبدیل می شود. بردارهای صورت ابعادی به اندازه N2×1 دارند. هر بردار صورت نرمال سازی می شود به این معنی که خواص مشترک از تمام بردارهای صورت حذف می شود. این با محاسبه ی صورت متوسص که شامل خواصی از تمام بردارهای صورت است و تفریق آن از هر یک از بردارهای صورت انجام می شود. ماتریس A شکل می یابد که شامل این بردارهای صورت است و به است شکل نمایش داده می شود:

A = [ф1, ф2, ф3,..., фM] و ابعاد N2×M دارد.

به صورتی که

Фk - بردار صورت گرفته شده پس از تفریق صورت متوسط

M – تعداد کل بردارهای صورت استفاده شده برای آموزش

Eigenfaceها از ماتریس کوواریانس با تکنیک کاهش ابعادی محاسبه می شوند(به صورتی که eigenface ها با ماتریس کوواریانس با ابعاد کاهش یافته محاسبه می شوند) به گونه ای که در فرمول داده شده است:

C = ATA

این ابعاد M×M دارد. بنابراین M تا eigenface، هر کدام با اندازه M با ضرب ساده ماتریس محاسبه می شود. از این M تا eigenface فقط K تا از آنها (بخش اصلی) با الگوریتم ابتکاری انتخاب می شود(با هوش مصنوعی) که شامل یکتاترین و حیاتی ترین اطلاعات هستند و بقیه را که شامل اطلاعات تکراری یا نویز دار هستند بدون از دست دادن اطلاعات ارزشمند حذف می کند. eigenface های اولیه از این K تا eigenface با پیش ضرب ماتریس A با هر یک از K تا eigenface محاسبه می شود. این روش زمان محاسبه و نویز را از عکس های ورودی می گیرد. این eigenface به شکل دهی عکس ها در مجموعه داده کمک می کنند. عکس اصلی با ضرب وزنها (w1, w2, w3...) با eigenface منطبق و جمع آنها محاسبه می شود، سپس صورت متوسط به آن اضافه می شود که قبلا کم شده بود. بنابراین هر عکس در یک مجموعه داده با یک بردار وزن Ω که نمایش eigenface از i امین صورت است نمایش داده می شود.

4.2.2 تشخیص eigenface

هنگامی که کارت کشیده شد، این فرایند اتفاق می افتد:

1. عکسی را از طریق وب کم بگیر و صورت را در آن تشخیص بده. اگر بیشتر از یک صورت در عکس بود، به صورت موقت دسترسی به حساب را به دلایل امنیت و حفظ حریم شخصی ببند. اگر فقط یک صورت بود آنگاه به فرایند را ادامه بده(مرحله 2)
2. صورت را به اندازه استاندارد N×N تغییر اندازه بده
3. صورت ورودی را به بردار صورت تبدیل کن
4. بردار صورت را نرمال سازی کن
5. بردار صورت نرمال شده را به فضای ویژخ منعکس کن
6. بردار وزن عکس ورودی را محاسبه کن
7. فاصله میان بردار وزن ورودی و تمام بردارهای مجموعه آموزشی را محاسبه کن
8. اگر فاصله کمتر از مقدار آستانه باشد، فرد تشخیص داده شده و تراکنش می تواند ادامه پیدا کند یا در غیر این صورت تراکنش نمی تواند ادامه داشته باشد.
9. کارکرد OTP

برای پیاده سازی OTP، ما از مودم GSM برای فرستادن پیامک(یک رمز یک بار مصرف) به شماره موبایل کاربر استفاده می کنیم. ایده استفاده از شماره موبایل بر ایمیل ترجیح دارد زیرا مردم در مناطق روستایی تلفن های ساده ای دارند که می تواند پیامک دریافت کند اما ارتباط اینترنتی و امکانات ایمیل ندارد. به دلیل اینکه موبایل ها همه جا حاضر هستند، ما تصمیم گرفتیم که از موبایل استفاده کنیم که همه مردم بتوانند از منافع سیستم پیشنهاد شده ی جدید استفاده کنند. کاربر OTP را فورا بعد از گذراندن تست تشخیص صورت دریافت می کند. هنگامی که OTP دریافت شد کاربر باید کدی را که 6 رقمی است وارد کند. کاربر 3 بار فرصت برای وارد کردن کد دارد. اگر کد در 3 تلاش پشت سر هم نادرست وارد شود حساب به صورت موقت بسته شده و پیغام اطلاع رسانی برای شماره موبایل ثبت شده فرستاده می شود. این قابلیت با هدف محدود کردن روش های کلاهبردارانه حمله به حساب یک کاربر با پوشیدن ماسک و یا در حالات نادر، اگر صورت کاربر غیر مجاز اشتباها با صورت کاربر مجاز تطبیق یابد است.

