Specialized Scientific Quarterly Journal of

Arman Process (APJ)

Threats and Approaches for Security in e-commerce services

A. Mohamadpoor [*,1]

[1] *Department of Electrical and Computer Engineering, Center of Tehran Branch, Islamic Azad University, Tehran, Iran*

ABSTRACT

Today, e-commerce has become a way of doing business in the modern world. Basically, e-commerce can not grow enough without security. To achieve a dynamic e-commerce, we must implement security in it within the framework of principles, so that we can use it as a sustainable sample of business. Security issues, unauthorized users, viruses and the like are terrifying for companies at any level of internet connection. Most companies focus on their hardware and software to deal with these problems. Understanding security threats and risks, especially the dangers of e-commerce, can be a great help in designing and building a secure infrastructure. This article discusses various ways to reduce security threats, especially in cases where the greatest threat is posed by unauthorized users, viruses and other forms of network intrusion; Finally, security approaches, recommendations and solutions to deal with these threats are provided.

KEYWORDS:
Security
E-business
Protocol
Business Models
Security Threats

Corresponding author
Al.mohamadpoor@yahoo.com

Submitted: 2021-08-01
Accepted: 2021-10-07

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
11	0	0

فصلنامه تخصصی

آرمان پردازش

خطرات و راهکارهای امنیت در خدمات تجارت الکترونیک

علی محمدپور *[1]

[1] گروه کامپیوتر، دانشکده برق و کامپیوتر، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

امروزه تجارت الکترونیکی به روشی برای کسب وکار در دنیای مدرن تبدیل شده است. اساسا تجارت الکترونیک بدون امنیت به اندازه کافی نمیتواند رشد پیدا کند. برای دستیابی به به یک تجارت الکترونیک پویا باید امنیت را در آن تحت چارچوب های اصولی پیاده سازی نماییم تا بتوانیم از آن به عنوان یک نمونه پایدار از تجارت استفاده کنیم. مسائل امنیتی، کاربران غیرمجاز، ویروسها و نظایر آنها برای شرکتها در هر سطحی از اتصال به اینترنت وحشتزا هستند. اغلب شرکتها برای مقابله با این مشکلات توجه خود را معطوف به سخت افزار و نرم افزار خود میسازند. فهم و درک صحیح از ریسک ها و خطرات امنیتی، به ویژه خطراتی که در دادوستدهای الکترونیکی وجود دارد، کمک زیادی در طراحی و معماری یک زیر ساختار امن و کارامد می نمایند. در این مقاله ریسک های بالقوه این حوزه بیان و روشهای مختلف درباره کاهش خطرات امنیتی بررسی شده است، به ویژه در مواردی که بیشترین تهدید از طرف کاربران غیرمجاز، ویروسها و سایر شکلهای نفوذ در شبکه انجام میگیرد؛ و در نهایتا توصیه ها و راه حل هائی برای مقابله با این تهدیدات ارائه گردیده است.

واژگان کلیدی:
امنیت
تجارت الکترونیک
پروتکل
مدلهای تجارت الکترونیک
خطرات امنیتی

[1] نویسنده مسئول

Al.Mohamadpoor@yahoo.com

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۱

مقدمه

یکی از بزرگترین موانع موجود بر سر راه توسعه تجارت الکترونیک، امنیّت مربوط به آن و تضمین داد و ستد از طریق شبکه وب می‌باشد. اعتماد و اطمینان در تجارت الکترونیک به مرور و در طی سال‌ها با پیشرفت فنّاوری مربوط به امور امنیتی افزایش یافته، اما طبیعی است با ورود به دنیای مدرن ارتباطات و اینترنت، که تجارت الکترونیکی بخشی از آن است، خطرات و تهدید مهاجمان که با بکارگیری روش‌های گوناگون درصدد ایجاد اختلال، انهدام و یا وارداوردن صدمه به اطلاعات هستند، همواره وجود داشته و خواهد داشت [1].

