الفصل التاسع: البنية التحتية للتجارة الإلكترونية

الكلمات المفتاحية:

برتكول الإنترنت – الإنترانت – الإكسترانت – الأنفاق – الشبكة الافتراضية الخاصة – جدران النار – مزود خدمة الإنترنت – الرزمة – الخصوصية – الأمن – البث عبر الوب – توصيل الوسائط المتعددة – التشفير – التوقيع الرقمي – الموجه – المبدل – بوابة الحصن، التوقيع الرقمي، التوقيع الإلكتروني، تقانة التشفير، المفتاح العام، المفتاح الخاص، البطاقة الذكية، كلمات السر.

ملخص:

يحاول هذا الفصل تغطية معظم المواضيع الخاصة بالبنية التحتية اللازمة للتجارة الإلكترونية بجميع أنماطها.

المخطط:

13 وحدة عناوينها بالترتيب المحدد:

1. مثال افتتاحي– شركة UPS تخدم الجمهور.
2. شبكة الشبكات.
3. برتوكولات الإنترنت.
4. أمن الإنترنت.
5. التشفير.
6. التوقيع الرقمي.
7. الشبكات الخاصة الافتراضية Virtual Private Network.
8. متطلبات إنشاء المخازن الإلكترونية.
9. المحادثة على الوب.
10. الإنترانت.
11. الإكسترانت.
12. تطبيقات شبكات الإنترانت والإكسترانت.
13. التمارين.

1. مثال افتتاحي– شركة UPS تخدم الجمهور:

تستند كل مواقع التجارة الإلكترونية بغض النظر عن هدفها الأساسي – B2C أو B2B – إلى نفس البنية الشبكية وبروتوكولات الاتصالات ومعايير الوب والأنظمة الأمنية.

يركز هذا الفصل على العتاد (Hardware) والبرمجيات الأساسية لملايين المواقع المعتادة على بيع الخدمات وعلى التحادث مع كل من الزبائن والشركاء، وعلى الرغم من أن النقاط المشتركة بين مواقع التجارة الإلكترونية تفوق في الأهمية الاختلافات بينها، إلا أنه تحتاج في بعض الأحيان لمكونات ومُخدّمات خاصة، وبشكل خاص في المواقع ذات الحركة الكبيرة أو المواقع التي تبيع الحاجات أو الخدمات المميزة، ويأخذ هذا الفصل في الاعتبار أيضاً بعض هذه المكونات الخاصة.

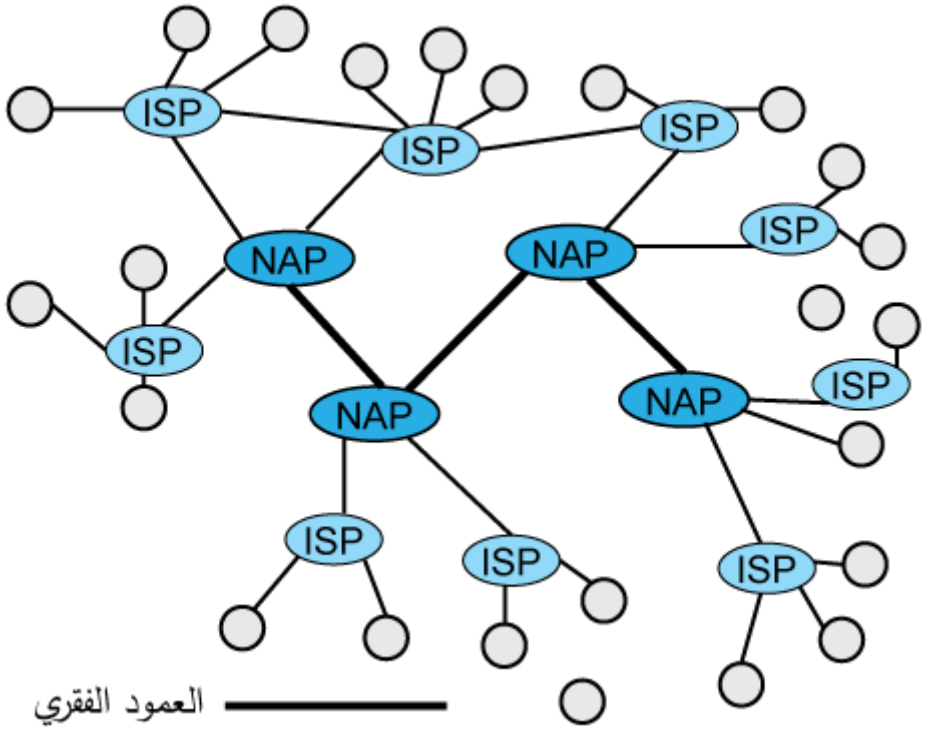
من المهم التذكير أن التكنولوجيا ليست هي المفتاح الحقيقي فمعظم المواقع تستخدم التكنولوجيا الأساسية نفسها بل أن المفتاح الأساسي هو الطريقة التي يجري بها توظيف التكنولوجيا والانتباه المعطى لتوجهات عمل الموقع.