5.1) تولید عدد تصادفی

ساخت دنباله ای از اعداد شبه تصادفی(Yn):

Y n+1 􀵌 ( a 􀵈 Y n + C ) mod (m) (2)

انتخاب a(چندبرابر کننده)، C(افزایش) و m(پیمانه) مهم هستند زیرا اعداد تصادفی ایجاد شده اگر به خوبی کنترل نشوند در دنباله هستند.

5.2 فرمول تولید اعداد تصادفی پیشنهاد شده

مشکل تولید کننده عدد تصادفی بالا این است که دنباله تعداد محدودی عدد صحیح دارد و دنباله در یک بازه زمانی تکرار می شود. بنابراین ما فرمول را با کاربرد فرمول تولید کننده عدد تصادفی یکسان به C تغییر می دهیم و این مقدار در افزایش تولید کننده عدد تصادفی جایگزین می شود. بنابراین فرمول تولیدکننده عدد تصادفی این است:

C 􀀃􀀃􀵌 ( b 􀵈􀀃X n + d ) mod (m)

X n+1􀀃􀀃􀀃􀵌 C

Y n+1 􀵌 ( a 􀵈􀀃Y n + C ) mod (m) (3)

عدد تصادفی(Y n+1) ایجاد شده OTP خواهد بود. ارزش m باید یک عدد اول بزرگ باشد تا اعداد بی ارتباط را جداکند. بنابراین سربار محاسباتی افزایش می یابد اما تکرار دنباله کاملا حذف می شود.

5.3) تابع درهم سازی رمزنگاری

چندین تابع رمزنگاری درهم سازی برای بهسازی درجه امنیت استفاده می شود. ما MD5 را برگزیده ایم که به عنوان هضم پیغام شناخته می شود زیرا تابع درهم سازی بسیار پرکاربردی است. به دلیل اینکه سریعترین تابع درهم سازی رمزنگاری است استفاده از MD5 مناسب است و در تعداد زیادی از پلتفرم ها پذیرفته شده است.

5.4 قدم ها

1. یک OTP 6 بیت با استفاده از تکنیک تولید عدد تصادفی تولید می شود.
2. این OTP تولید شده به شماره موبایل کاربر فرستاده می شود.
3. این OTP تحت فرایند درهم سازی MD5 می رود و بنابراین به صورت رمز شده در می آید و به صورت موقتی در پایگاه داده ای که بعد از یک دقیقه پاک می شود ذخیره می شود.
4. کاربر باید OTP را در یک دقیقه وارد کند
5. OTP وارد شده توسط کاربر دوباره تحت تکنیک درهم سازش مشابهی می رود و با مقدار OTP ذخیره شده به صورت موقت در پایگاه داده مقایسه می شود.
6. اگر منطبق باشد آنگاه تراکنش می تواند ادامه یابد
7. مراحل 1تا5 برای هر تراکنش جدید تکرار می شود

مدل چگونه از دزدی جلوگیری می کند

وابستگی خطی سیستم پیشنهاد شده ی ما در سه فاز نیازمندی کارت، تشخیص صورت و OTP یک نقش حیاتی را در جلوگیری از سرقت به شکل زیر بازی می کند:

1. اگر یک سارق یک کارت جعلی را برای دسترسی به یک حساب بسازد، صورت دزد با صورت صاحب حساب منطبق نیست.
2. در حالات نادر، اگر دزد بخواهد با استفاده از ماسک صورتش با صاحب حساب منطبق شود، در آن صورت OTP به شماره ثبت شده ی کاربرد فرستاده می شود که از طرفی به کاربر هشدار می دهد که فردی برای دسترسی به حساب تلاش می کند
3. فرض کنیم که موبایل یک کاربر دزدیده شود، کاربر می تواند شماره موبایل را با ارتباط با اپراتور غیر فعال کند که باعث جلوگیری از رسیدن OTP به موبایل دزدیده شده می شود که از دسترسی غیرمجاز به حساب جلوگیری می کند.