در این راستا، ایجاد ایمنی و رفع هرگونه تهدید در انجام معاملات اقتصادی و نیز قانونمندی و مطمئن‌بودن فعالیت‌ها و مخفی‌ماندن اطلاعات مربوط به عنوان توقّعات مشتریان یا سرویس‌گیرندگان مطرح بوده و در مقابل سرویس‌دهندگان نیز انتظار فعالیّت همراه با دقّت کاربر، عدم انجام اعمال خلاف مقرّرات و قوانین شبکه و اجتناب از تخریب و صدمه‌زدن به سایت‌ها را از مشتریان دارند. در عین حال، هر دو طرف از واسطه انتقال دهنده اطّلاعات که همانا سیستم‌های مخابراتی هستند، توقع جلوگیری از استراق اطلاعات و نفوذ ناخواسته را دارند. به عبارت دیگر در مباحث مربوط به امنیت شبکه اینترنت، ایمنی کاربر، ایمنی سرویس‌دهنده و ایمنی مخابراتی از رئوس مطالب مورد توجه هستند. در این مقاله سعی گردیده تا مسایل امنیتی مربوط به اینترنت و تجارت الکترونیکی و روش‌های ایمن‌سازی در این زمینه توضیح داده شده و درک مناسبی از اهمیّت و نقش آن به خواننده ارائه گردد [2, 3] .

خطرات و تهدیدهای عمومی در حوزه خدمات تجارت الکترونیک

بررسی‌های آماری حاکی از آن است که تهدیدهای عمومی مربوط به شبکه وب و سیستم‌های سرویس‌دهنده اینترنتی (سرورها) سرویسهای تجاری به شرح زیر می‌باشد [4-7]:

- ورود و نفوذ به سیستم‌های بانکی و برداشت‌های غیرمجاز از حساب‌های بانکی فعال:

لازم به ذکر است که مهاجمین با در نظر گرفتن رخنه های امنیتی و شرایط حساب‌های بانکی فعال، پس از نفوذ، اقدام به تخلیه حساب و یا جابجایی غیرمجاز پول نمایند.

- انجام معاملات صوری و رسید سازی غیرواقعی به صورت الکترونیکی جهت کسب اعتبار:

اعتبارات بانکی به حساب‌هایی تعلق می‌گیرد که دارای گردش مالی بالایی باشند و اساساً با در نظر گرفتن این که گردش‌های مالی مناسب با انجام معاملات و تنظیم قراردادهای مطلوب با ارقام بالا به وجود می‌آید، لذا با استفاده از سیستم عقد قراردادهای الکترونیکی و ایجاد پرونده‌های مالی غیرواقعی در بانک اطلاعاتی، سوءاستفاده‌گران به هدف خود می‌رسند [5] .

- گشایش حساب‌های غیرواقعی و انجام معاملات غیر حقیقی:

مهاجمان در این زمینه سعی در ایجاد حساب‌های جاری و یا ارزی غیرواقعی می‌نمایند و در آنها همچون قبل سعی در ایجاد معاملات غیرواقعی و نقل و انتقالات پول می‌نمایند. بدیهی است با در نظر گرفتن غیرواقعی‌بودن حساب‌ها، پیگیری وضعیت صاحب‌حساب و یا کنترل آن و فرآیند اقتصادی قابل انجام نبوده و به راحتی از آن سوء استفاده می‌شود [3, 6].

- جعل و تغییر در اسناد مالی و بانکی:

در این مورد، مهاجمین با نفوذ به سیستم‌های مالی سعی در ایجاد تغییر در حساب‌های بانکی نموده و معمولاً مدارک مهم را مورد تهاجم قرار می‌دهند. بدیهی است در این شکل از تخریب نیز منافع مالی سرشاری برای مهاجمان تامین می‌گردد.

- کپی‌برداری غیر مجاز و یا سرقت اطلاعات:

در این مورد، معمولاً مهاجمان سعی در کپی‌برداری و یا سرقت از اطلاعاتی می‌نمایند که دارای طبقه‌بندی اطلاعاتی است. با عنایت به اینکه غالب مراکز استراتژیک و سازمان‌ها اقدام به مکانیزه‌کردن فرآیند نگهداری از اسناد و مدارک و انجام امور اداری روزانه خود می‌نماید، لذا معمولاً با ایجاد لایه‌های دسترسی گوناگون، امکان استفاده از بانک‌های اطلاعاتی را برای مدیران و یا افراد مجاز مهیا نموده‌اند. با این حال خطر نفوذ مهاجمان و در پی آن خطر سرقت اطلاعات و کپی‌برداری از آنها همواره نگران‌کننده خواهد بود و از عمده مشکلات امنیتی در تجارت الکترونیک می‌باشد.در حقیقت مهاجمین با استفاده از دسترسی به کدهای کاربران، به اطلاعات طبقه‌بندی و با ارزش دست‌یافته و بدین وسیله اقدام به سرقت اطلاعات می‌نمایند [7, 8].