مثال: شركة UPS (United Parcel Service) تخدم الجمهور:

تعمل شركة UPS منذ 1907 كشركة توزيع للرزم، وهي شركة توزيع الرزم الأكبر في العالم، حيث تنقل أكثر من 3 مليارات طرد ومستند في السنة. قامت UPS ولفترة زمنية بتوفير الوسائل للزبائن لرصد شحناتهم – تحديد حالة ووضع رزمة خاصة. في الماضي، كانت هذه العملية تجري بشكل رئيسي عبر الهاتف، وقد كانت خدمة هذه المكالمات أمر مكلف (الكلفة التقديرية 2$ لكل مكالمة).
بنت UPS في 1995 موقع وب. في البداية، كان الموقع موقعاً بسيطاً يجري تشغيله من خلال مُخدّم وب واحد ويتكون من مجموعة صغيرة من صفحات وب ستاتيكية (ساكنة)، ثم جرى في العام 1997 إنشاء موقع وب جديد لخدمة الزبائن

يزود هذا الموقع، بالإضافة إلى معلومات تسويقية عامة، الزبائن بوسائل للقيام بالرصد على الوب، لتحديد التكلفة وزمن العبور لتسليم الرزمة، لتحديد موعد وصول الرزمة من أجل الشحن، ولإيجاد الوسيلة الأقرب، بينما تكون الواجهة بسيطة بشكل كاف، تكون المعالجة البرمجية معقدة قليلاً. لذا جرى تعديل موقع وب UPS لمعالجة كمية كبيرة من الحركة على الشبكة (الحركة الشبكية). حيث يتعرض الموقع لملايين الاستعلامات اليومية!

2. شبكة الشبكات:



واجهت الشركات صعوبات رئيسية في إيصال التطبيقات والمعلومات على الوب في الماضي حتى إلى موظفيها، خاصة عبر المناطق المتباعدة جغرافياً وإلى المستخدمين البعيدين.

تستطيع الشركات اليوم وبسهولة إيصال المعلومات إلى الموظفين، الزبائن، الشركاء، وإلى العموم بغض النظر عن الموقع الجغرافي. يُشير العديد من المراقبين إلى الوب كحافز لهذا التغيير لكن رغم ذلك، بدون 30 سنة أو أكثر من التطوير في البنية التحتية للشبكة العالمية التي نسميها الإنترنت فإن الوب لم يكن ممكناً.

بينما يستخدم العديد منا الإنترنت يومياً فإن قلة منا تملك فهماً واضحاً لعملها الأساسي. من وجهة نظر فيزيائية (مادية)، فالإنترنت هي شبكة مكونة من آلاف الشبكات المتصلة فيما بينها حيث تتضمن هذه الشبكات:

1. الأعمدة الفقرية (Backbones) المتصلة فيما بينها والتي تملك انتشار عالمي
2. شبكات فرعية متنوعة للولوج/ للتسليم
3. آلاف الشبكات الخاصة وشبكات المؤسسات والتي تصل بين المُخدّمات التنظيمية المتنوعة وتحتوي على العديد من المعلومات المهمة.

يجري تشغيل الأعمدة الفقرية بواسطة مزودي خدمة الشبكة NSP (Providers Network Service). وتدار شبكات التسليم الفرعية من خلال مزودات خدمة الإنترنت ISP (Internet Service Providers) المحلية والإقليمية.
تتبادل كل ISP البيانات مع NSP في نقاط ولوج الشبكة NAP (Network Access Points). يقدم الشكل الموجود أعلاه منظراً علوياً للوصلات الداخلية بين NAPs، ISPs، والأعمدة الفقرية.

عندما يطرح المستخدم من الحاسوب الخاص به/بها استعلاماً عبر الإنترنت، فمن المحتمل أن يعبر هذا الاستعلام شبكة ISP، لينتقل عبر عمود فقري أو أكثر، ويقطع شبكة ISP أخرى إلى الحاسوب الذي يحتوي المعلومات.

تتبع الإجابة على هذا الاستعلام مساراً مشابهاً. لا يوجد من أجل أي استعلام وإجابة مرتبطة به مسار معدٌ سلفاً. في الحقيقة، يجري تقسيم الاستعلام والإجابة إلى رزم ويمكن للرزم أن تتبع مسارات مختلفة. يجري تحديد المسارات التي تمر عبرها الرزم بواسطة حواسيب خاصة تدعى الموجهات (Routers). تملك الموجهات خرائط قابلة للتحديث للشبكات على الإنترنت والتي تقوم بتهيئة الشبكات لتحديد مسارات الرزم. تُعتبر شركة Cisco (www.cisco.com) المزود الأول للموجهات عالية السرعة.