برای شکستن این 3 فاز، یک دزد باید کارت را جعل/دزدی کند، سپس باید صورت کاربر را جعل کند و گوشی کاربر را بدزدد. بنابراین عبور از این سیستم تنها در صورتی ممکن است که کاربر در گزارش دزدی/تعویض گوشی یا دزدی/تعویض ATM کارت برای غیرفعال کردن حساب بی توجهی کند.

🡪 OTP تشخیص صورت 🡪 کشیدن کارت

شکل1. جریان کار مدل

فلوچارت



شروع

کشیدن کارت

مرحله تشخیص صورت

حساب موقتا بسته می شود

بیشتر از یک صورت؟

تشخیص صورت بر اساس پی سی ای

پایان

تشخیص داده شد؟

رمز به شماره ثبت شده فرستاده می شود

فشردن دکمه ارسال مجدد

رمز دریافت شد؟

وارد کردن رمز



I=o را برای ذخیره کردن تعداد ورود ها ایجاد می کند

I<3

حساب به صورت موقت بسته می شود و کاربر خبردار می شود

دوباره وارد کنید، i++

رمز تطبیق داده شد

تراکنش می تواند ادامه داشته باشد

پایان

شکل2. مدل پیشنهاد شده ی ATM

مشکلات مدل و چگونگی غلبه بر آن ها

1. یکی از مشکلات اصلی این مدل هنگامی است که دوربین به خوبی کار نمی کند یا آسیب دیده است. این حالت های غیرعادی تکنیکال مانع تراکنش می شود. بنابراین برای حل این مشکل ما یک دکمه "گزارش" را بر روی صفحه در طول فاز تشخیص صورت معرفی کرده ایم. این مسئولان بانک را مطلع می کند و مشکل به زودی می تواند حل شود. برای جلوگیری از استفاده غیر ضروری از دکمه گزارش، جزییات کاربر به مسئولان ارایه می شود تا کاربری را که گزارش مشکل را داده است بشناسند.
2. اگر کاربر OTP را بعد از مدت کوتاهی از فاز تشخیص صورت دریافت نکرد، می تواند تراکنش را به تعلیق بیاندازد و کاربر را اذیت کند. برای غلبه بر این حالت یک کلید "دوباره فرستادن OTP " گذاشته شده که OTP را دوباره می فرستد.
3. مشکل اصلی این سیستم این است که اگر یک سرویس شبکه ی خاصی پایین بیاید، دریافت OTP‍ برای کاربر غیرممکن خواد یود

دید آینده

همان طور که در جدول 1 ذکر کرده ایم، تکنیک تشخیص صورت در مقایسه با سایر بیومتریک ها چالش برانگیزتر است بنابراین الگوریتم کاراتری باید توسعه یابد. مشکلات در تکنیک تشخیص صورت مانند ناتوانی در تشخیص صورت هنگامی که ریش، پیرشدن، عینک و کلاه وجود دارد می تواند اصلاح و حذف یا کاهش یابد. اگر هزینه ی تشخیص عنبیه یا قرنیه کاهش یابد، می شود به جای تشخیص صورت مورد استفاده قرار گیرد.

نتیجه گیری

این پروژه هنوز تحت توسعه است. مدل، تحلیل کیفی الگوریتم استفاده شده بر اساس متریک های الگوریتم موجود را نشان می دهد. بر اساس آمار تشخیص صورت PCA پایه بسیار دقیق است، زمان محاسبه ی کمتر و فضای ذخیره کمتری را به دلیل اینکه عکس های آموزش دیده به فرم نمایش آنها در یک پایه کاهش یافته ذخیره می شوند نیاز دارد. بعد از اتمام پروژه ما جنبه های کیفی مدل را جمع آوری می کنیم و آن را با نتایج کیفی برای اثبات بیشتر مقایسه می کنیم.