- ایجاد تغییر غیرمجاز و دستکاری در اطلاعات:

این مورد در برخی از سیستم‌های مالی و اقتصادی و نیز در بانک‌های اطلاعاتی رسمی دیده شده است. نفوذ و دستکاری اطلاعات موجود بر روی شبکه‌های بانکی با درنظرگرفتن گستره فعالیت این نوع از شبکه‌ها، منافع اقتصادی مطلوبی را برای مهاجمان به دنبال داشته است. دستکاری بانک‌های اطلاعاتی و اخبار و تغییر اطلاعات سایت‌های بازرگانی از دیگر معضلات این مبحث از امنیت شبکه می‌باشد.

- انتشار غیرمجاز اطلاعات:

انتشار اطلاعات طبقه‌بندی شده دولتی، شخصی، اقتصادی و ... توسط مهاجمان از دیگر نگرانی‌های ویژه اداره‌کنندگان سیستم‌های اطلاعاتی است. معمولاً این تهدیدها بر روی

سایت‌هایی دیده می‌شود که در آنها اطلاعات طبقه‌بندی شده سیاسی، علمی، اقتصادی نگهداری می‌شوند. از جمله این سایت‌ها می‌توان به پایگاه‌های اطلاعات مراکز علمی یا بانک‌های اطلاعاتی مربوط به سوابق امنیتی و موارد استراتژیک اشاره نمود.

◙ تغییر در ساختار ظاهری سایت:

در بسیاری از مواقع دیده شده است که محتوای ظاهری سایت‌های اینترنتی که در معرض مراجعه‌کنندگان قرار دارد، به صورت ناگهانی و بدون آگاهی مدیران آن سایت‌ها تغییر نموده است. بدین ترتیب که مهاجمان صفحات اصلی سایت را با صفحات دیگری جابجا نموده و عملاً استفاده از محتوای اصلی سایت را برای کاربران اختصاصی و عمومی غیرممکن می‌سازد. در بعضی مواقع غیرممکن می‌سازد. در بعضی مواقع نیز شاهد هدایت ناخواسته کاربر از سایت مذکور به سایت‌های غیرمجاز دیگر به منظور درامدزائی غیرقانونی هستیم.

◙ تخریب بانک‌های اطلاعاتی:

در مواقعی دیده می‌شود که مهاجمان پس از نفوذ به سیستم، باعث انهدام بانک‌های اطلاعاتی موجود در آن گردیده و خسارات جبران‌ناپذیری را به سازمان‌های مربوطه وارد می‌آورند.

◙ ایجاد دسترسی، تعریف کاربران جدید و تخریب نامحسوس:

در بسیاری از شبکه‌های تجاری که در آنها کاربران زیادی فعالیت می‌کنند، کنترل فردفرد مراجعه‌کنندگان و کاربران برای مسئولین سایت‌ها، امکان‌پذیر نیست، به این ترتیب همواره خطر نفوذ و ایجاد سطوح دسترسی جدید و یا کاربران مجازی وجود دارد. بدیهی است در این شکل از خرابکاری‌های شبکه‌ای، مهاجمین قادر خواهند بود به صورت نامحسوس کلیه تراکنش‌ها و فرآیندهای گوناگون موجود در سایت را مورد بازبینی قرار داده و از آن سوءاستفاده نمایند که این کار با دسترسی به کد عبور شبکه به راحتی قابل انجام است [9].

عوامل موثر در تخریب امنیت شبکه وب

بعضی از عوامل موثر در ساختار شبکه‌های سیستم های تجاری که باعث می‌گردند تا مهاجمان امکان نفوذ و حمله به شبکه را پیدا نمایند، به شرح زیر هستند [9-11]:

◙ اجازه استفاده از سرویس‌های گوناگون در سرور:

سرورهای شبکه از سرویس‌های گوناگونی نظیر HTTP و FTP استفاده می کنند. بطور مثال هم اکنون استفاده از امکانات HTTP بر روی TCP/IP با توجه به گستردگی سرویس‌های آن مورد توجه قرار گرفته است و لذا وجود حفره‌های فراوان و بسترسازی مناسب برای مهاجمین در این پروتکل مشهور، موجبات پدیدآمدن اختلالات امنیتی فراوان در شبکه می‌گردد.