3. برتوكولات الإنترنت:

يتلخص عمل الإنترنت بعمل مجموعة البروتوكولات التي تستطيع معالجة الاتصالات بين أي حاسوبين (أو أكثر)، باستخدام أي نوع من أنظمة التشغيل. لتعقيد المشاكل نستطيع أن نفترض أن أي نظام موصول بالشبكة لا يملك أية معرفة حول الأنظمة الأخرى: لا توجد أي طريقة لمعرفة أين يوجد هذا النظام وما نوع البرمجية التي يستخدمها، أو نوع المعدات التي يُشغّلها.

البرتوكول هو مجموعة من القواعد التي تحدد كيف يتصل حاسوبان أحدهما مع الآخر عبر الشبكة. وتقوم البروتوكولات التي جرى عليها تصميم الإنترنت على مجموعة من مبادئ التصميم:

- قابلية التشغيل: يدعم النظام الحواسيب والبرمجيات الواردة من عدة بائعين، وهذا يعني بالنسبة للتجارة الإلكترونية بأن الشركات أو الزبائن غير مطالبين بشراء أنظمة محددة لقيادة العمل
- الطبقية: تعمل مجموعة بروتوكولات الإنترنت في طبقات حيث تبني كل طبقة على طبقات ذات مستويات أدنى
- البساطة: توفر كل طبقة في البنية فقط بضع وظائف أو عمليات، وهذا يعني بأن مبرمجي التطبيقات بعيدين عن تعقيدات العتاد (Hardware) الأساسي
- نهاية –إلى– نهاية: تعتمد الإنترنت على بروتوكولات " نهاية – إلى – نهاية "، وهذا يعني بأن تفسير البيانات يحدث في طبقة التطبيق (جانب الإرسال والاستقبال) وليس في طبقات الشبكة. إنه يشبه إلى حد كبير مكتب البريد: إن عمل مكتب البريد هو تسليم الرسائل، أما من يهتم بمحتويات الرسالة هما فقط المرسل والمستقبل.

1.3. عائلة TCP/IP:

هو بروتوكول التحكم بالإرسال/ بروتوكول الإنترنت (TCP/IP)، الذي يجب أن يعمل بهي حاسوب أو نظام موصول بالإنترنت، فعلياً وكما هو موضح في الشكل الموجود أدناه فإن TCP/IP مؤلف من بروتوكولين – TCPو IP وليسا بروتوكول واحد.

يسمح TCP لحاسوبين بالاتصال أحدهما بالآخر بأسلوب موثوق. يجب على TCP الإشعار عن كل اتصال. إذا لم يجر الإشعار عن الاتصال ضمن زمن معقول، عندها يجب على الحاسوب المرسل إعادة إرسال البيانات.

بهدف إرسال استعلام أو إجابة إلى حاسوب آخر على الإنترنت، يجب تقسيم الاستعلام أو الاستجابة إلى رزم (Packets) معنونة بعناوين الحواسيب المرسلة والمستقبلية، عندها يأتي دور IP.

طبقة التطبيق FTP, HTTP, Telnet, NNTP	
طبقة النقل	
بروتوكول Datagram المستخدم (UDP)	بروتوكول التحكم بالإرسال (TCP)
بروتوكول الإنترنت (IP)	
طبقة واجهة الشبكة	
الطبقة الفيزيائية	

ينسق IP الرزم ويسند العناوين، ويكون طول عناوين الإنترنت 32 بت ويجري كتابتها على شكل أربعة مجموعات من الأعداد يجري الفصل بينها بنقط، مثل: 130.201.55.9، يُسمى هذا التنسيق بالعنونة الرباعية النقطية (Dotted Quad Addressing). على الوب قد تكون ملماً بعناوين مثل www.Google.com خلف كل من هذه العناوين المشابهة للغة الإنكليزية يوجد عنوان رقمي 32 بت.

إن العدد الأعظم المتاح للعناوين هو أكبر بقليل من 4 مليارات (2 مرفوعة للقوة 32)، يبدو هذا كعدد كبير، خاصة وأن عدد الحواسيب على الإنترنت لا يزال بالملايين.

