

دانشگاه صنعتي امیرکبیر  
(پلی تکنیک تهران)

دانشكده مهندسی کامپیوتر و فناوری اطلاعات

عنوان

آشنائی با پروتکل HTTPS

نگارش

سید محمد مهدی موسوی

استاد راهنما

دکتر رضا صفابخش

خرداد ۱۳۹۵

چكيده

فهرست عناوین

۱ مقدمه

فصل ۲

فصل ۳

....

فصلN

جمع بندی و نتیجه گیری

منابع و مراجع

اول فصل حتما باید از اینور صفحه شروع شود (سمت چپ)

مقدمه

یادم باشه که این صفحه حتما با شماره ی ۱ مشخص شود

یادم باشه که صفحات قبل حتما با حروف آ تا ... و مشخص شود .

۲ فصل دوم

یادم باشه که حتما از شکل استفاده کنم

فوتر و هدر حتما قرار دهم

یادم باشه که حتما بصورت

۱

۱.۱.۱

۱.۱.۲

مطالب باید دسته بندی شود .

عدد ها حتما باید به زبان فارسی باشد ۱ ۲ ۳ ۳ ۴

جمع بندی و نتیجه گیری

منابع و مراجع

در آخر کار هم حتما باید از نظر نگارشی بررسی شود

چکیده

مقدمه

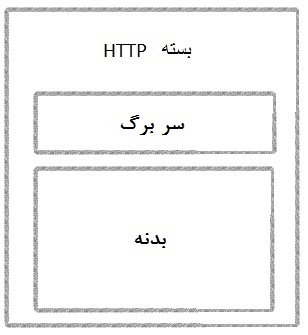
امروزه امنیت شبکه یکی از مسائل مهم برای ادارات و شرکت های دولتی و سازمان های کوچک و بزرگ است. فضای مجازی به دلیل گسترگی و عدم کنترل پذیری رویکردی سیستماتیک را برای امنیت شبکه می طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفته یک انتخاب نیست، بلکه یک ضرورت است. محافظت از اطلاعات اختصاصی، به منابع مالی نامحدود و عجیب نیاز ندارد بلکه با درکی از مسأله، خلق یک طرح امنیتی استراتژیک و تاکتیکی می تواند تمرینی آسان باشد در این اثر به بررسی راه کار های امنیت بخشید به پروتکل HTTP از طریق دو پروتکل لایه ی امنیت می پردازیم .

فصل ۲

مروری بر پروتکل HTTP[[1]](#footnote-1)

پروتکل HTTP یک از پروتکل های لایه ی کاربرد[[2]](#footnote-2) در شبکه های کامپیوتری است که توسط آقای تیم برنرس لی[[3]](#footnote-3) در نوامبر سال ۱۹۸۹ بنا نهاده شد .

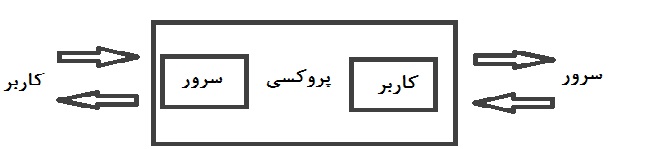
HTTP پروتکلی است که برای انتقال محتوای ابرمتن[[4]](#footnote-4) میان کاربران و رایانه های خدمات رسان[[5]](#footnote-5) مورد استفاده قرار می گیرد. این پروتکل داده را در قالب بسته ها [[6]](#footnote-6) مبادله می کند . در شکل زیر ساختار این پروتکل را مشاهده می کنید. بسته های این پروتکل شامل دو بخش سربرگ و بدنه می باشد. در سربرگ اطلاعات گیرنده، فرستنده، و ویژگی های بسته مانند اندازه ی بسته نوع ارتباط و مواردی از این دست قرار می گیرد . در بدنه اطلاعاتی که طرفین می خواهند با همدیگر مبادله کنند قرار می گیرد .

شکل 1

حال که با این پروتکل بیشتر آشنا شدیم بهتر است ببینیم که چرا و چگونه امنیت این پروتکل تهدید می شود . به جهت همی منظور بهتر است آشنائی به تجهیزات میانی شبکه داشته باشیم در ادامه با پروکسی ها به عنوان یک نمونه از عناصر میانی آشنا می شویم که بصورت گسترده ای مورد استفاده قرار می گیرد .