◙ عدم رعایت تدابیر امنیّتی در نرم‌افزارهای سرورها: معمولاً سرویس‌دهندگان وب جهت سهولت دسترسی و یا انجام امور کاربران و مشتریان خود اقدام به نصب نرم‌افزارهای کاربردی بر روی سیستم خود می‌نمایند که غالباً فاقد تدابیر لازم امنیتی می‌باشد. لذا بررسی و پیش‌بینی اقدامات که باید مورد توجه سرویس‌دهندگان وب قرار گیرد، نصب و راه‌اندازی نرم‌افزارهای Capture و یا ذخیره‌کننده Log بر روی سرور می‌باشد.

◙ اعتماد به عملکرد کاربران:

یکی دیگر از کاستی‌های سرورها در ارایه سرویس‌های برخط، اعتماد به عملکرد قانونی و صحیح کاربران است. در حقیقت همین ذهنیّت موجب عدم کنترل کاربران خواهد شد. البته زمینه این مشکل شبیه مورد قبلی است، اما در این جا تراکم عملیات‌های انجام‌شده و درصد بروز خطا برای سرویس‌دهندگان موجب عدم کنترل عملکرد و تراکنش‌های اقتصادی کاربر می‌گردد. لذا هیچ‌گاه نباید به روال های امنیتی و عملکرد کلی کاربران یک سایت کامل اعتماد داشت.

◙ عدم وجود روش‌های مناسب شناسایی کاربر:

یکی دیگر از نقاط ضعف سرورها، عدم استفاده از روش‌های مناسب شناسایی کاربران مجاز به استفاده از امکانات سیستم می‌باشد. امروزه عمده‌ترین روش شناسایی کاربر، نام شناسایی و کلمه عبور او می‌باشد، که براساس آمار رسمی یکی از مهمترین راه‌های سوءاستفاده از سایت‌ها، به دست‌آوردن اطلاعات و استفاده غیرمجاز از آنها می‌باشد.

◙ عدم شناخت کافی از صحّت اطلاعات دریافتی:

یکی دیگر از نقاط ضعف موجود در سرورها، عدم کنترل اطلاعات دریافتی و ارسالی از سوی کاربران می‌باشد. در حقیقت شیوه‌ای مرسوم که توسط مهاجمان مورد استفاده قرار می‌گیرد، ارسال Script و یا برنامه‌های پس از نفوذ بر روی سرورها می‌باشد که پس از دریافت‌های مذکور، مهاجم به سهولت قابلیت تخریب، تغییر و نهایتاً ایجاد اختلال در سایت را خواهد داشت.

راهکارها و تدابیر امنیتی

همان‌طور که گفته شد، تجارت الکترونیکی نیازمند بستری ایمن برای مخابره و دریافت استاد بازرگانی و اطلاعات است. این فن‌آوری نوین، در همان حال که دقّت و سرعت پردازش را افزایش داده است، باید پاسخگوی مسائل و خطراتی باشد که برای آن پیش می‌آید. در تجارت الکترونیکی علاوه بر دو طرف معامله یعنی فروشنده و مشتری، بانک‌های آن دو و واسطه‌ها و حمل‌کنندگان کالاها نیز با کار درگیر هستند. در هر یک از مراحل تجارت الکترونیکی یعنی از هنگام مراجعه مشتری به سایت فروشنده تا آخرین مرحله که تحویل کالا به مشتری است، پیام‌های الکترونیکی میان فروشنده و مشتری و بانک‌های آن دو

به عنوان درخواست‌ها، پاسخ‌ها، اسناد مالی و بازرگانی و... رد و بدل می‌گردد و خطرات بسیاری، پیام‌ها را تهدید می‌کند که این موارد می‌توانند رابطه سالم بین دو طرف معامله را مخدوش نموده و باعث ضررهای جبران‌ناپذیر اقتصادی به طرفین گردد، لذا برای انجام داد و ستدهای الکترونیکی، بایستی به مسایل امنیتی در رابطه با تجارت الکترونیکی که امکان بروز آنها وجود دارد، مورد بحث قرار می‌گیرند که می‌توان این مسایل را در ۵ دسته کلی زیر تقسیم‌بندی نمود:

■ تایید هویّت یا اصالت:

اینترنت با توجّه به طبیعت آن یک محیط ناشناس و گمنام است و این گمنامی بر تجارت الکترونیکی اثر می‌گذارد. یعنی هنگام انجام معامله بایستی هویّت هرکدام از طرفین برای طرف دیگر تایید گردد. تایید هویت یا اصالت فرآیندی است که تضمین می‌کند، هویت هر یک از طرفین همان است که ادّعا می‌شود. این قضیه وقتی اهمیّت بیشتری پیدا می‌کند که معاملات با حجم و ارزش بالا و یا معاملاتی که شامل ردّ و بدل‌شدن اطلاعات حسّاس می‌باشند، انجام می‌گیرد. روش‌های عمومی تایید هویّت شامل انواع الگوریتم های رمزگذاری با کلید عمومی و خصوصی، پروتکل ها، استانداردها، گواهینامه‌ها و امضاهای دیجیتالی هستند.

■ محرمانه‌ماندن داده‌ها:

محرمانه‌ماندن داده‌ها و اطّلاعات برای حفاظت از آنها در مقابل سوءاستفاده ضروری است. سطح امنیت در نظر گرفته شده در یک سایت تجاری به اطلاعات ارائه‌شده در آن و لزوم محرمانه‌ماندن آنها بستگی دارد. به عنوان مثال در یک سایت B2B که در هنگام مذاکرات بین طرفین معامله، اطّلاعات مهمّی مثل قیمت‌ها رد و بدل می‌شود، امنیت در سطح بالایی قرار داشته ولی اطلاعات مثل وضع هوا یا قیمت محصولات استوک می‌تواند سطح پایینی از امنیت باشد و محرمانه‌ماندن آنها لزومی ندارد.

■ کنترل دسترسی:

با اعمال کنترل دسترسی می‌توان منابعی را که کاربر می‌تواند در سیستم یا شبکه به آنها دسترسی داشته باشد را کنترل نموده و در حقیقت کنترل دسترسی فرآیندی است که تعیین می‌کند یک کاربر اجازه انجام چه کارهایی را دارد. به این طریق از دسترسی غیرمجاز به منابع و مراجع اطلاعاتی جلوگیری می‌گردد. برای انجام این کنترل معمولاً از نام کاربر و کلمه عبور استفاده می‌گردد و هر کاربر با واردکردن این دو مشخصه که مخصوص اوست، می‌تواند به مرحله بعدی دسترسی داشته باشد.

■ تمامیّت یا درستی داده‌ها:

بایستی این اطمینان حاصل شود که داده‌ها و اطّلاعاتی که ارسال می‌شوند، در حین ارسال دچار تغییر و دستکاری نشوند. بدون سرویس‌های تامین امنیت که می‌کوشند تا پیام فرستاده شده در شبکه، در حین ارسال دچار تغییر و دستکاری نگردد، یک شخص مهاجم می‌تواند پیام را در حین ارسال، دریافت کرده، آنها را تغییر داده و مجدّداً در شبکه ارسال کند، بدون این که این تغییرات برای گیرنده پیام آشکار باشد. یکی از روش‌های متداول برای حفاظت از داده‌ها در مقابل دستکاری، رمزگذاری آنهاست که در ابتدای ارسال پیام انجام می‌گیرد و در مقصد پیام برای استفاده دریافت کننده رمزگشایی می‌شود [10].

■ عدم انکار:

عدم انکار یعنی این که طرفین معامله نتوانند محتویات پیام مبادله‌شده و خرید و فروش انجام شده را انکار نمایند و به عبارت دیگر اثبات این که این معامله بین دو طرف مشخص شده انجام می‌گیرد.برای تامین این هدف و حذف انکار پیام یا مبادله از امضاهای دیجیتالی یا رسیدهای الکترونیکی استفاده می‌گردد. هنگامی که به شبکه وب متصل می‌شوید، کلمات تایپ‌شده از طریق کیبورد یا هر وسیله دیگری برای واردکردن داده‌ها (مثل موس یا دستورات صوتی و غیره)، دقیقاً به همان شکل به وب انتقال می‌یابند و همان‌طور که هستند ارسال می‌گردند. اما در بسیاری مواقع، شما به عنوان مشتری و همچنین دریافت‌کننده داده‌ها به عنوان فروشنده، ترجیح می‌دهید و لازم می‌دانید که از داده‌ها و اطلاعات ارسال‌شده، فی‌مابین در مقابل هرگونه سوءاستفاده محافظت گردند و به عبارتی امنیت داده‌ها و اطلاعات تامین گردد. به طور مثال کارت اعتباری شما از این قبیل تراکنش ها است. در هنگام پرداخت پول در تجارت الکترونیکی و ارسال شماره از طریق اینترنت به سایت تجارت الکترونیکی و بانک شما، لازم است از آن محافظت شده و قابل خواندن و سوءاستفاده نباشد [8, 11].