أحد المشاكل هو أنه لا يجري إسناد العناوين بشكل مفرد بل بشكل كتل (Blocks)، على سبيل المثال، عندما أخذت HP (Hewlett Packard) كتلة العناوين التي تبدأ بالرقم "15"، استطاعت إسناد أكثر من 16 مليون عنوان إلى الحواسيب في الشبكات وجرى إسناد كتل أصغر من العناوين إلى المنظمات الأصغر، بينما تخفض عمليات الإسناد الكتلية العمل الذي تحتاج الموجهات (أجهزة التمرير) القيام به (مثلاً، إذا بدأ عنوان بالرقم 15، فذلك يعني أن الرسالة ذاهبة لحاسوب في شبكة HP.

إلا أن هذا الأسلوب في العنونة أدى إلى نضوب في العناوين، ولهذا السبب، بدأت هيئات متنوعة في مجتمع الإنترنت في بداية التسعينات بإنشاء الجيل التالي من بروتوكول الإنترنت IPNG (Next Generation Internet Protocol)، حيث بدأ اعتماد هذا البروتوكول باستخدام عناوين بطول 128 بت. سيسمح هذا لكادرليون حاسوب (10 مرفوعة للقوة 15) بالوصل مع الإنترنت، ووفقاً لهذه الخطة، مثلاً، يستطيع أحد ما أن يتخيل منازل شخصية يملك كل منها شبكته الخاصة. يمكن استخدام هذه الشبكات الداخلية للاتصال الداخلي والولوج ليس فقط للحواسيب داخل المنزل بل أيضاً لمجال عريض من الأدوات المنزلية كل بعنوانه المميز.

2.3. أسماء النطاقات:

تُشير أسماء مثل www.microsoft.com إلى حواسيب على الإنترنت تُسمى أسماء النطاقات. وهي مقسمة إلى أجزاء (قطع) مفصولة عن بعضها بواسطة نقاط. الجزء في أقصى اليسار هو اسم الحاسوب المحدد، الجزء في أقصى اليمين هو نطاق القمة والتي ينتمي إليها الحاسوب، والأجزاء في الوسط هي النطاقات الفرعية.

جرى تنظيم أسماء النطاقات بأسلوب هرمي. يوجد في قمة الهرم النطاق الجذر وتحت الجذر توجد نطاقات قمة (مثل: net, gov, com, org, edu, ...). يوجد تحت كل نطاق قمة الطبقة التالية من النطاقات الفرعية وتحتها توجد طبقة أخرى من النطاقات الفرعية وهكذا. إن عقد الأوراق في البنية الهرمية هي الحواسيب الفعلية.

عندما يرغب المستخدمون بالولوج لحاسوب خاص، فإنهم عادةً ما يقومون بذلك من خلال كتابة اسم النطاق بشكل كامل وليس كتابة العنوان الرقمي. خلف الكواليس، يجري تحويل اسم النطاق إلى العنوان الرقمي الموافق بواسطة مُخدّم خاص يسمى مُخدّم اسم النطاق. تزود كل منظمة على الأقل بمُخدّمي اسم نطاق، المُخدّم الأولي والمُخدّم الثانوي، وذلك لمعالجة التحميل الزائد. على الرغم من انخراط عدة مُخدّمات اسم نطاق في العملية إلا أن الزمن الذي تستغرقه العملية بأكملها من رتبة الميكرو ثانية.

تتحكم IANA (Internet Assigned Numbers Authority) بنظام اسم النطاق. ويستطيع أي شخص التقدم للحصول على اسم. من البديهي بأن الأسماء التي يجري إسنادها يجب أن تكون وحيدة. تكمن الصعوبة بأنه يوجد في العالم عدة شركات ومنظمات لها الاسم نفسه. فكر بعدد الشركات في الولايات المتحدة التي لها اسم ABC. توجد شركة إرسال تلفزيونية بهذا الاسم ولكن يوجد أيضاً مخازن مثل ABC App Liances، في حين يوجد موقع واحد فقط www.abc.com. الأسماء التي جرى إصدارها أولاً تجري خدمتها أولاً. يجب أن يثبت المتقدم بأن له الحق القانوني لاستخدام الاسم. إذا حصل نزاع ما تربح الشركة أو المنظمة ذات العلامة التجارية المبكرة. تقضي إحدى الطرق التي جرى اقتراحها لتقليل النزاعات على أسماء النطاق بالسماح بأسماء قمة إضافية (مثال، tv والذي سينتج عنوان مثل www.abc.tv).

3.3. تطبيقات زبون/ مُخدّم في الإنترنت:

لا يتعامل المستخدمون مع بروتوكولات المستوى الأخفض TCP/IP التي تستند الإنترنت عليها. بالمقابل، يتفاعل المستخدمون مع الإنترنت من خلال عدة تطبيقات زبون / مُخدّم.