**پروکسی[[7]](#footnote-7)**

پروکسی ها یکی از عناصر میانی در شبکه های کامپیوتری هستند که به فراوانی مورد استفاده قرار می گیرند این عنصر برای کاربر نقش رایانه ی خدمات رسان، و برای رایانه ی خدمات رسان نقش کاربر را بازی می کند .

شکل ۲

کاربرد های پروکسی

* حسابرسی [[8]](#footnote-8)

کاربران قبل از اینکه به شبکه ی جهانی اینترنت دسترسی پیدا کنند نیاز است که حویت آنها احراز شود و دلیلی هم ندارد که هویت افراد و اعمالی که در فضای مجازی انجام داده اند مخفی بماند به همین منظور پروکسی ها به عنوان عناصر میانی وظیفه دارند که فعالیت های کاربران را نگه داری کنند و اگر اعمال غیر قانونی از افراد سر نزند و بتوان با موارد این چنینی بر خورد کرد .

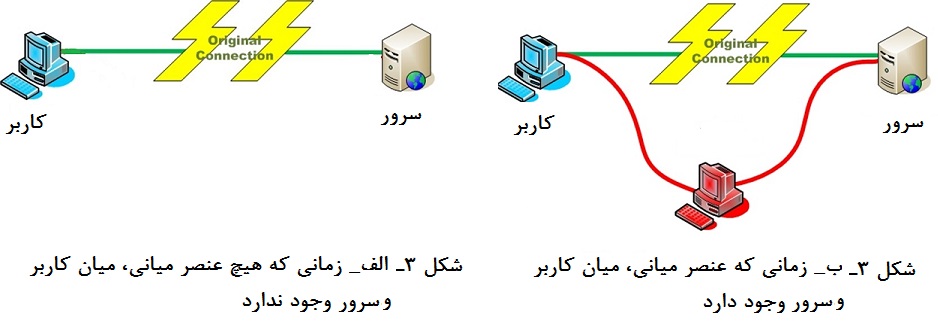
* مخفی ماندن برخط[[9]](#footnote-9)

پروکسی در معنا یعنی "وکیل" و در تعریف پروکسی ها هم گفتیم که پروکسی ها عناصری هستند که برای کاربر نقش سرور و برای سرور نقش کاربر را بازی می کنند پس به نظر می رسد که فعالیت هائی که کاربران انجام می دهد به اسم پروکسی ها ثبت می شود و هر کاری که کاربر انجام داده به مثابه این است که پروکسی انجام داده و از این طریق هویت شخص مخفی می ماند . لازم به ذکر است که مخفی ماندن برخط در فضای مجازی شبیه به یک شوخی با مزه است. حتی اگر صد ها پروکسی و عناصر میانی استفاده کنید نمی توانید هویت خود را در فضای مجازی مخفی نگه دارید[[10]](#footnote-10) .

* امنیت پروتکل HTTP

مزایای پروکسی ها را بررسی کردیم اما این عناصر مشکلاتی را برای ما ایجاد می کنند و از جمله ی این مشکلات، تهدید امنیت در شبکه و به تبع آن تهدید امنیت پروتکل HTTP است .

همانطور که در شکل زیر مشاهد می کنید دو حالت را بررسی می کنیم در حالت اول فرض می کنیم که هیچ عنصر میانی، میان کاربر و سرور قرار ندارد در اینصورت هیچ مشکلی برای امنیت این پروتکل پیش نمی آید اما رخ دادن چنین حالتی در شبکه غیر ممکن است و بطور قطع در شبکه عنصر میانی وجود دارد (حالت دوم) در اینصورت محتوای بسته های توسط عناصر میانی قابل دسترسی و شنود است و اگر اطلاعات مهم و محرمانه ای منتقل شود امنیت این اطلاعات غیر قابل تضمین است .