لازم به ذکر است، قبل از شروع هر کاری در زمینه مقابله با خطرها، بایستی بیان داشت که هیچگاه نمی توان تمامی تهدیدها را به طور کامل مرتفع ساخت. چرا که درآن هنگام دیگرخطری باقی نمی ماند و این به معنای امنیت صد در صد می باشد که چنین چیزی تعریف نشده است.

نتیجه گیری

امنیت، حفظ حریم شخصی، طراحی و محتوای وب سایت های تجارت الکترونیک از مهمترین عوامل شکل گیری اعتماد در تراکنش های انلاین از دید کاربران اینترنتی است. رشد مداوم تکنولوژی در جامعه منجر به شیوه های مناسبی برای خرید انلاین شده اما این شیوه ها سبب تنبلی و بی دقتی در مورد اطلاعات شخصی شده است. بنابراین هر کسب و کار تجاری باید مطالعات گسترده ایی در خصوص ویژگیهای امنیتی و افزایش آگاهی در خصوص قوانین و سیاست های امنیتی انجام دهد تا اعتماد را برای کاربران خود ایجاد کند. محققان پیشنهاد می دهند که خریداران اینترنتی باید انگیزه های خود را برای مراقبت

از اطلاعات شخصی خود داشته و آگاه از حضور هکرها باشند. و در صفحات مختلف هرگز اطلاعات خود را وارد نکنند و باید آگاه از کاربرانی باشند که برای آنها ایمیل ارسال می کنند. لازم است که بدون شناسایی فرد یا سایت فرستنده پیام به هیچ وجه روی آن کلیک نکنند. مجرمان اینترنتی با استفاده از نقاط آسیبی پذیر از یک سو، اشتباهات افراد در زمان خرید اینترنتی از سایت های ناامن و از سوی دیگر ویروسی شدن و ارائه اطلاعات غیر ضروری به سایتها امنیت یک فرایند یا تجارت را به مخاطره می اندازد.

مراجع

[1] Yang, S., J. Han, J. Li, et al. 2018. Identity-based undetachable digital signature for mobile agents in electronic commerce. *Soft Computing* 22: 1–15.

[2] S. N. Ahmad, M. Laroche, Analyzing electronic word of mouth: A social commerce construct, Int. J. of Inf. Man. 37, 3, 202-213, (2017) https://doi.org/10.1016/j.ijinfomgt.2016.08.004

[3] Al-Jaljouli, R., J. Abawajy, M. M. Hassan, et al. 2016. Secure multi-attribute one-to-many bilateral negotiation framework for e-commerce. *IEEE Transactions on Services Computing* 11: 1–1.

[4] Alsaad, A., R. Mohamad, and N.A. Ismail. 2017. The moderating role of trust in business to business electronic commerce (B2B EC) adoption. *Computers in Human Behavior* 68: 157–169.

[5] T. Y. Kim, R. Dekker, C. Heij, Cross-border electronic commerce: Distance effects and express delivery in European Union markets, Int. J. of Elec. Comm. 21, 2, 184-218, (2017) https://doi.org/10.1080/10864415.2016.1234283

[6] Farash, M. S., S. A. Chaudhry, M. Heydari, et al. 2017. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. International Journal of Communication Systems 30 (4): n/a-n/a.

[7] Royan, B. 2013. Electronic commerce and the Scottish cultural resources access network. Vine 30 (3): 41–43.

[8] E. Turban, J. Whiteside, D. King, Outland, Introduction to electronic commerce and social commerce, (Springer, 2017) https://link.springer.com/content/pdf/10.1007/978-3-319-50091-1.pdf

[9] Amit, B., & Steve, M. (2003). Authentication in e-commerce. Communications of the ACM, 46, 159–166.

[10] Antoniou, G., Batten, L., & Parampalli, U. (2008). A trusted approach to e-commerce. In W. Jonker & M. Petkovic (Eds.), SDM 2008 (Vol. 5159, pp. 119–132).

[11] Ashrafi, M. Z., & Ng, S. K. (2008). Enabling privacy-preserving e-payment processing. In Lecture notes in computer science (vol. 4947, p. 596).