وكما يشير الاسم، يوجد في تطبيق زبون/ مُخدّم فئتان رئيسيتان من البرمجيات:

- برمجية الزبون، تتواجد عادةً في سطح مكتب المستخدم وتوفر تجوال وعرض
- برمجية المُخدّم، تتواجد عادةً في محطة عمل أو حاسوب مُخدّم – وتوفر خدمات الولوج للبيانات (حيث تكون البيانات بسيطة مثل ملف أو معقدة مثل قاعدة بيانات تربط بين بياناتها علاقات محددة).

سجري ادراج تطبيقات زبون/ مُخدّم الأوسع استخداماً في الإنترنت لاحقاً. بالنظر لما جرى تدوينه في الجدول التالي، تعمل كل من هذه التطبيقات وفق واحد أو أكثر من البروتوكولات التي تدير عمليات اتصال المُخدّمات والزبائن بعضهم ببعض.

التطبيق	البروتوكول	الهدف
البريد الإلكتروني	Simple Mail Transport Protocol (SMTP) Post Office Protocol Ver.3 (POP3) Multipurpose Internet Mail Extensions (HIME)	يسمح بإرسال الرسائل النصية والملحقات الرقمية عبر الإنترنت
نقل الملفات	File Transfer Protocol (FTP)	يهيئ تحميل وتنزيل الملفات عبر الإنترنت
المحادثة	Internet Relay Chat Protocol (IRC)	يوفر طريقة للمستخدمين للتحادث في الزمن الحقيقي عبر الإنترنت، تُسمى مجموعات المحادثة في الزمن الحقيقي بالقنوات.
استخدام شبكة المجموعات الإخبارية	Network News Transfer Protocol (NNTP)	منتديات للمناقشة حيث يستطيع المستخدمون وبشكل غير متزامن إرسال رسائلهم وقراءة الرسائل التي جرى إرسالها من قبل الآخرين
شبكة الوب العالمية	Hyper Text Transport Protocol (HTTP)	يقدم ولوج لمستندات مشتركة، برامج قابلة للتنفيذ، وموارد إنترنت أخرى

4.3. الوب كتطبيق مُخدّم/ زبون:

تحول الوب WWW (World Wide Web) إلى التطبيق الأكثر استخداماً من بين تطبيقات الإنترنت. وتعتمد الأغلبية الساحقة من تطبيقات التجارة الإلكترونية على الوب. في تطبيقات كهذه، يُسمى الزبائن بمتصفحي الوب وتُسمى المُخدّمات بمُخدّمات الوب.

يحتاج المتصفحون والمُخدّمات، وكما في تطبيقات زبون/ مُخدّم الأخرى، لما يلي:

1. إيجاد بعضهم البعض، وبالتالي إرسال الاستعلامات وتلقي الإجابات وغيرها؛
2. الاتصال أحدهما بالأخر.

لتلبية هذه الحاجات، جرى إدخال خطة عنونة وبروتوكول يدعى بروتوكول نقل النصوص التشعبية HTTP (Hyper Tent Transport Protocol) المعتمد على التنسيق القياسي لعناوين الإنترنت URLs (Universal Resource Locators).

اعتاد المستخدم عموماً على عناوين مثل "www.anywhere.com" التي تمثل عنواناً افتراضياً يعبر في حقيقته عن عنوان كامل هو:

ملف/ دليل/ {بوابة:} اسم المُخدّم//: طريقة الولوج.

حيث يمكن أن تكون طريقة الولوج هي إحدى تطبيقات gopher، أو ftp، أو http أو telnet.

5.3. بروتوكول نقل النصوص التشعبية:

ينتقل المستخدمون من صفحة لأرى بالنقر على الارتباطات التشعبية في الصفحة، حيث يوجد خلف عملية النقر على النص التشعبي، عملية انتقال لفتح نص أو مستند أو تنفيذ عملية على مخدم ما.

عندما يقوم المستخدم بالنقر على تلك الوصلات التشعبية، تأخذ سلسلة من الأفعال مكانها خلف الكواليس. أولا، تطلب الوصلة مُخدّم الوب المحدد في URL الموافق للوصلة. ثم يُصدر المتصفح استعلاما للمُخدّم يطلب فيه المستند الموجود لديه ضمن هذا العنوان، حيث يقوم المُخدّم بإرسال المستند أو الصفحة إلى المتصفح. في هذه النقطة، يعرض المتصفح الصفحة الجديدة ويجري إغلاق الوصلة مع المُخدّم.

من أجل كل استعلام للبروتوكول HTTP يفتح المتصفح وصلة جديدة يجري إغلاقها مباشرة بعد الحصول على المستند المطلوب لتزول العلاقة بين المخدم والمتصفح والتي نشأت بالنقر على الوصلة. يتم توصيف هذا الوضع بالقول أن البروتوكول HTTP لا يستطيع تذكر سلسلة من الطلبات المتتالية والمرتبطة ببعضها البعض وهو لا يحتفظ بتسلسل حالاته (Stateless).