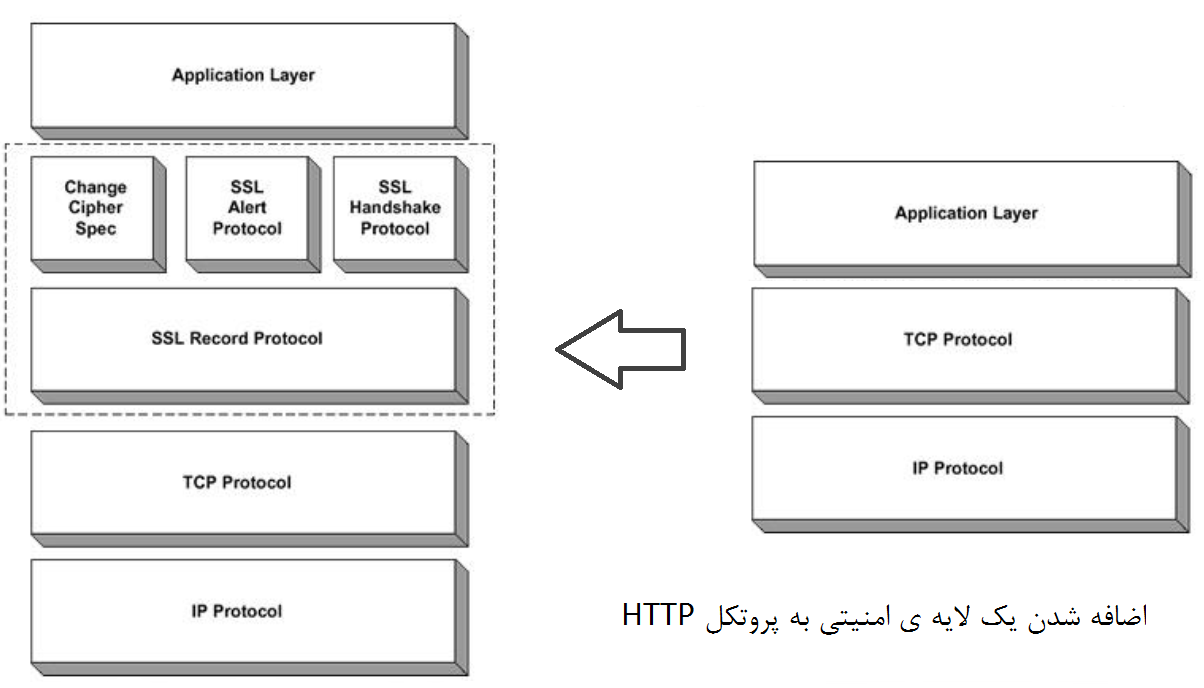
شکل ۳

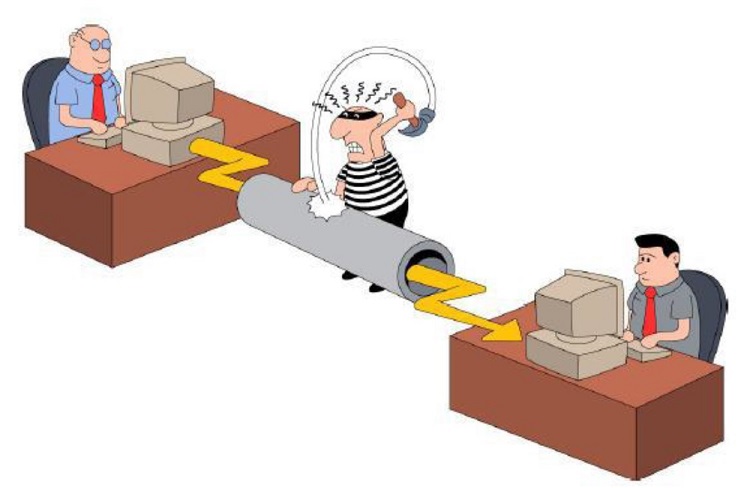
در فصل آینده به راهکار ها و بازنگری هائی در این پروتکل می پردازیم که این پروتکل را برای ما قابل امن می کند .

فصل ۳

HTTPS[[11]](#footnote-11) راهکاری برای امن کردن پروتکل HTTP

در فصل قبل بررسی کردیم که عناصر میانی، در میان مسیر کاربر و سرور قرار می گیرند و پیام های مبادله شده را شنود می کنند به نظر می رسد اگر پیام ها به گونه ای باشد که فقط گیرنده و فرستنده آن را بفهمند مشکل ما حل شده است. پس پروتکل HTTPS پروتکل HTTP را به اینصورت اصلاح می کند که پیام هائی که فرستنده و گیرنده با هم تبادل می کنند به گونه ای رمز گذاری شود که فقط توسط خودشان قابل رمزگشائی باشد. این اصلاحیه با اضافه کردن یک لایه ی امنیتی[[12]](#footnote-12)، امنیت را فراهم می کند . این لایه از دو پروتکل [[13]](#footnote-13)TLS یا [[14]](#footnote-14)SSL استفاده می کند که اساس این دو پروتکل بر مبنای رمز گذاری اطلاعات است . این امر در شکل زیر قابل مشاهد است .

شکل ۴

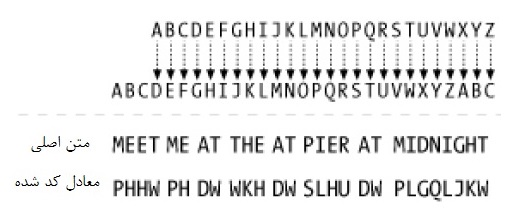
همانطور که در شکل زیر مشاهده می کنید کار لایه امنیتی این است که دسترسی به اطلاعات در میانه ی مسیر را برای، کسانی که قصد سؤ استفاده از اطلاعات را دارند، محدود کند.

شکل 5

* بررسی الگوریتم های رمزگذاری اطلاعات

دو پروتکلی که لایه ی امنیت برای برقراری امنیت استفاده می کند برمبنای رمزگذاری و رمز گشائی اطلاعات است پس نیاز است بصورت مختصر الگوریتم های مورد استفاده را بررسی کنیم . قبل از اینکه سراغ این الگوریتم ها برویم باید به این نکته دقت کنیم که رمز گذری اطلاعات قبل از کامپیوتر ها و در واقع صد ها سال پیش از تولد کامپیوتر ها مورد استفاده قرار می گرفته و بیشتر برای حفظ اسرار جنگی و اطلاعات سری و بسیار مهم کاربرد داشته است .

الگوریتم هائی که قبل از تولد کامپیوتر ها استفاده می شدن بسیار ساده بودند در شکل زیر یکی از این الگوریتم ها را بررسی می کنیم . در این الگوریتم برای رمز گذاری اطلاعات، هر حرف با سه حرف بعد از خودش جایگزین می شود بطور مثال بجای T حرف W را قرار می دهیم و متن اصلی در شکل را به معادل کد شده تبدیل می کنیم و می بینیم که عبارتی که دارای مفهوم است، به یک عبارت غیر قابل فهم تبدیل شده است. بدیهی است که برای رمز گشائی لازم است که هر کاری که برای رمزگذاری انجام داده ایم، بصورت عکس انجام دهیم .

شکل 6

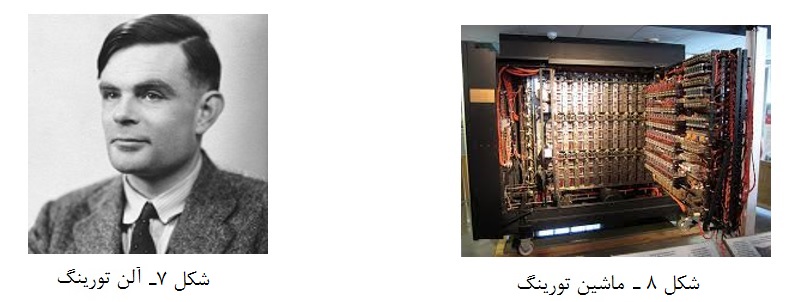
بررسی مشکلات الگوریتم های ساده

1. به دلیل اینکه رمزگذاری اطلاعات توسط الگوریتم های ساده صورت می گرفت، ممکن بود با کمی بازی با متن کد شده، الگوریتم به کار رفته برای رمز گذاری حدس زده می شد و به کل امنیت اطلاعات به خطر می افتاد .
2. فرض کنید که صد شرکت برای حفظ اطلاعات خود از یک الگوریتم استفاده می کردند در اینصورت اگر یکی از این شرکت ها سهل انگاری کند و الگوریتم، به دست افراد سؤ استفاده گر بیفتد امنیت سایر شرکت ها به خطر می افتد .
3. چون عمل رمز گذاری توسط انسان انجام میشد مدت زمانی که طول می کشید که رمز گذاری انجام شود زیاد بود و همچنین بسیار کار طاقت فرسائی بود و نیاز به دقت بالائی داشت .