يشكل هذا الأسلوب في العمل مشكلة كبيرة لتطبيقات التجارة الإلكترونية، فالمستخدم ينحو لأن يكون له سلسلة من التفاعلات مع التطبيق. خذ على سبيل المثال حالة المشتري الذي ينتقل من صفحة لأخرى عبر مخزن تسوق افتراضي حيث يختار أغراض متنوعة ليشتريها أثناء انتقاله وذلك من عدة صفحات، وفي كل مرة يضع الأغراض المحددة في عربة تسوق افتراضية، مما يطرح السؤال التالي: إذا لم يكن المُخدّم قادرا على الحفاظ على المعلومات عند الانتقال من صفحة لأخرى، ويقوم بإغلاق الاتصال بعد كل نقرة ونسيان الحالة، فأين وكيف سيجري حفظ محتويات عربة التسوق الافتراضية؟.

طبعاً تم تقديم حلول برمجية عديدة وإضافية تمت على مستوى برمجة تطبيقات الوب، لهذا الإشكال الذي طرحته طبيعة تصميم وتنفيذ بروتوكول نقل النصوص، وهذه الحلول البرمجية ليست في إطار هذا المقرر.

6.3. متصفحات الوب:

سعت النسخ المبكرة من متصفحات الوب لعرض صفحات الوب التي تحوي نصاً ورسوماً بسيطة. يوجد اليوم عدد كبير من متصفحات الوب التي تقدم كل منهما مجموعة من الوظائف والميزات المتنوعة.

7.3. مُخدّمات الوب:

لا نعني بمُخدّم الوب عتاداً (Hardware) بل نظاماً برمجياً. ويوجد عدد كبير من مخدّمات الوب في السوق، الوظيفة الرئيسية لكل هذه البرمجيات هي خدمة HTTP. بالإضافة لذلك تدعم مُخدّمات الوب الوظائف التالية:

- التحكم بالولوج: تحدد من يستطيع الولوج للأدلة أو الملفات الخاصة على مُخدّم الوب؛
- تشغيل النصوص البرمجية والبرامج الخارجية لإضافة وظائف على صفحات الوب أو توفير ولوج لقواعد البيانات والبيانات الديناميكية الأخرى، حيث يجري القيام بذلك من خلال مكتبات برمجية متنوعة؛
- معالجة وإدارة كل من وظائف المُخدّم ومحتويات موقع الوب؛
- تسجيل المناقلات التي يقوم بها المستخدمون. توفر ملفات المناقلة هذه البيانات التي يمكن تحليلها إحصائيا لتحديد الصفة العامة للمستخدمين (مثال، ما المتصفحات التي يستخدمونها) والمحتوى الذي نال اهتمامهم.

4. أمن الإنترنت:

يُذكر الأمن كعقبة رئيسية للتجارة الإلكترونية، حيث يخشى المشترون، مثلاً، من إرسال معلومات بطاقة الاعتماد عبر الوب. يقلق المشترون من إساءة المخترقين (Hackers) لأنظمتهم. بينما تقوى الحاجة للأمن عند انتقال الشركة إلى شركة تجارة إلكترونية تقوم بمناقلات مالية عبر الوب.

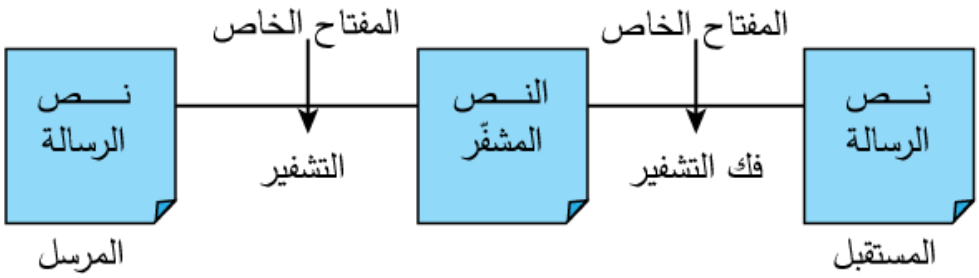
حدد NCSA (National Computer Security Association) أربعة أحجار زاوية لأمن التجارة تضمنت ما يلي:

- التحقّق (Authenticity) – هل لمرسل الرسالة (زبون أو مُخدّم) الحق بذلك؟ إن الوسائل الأساسية للتحقق من شخصية المستخدم في TCP/IP هي كلمة المرور، ولكن يمكن التنبؤ بكلمة المرور واعتراضها.
- الخصوصية (Privacy) – هل محتويات الرسالة سرية ومعروفة فقط للمرسل والمستقبل؟ يمكن أن تحدث عمليات خرق الخصوصية خلال وبعد فترة الإرسال. حالما يجري استقبال الرسالة، يجب على المرسل أن يتأكد بأن المحتويات بقيت خاصة.
- التكاملية (Integrity) – هل جرى تعديل محتويات الرسالة (بشكل مقصود أو عرضي) خلال الإرسال؟ إذ يرسل TCP/IP رزم البيانات في نصوص وتمر الرزم التي تعود إلى رسالة معينة على عدد من الموجهات والخطوط عند انتقالها من الزبون إلى المُخدّم وبالعكس، فهي عرضة للالتقاط والتعديل في الطريق.
- عدم الرفض (Nonrepudiation) – هل يستطيع مرسل الرسالة أن ينفي أنه قد أرسل الرسالة فعليا؟ إذا طلبت سلعة من خلال كتالوج الطلب البريدي وجرى دفع ثمنها بواسطة شيك فإنه من الصعوبة التشكيك في صدق الطلب. على نحوٍ مشابه، إذا كنت تستخدم كتالوج موقع الوب وتدفع بواسطة بطاقة ائتمان، تستطيع عادة أن تعترض على تحرير الطلب على الرغم من أن ملف سجل الولوج الذي ينشئه ويحدثه المُخدّم بشكل تلقائي قد سجل عنوان إنترنت المرسل. إن مفتاح عدم الرفض هو التوقيع والذي يجعل مسألة التشكيك صعبة.

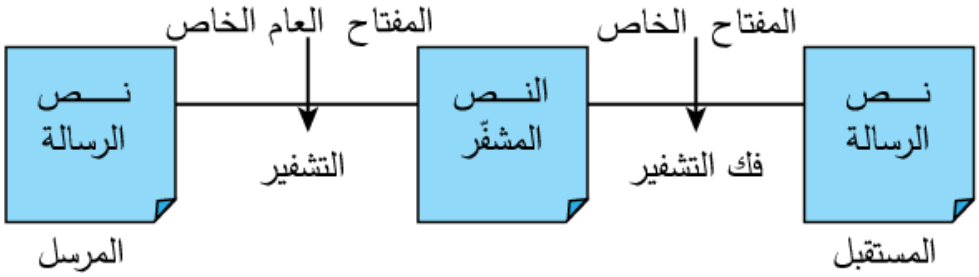
بالنتيجة، يتطلب الحفاظ على أمن التجارة الإلكترونية أن تكون أحجار الزاوية آمنة. يعني ذلك في حدوده الدنيا بأنه يجب حماية خصوصية البيانات والرسائل، يجب التحقق من الشخصيات وأن تكون الشخصيات قابلة للتحقق، ويجب التحكم بالولوج غير المسموح به.

5. التشفير:

- التشفير بالمفتاح الخاص والمتزامن:



- التشفير بالمفتاح العام:



توجد طريقة واحدة للتأكد من سرية وخصوصية الرسائل وهي التأكد من أنه حتى لو وقعت الرسالة بين أيدي الشخاص الخاطئين فإنها لن يتمكنوا من قراءتها. هذا ما يقوم به التشفير Cryptography. يعود علم التشفير لأيام الإغريق، وتعتمد أنظمة اليوم على صيغ رياضية معقدة وخوارزميات حاسوبية، لكن بغض النظر عن مستوى التعقيد، يعتمد التشفير على أربعة أجزاء رئيسية:

1. النص الصرف (Plain text) – الرسالة الأصلية القابلة للقراءة بواسطة الإنسان
2. النص المشفّر (Cipher text) – وهي رسالة النص بعد أن تشفر بصيغة غير قابلة للقراءة
3. خوارزمية التشفير – تستخدم صيغة رياضية لتحويل النص الصرف إلى نص مشفّر والعكس بالعكس
4. المفتاح – يُستخدم المفتاح لتشفير وفك تشفير الرسالة. تنتج المفاتيح المختلفة نصوص مشفّرة مختلفة عند استخدامها مع الخوارزمية نفسها.

لا يقوم التشفير بتشفير النصوص الصرفة فحسب ولكن يشفّر أيضاً المعلومات ذات الأنماط الخاصة كالفيديو، والصوت، والبرجيات من أجل الإرسال الآمن عبر الإنترنت.