* اختراع کامپیوتر ها

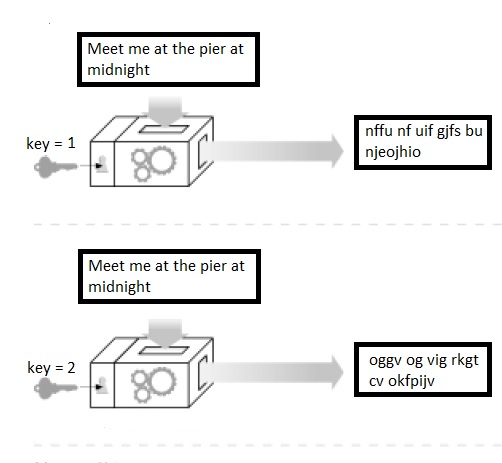
با اختراع کامپیوتر ها تحولی در رمز گذاری ایجاد شد کامپیوتر ها مزیت هائی نسبت به ما داشتند که از جمله آن می توان به سرعت بالا، قابلیت اجرای الگوریتم های پیچیده تر، و همچنین عدم اشتباه در محاسبات، اشاره کرد. جالب است که بدانید که کامپیوتر های برنامه پذیر بخاطر رمزگشائی اختراع شدند

در جنگ جهانی دوم آلمان ها قبل از رد و بدل کردن پیام ها، آنها را رمز گذاری می کردند و کشور انگلستان و سایر کشور ها که پیام ها را شنود می کردند با یکسری پیام های غیر قابل فهم مواجه می شدند به جهت همین موضوع یک تیم برای شکستن کد ها استخدام کردند که این تیم به سرپرستی آلن تورینگ ماشینی اختراع کرد که قادر بود این رمز گذاری را بشکند . این کامپیوتر ها، نسل اولیه کامپیوتر های برنامه پذیر بودند. با این کار تورینگ جنگ جهانی دوم حدود دو سال زود تر به پایان رسید و جان ملیون ها انسان بی گناه حفظ شد .



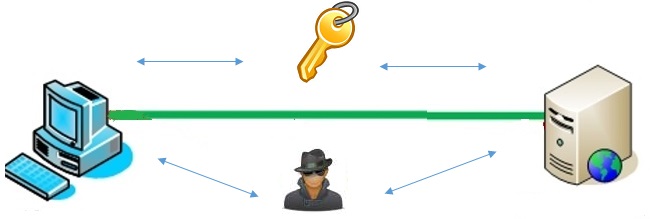
* الگوریتم های رمزگذاری بر اساس کلید

به الگوریتم قبلی باز گردیم، به جای اینکه هر حرف را با سه حرف بعدی جایگزین کنیم هر حرف را با k تا حرف بعدی جایگزین می گیریم و مطابق شکل زیر الگوریتم یک کلید به عنوان ورودی می گیرد و اطلاعات را کد می کند و نکته قابل توجه این است که فقط سری ماندن کلید اهمیت دارد و اگر الگوریتم لو برود با مخفی ماندن کلید هیچ مشکلی برای امنیت اطلاعات پیش نمی آید . در شکل زیر مشاهده می کنید که خروجی به ازای هر کلید با دیگر خروجی ها تفاوت دارد .

شکل 9

الگوریتم رمز گذاری کلید عمومی[[15]](#footnote-15)

این الگوریتم برای رمز گذاری و رمز گشائی اطلاعات از یک کلید عمومی استفاده می کند به عبارت دیگر فرستنده و گیرنده برای رمز گذاری و رمز گشائی فقط از یک کلید یکسان استفاده می کنند. مشکلی که این الگوریتم دارد این است که فرستنده و گیرنده نیاز دارند به نحوی کلید را با یکدیگر مبادله کنند و اگر در میان مسیر کلید در دسترس دیگران قرار بگیرد، همه ی کار های انجام شده بی فایده می شود و مانند این است که عمل کد گذاری اطلاعات صورت نگرفته است . در شکل زیر این امر به وضوح قابل مشاهده است .

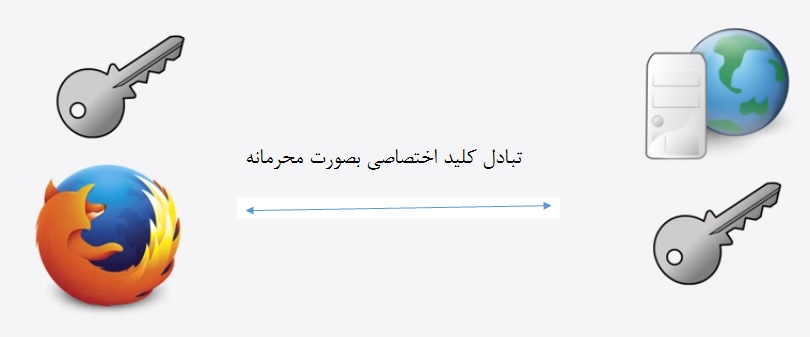
شکل 10

* الگوریتم کد گذاری بر اساس کلید اختصاصی[[16]](#footnote-16)

در الگوریتم کدگذاری بر اساس کلید عمومی، مشکل تبادل کلید عمومی بود. در این روش، الگوریتم رمز گذاری را با کلید عمومی انجام می دهد و رمز گشائی را فقط با کلید اختصاصی انجام می دهد حال همه از کلید عمومی اطلاع دارند اما فقط فرستنده و گیرنده از کلید اختصاصی خبر دارند و می توانند رمز گشائی را انجام دهند .

* مبادله ی کلید اختصاصی

حال که قرار است کلید اختصاصی فقط بصورت محرمانه در اختیار گیرنده و فرستنده باشد لازم است به گونه ای مبادله شوند که فقط در سمت خودشان قابل مشاهده باشد برای این منظور همانطور که در شکل زیر مشاهده می کنید سرور یک الگوریتم در نظر می گیرد که با یک کلید عمومی رمز گذاری انجام می شود و فقط با کلید اختصاصی رمز گشائی صورت می پذیرد، سپس کلید عمومی را برای کاربر ارسال می کند، کاربر پس از دریافت کلید اختصاصی خود را رمز گذاری می کند و برای سرور ارسال می کند. سرور پس از دریافت کلید آن را رمزگشائی می کند و از این پس از این کلید برای رمز گشائی استفاده می کند و مطمئن هستیم که این کلید محرمانه است و فقط فرستنده و گیرنده از آن خبر دارند .

شکل 11

فصل 4 جمع بندی و نتیجه گیری

با توجه به اهمیت حفظ اطلاعات، روش های امنیت دادن به اطلاعات را بررسی کردیم و دیدیم که می توان با استفاده از پروتکل HTTPS امنیت کامل را در ارتباطات ایجاد کرد و دیدیم که این پروتکل امنیت را صد در صد ایجاد کرده و حفاظت اطلاعات را تضمین می کند . باید به این نکته توجه کنیم که بدون دلیل نباید از پروتکل HTTPS استفاده کرد، زیرا این پروتکل برای ما هزینه دارد. در موارد که نیاز به امنیت است باید از این پروتکل استفاده کنیم بطور مثال سیستم های مالی مثل بانک ها، سیستم های دفاعی، سیستم اطلاعاتی، و هر سازمان یا ارگانی که اطلاعات مهمی را رد و بدل می کند باید از این پروتکل استفاده کند. در مقابل اطلاعاتی که مهم نیستند مانند اطلاعات یک وب سایت خبری یا یک وب سایت تبلیغاتی که اطلاعات بصورت عمومی در اختیار همه گان است نیازی به استفاده از پروتکل HTTPS نیست و بهتر است که از پروتکل HTTP استفاده کند

منابع و مراجع

1. Hypertext Transfer Protocol [↑](#footnote-ref-1)
2. Application [↑](#footnote-ref-2)
3. Tim Berners-Lee [↑](#footnote-ref-3)
4. Hyper Text [↑](#footnote-ref-4)
5. Computer Servers [↑](#footnote-ref-5)
6. Packets [↑](#footnote-ref-6)
7. Proxy [↑](#footnote-ref-7)
8. Accounting [↑](#footnote-ref-8)
9. Stay Anonymous Online [↑](#footnote-ref-9)
10. بررسی جزئیات این مسئله در این اثر میسر نیست فقط در همین حد که به هیچ نحو نمی توان از پروکسی ها و عناصر میانی برای مخفی ماندن استفاده کرد زیرا تمهیداتی اندیشیده شده است که می تواند فعالیت های افراد در فضای مجازی را، رد گیری کرد . [↑](#footnote-ref-10)
11. Hypertext Transfer Protocol Secure [↑](#footnote-ref-11)
12. Secure Layer [↑](#footnote-ref-12)
13. Transport Layer Security [↑](#footnote-ref-13)
14. Secure Sockets Layer [↑](#footnote-ref-14)
15. Public Key [↑](#footnote-ref-15)
16. Private Key [↑](#footnote-ref-16)