يمكن استخدام عدة خوارزميات لتشفير الرسائل. حتى لو كانت الخوارزمية معروفة، تبقى الرسالة غير معروفة طالما المفتاح غير معروف. لكن السهل التنبؤ بالمفتاح من خلال حاسوب يجرب كل الإمكانيات حتى يجري فك تشفير الرسالة، وهذا ما يفسر أن طول المفتاح هو العامل الأساسي لأمن الرسالة. فإذا كان طول المفتاح 4 بت

(مثلا 0101)، سيكون هناك 16 إمكانية (2 مرفوعة للقوة 4) لقيمة المفتاح. وإذا كان طول المفاتيح 56 بت (2 مرفوعة للقوة 56) فهناك تقريباً 72 كادرليون إمكانية.

كانت الحواسيب سابقاً غير قادرة على كسر المفاتيح رغم إمكاناتها الكبيرة. أما اليوم، فتستطيع الحواسيب عالية السرعة تجريب ملايين الاحتمالات بالثانية. ويجرى تسريع الحواسيب أيضاً باستخدام المعالجات التفرعية (Parallel Processors) حيث يعمل كل معالج على جزء أصغر من المفاتيح الممكنة. ويعتمد الطول الفعلي للمفتاح على عوامل متنوعة.

كانت خوارزميات التشفير تاريخياً متناظرة وهذا يعني بأن المفتاح نفسه يستخدم لتشفير وفك تشفير الرسالة أي أن على المرسل والمستقبل الاتفاق سلفا على المفتاح. يُسمى تشفير المفتاح المتناظر أيضاً بالتشفير بالمفتاح الخاص. يوجد تنوع واسع في خوارزميات التشفير المتناظر. كانت الخوارزمية الأوسع استخداما هي خوارزمية DES والتي أجاز استخدامها المعهد الوطني للمعايير والتكنولوجيا NIST (National Institute of Standards and Technology) وذلك من أجل استخدامها مع المستندات الحكومية غير المصنفة. وظفت DES مفاتيح بطول 56 بت. أثناء استخدام DES جرى ابتكار خوارزميات أخرى بسبب تأثرها بالحوسبة السريعة. تصل أطوال مفاتيح الشيفرة فيها الآن إلى 2.048 بت.
توجد صعوبة واحدة في التشفير بالمفتاح المتناظر أو المفتاح الخاص وهي الحاجة لإرسال العديد من الرسائل بين المستخدمين أو بين المستخدمين والمخدمات لتبادل المفاتيح المتناظرة. وفب حال مخدمات الوب يزداد الأمر صعوبة مع الحاجة لتوزيع مفتاح المُخدّم الخاص على الآلاف من المستخدمين، فلا يوجد أي طريقة تحفظ سرية المفتاح لمدة طويلة. لهذه الأسباب، جرى ابتكار نوع جديد من الخوارزميات، تسمى التشفير بالمفتاح العام وذلك في العام 1976.

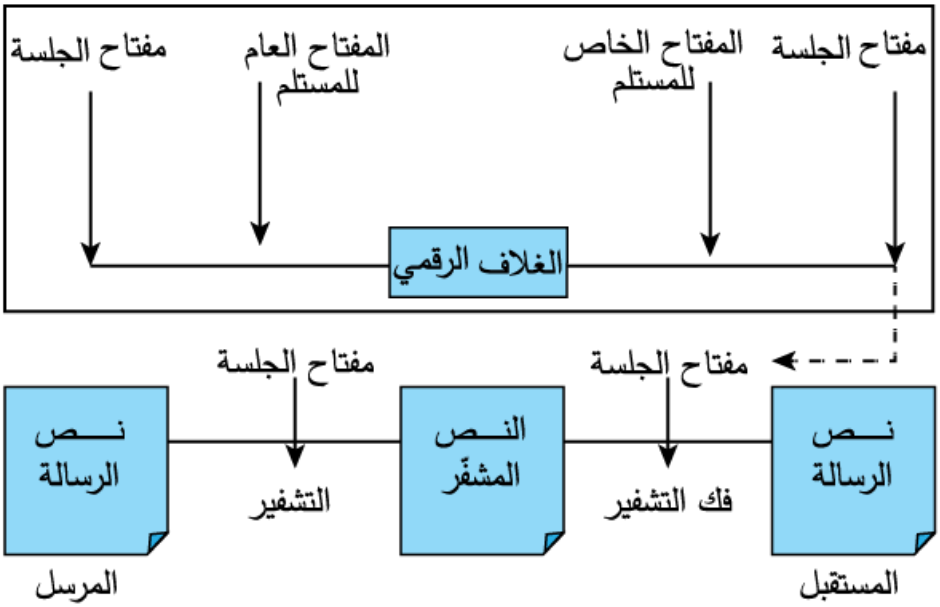
يعرف التشفير بالمفتاح العام أيضاً بالتشفير غير المتناظر، حيث يستخدم زوجا من المفاتيح – واحد عام واحد خاص. المفتاح العام متاح لأي شخص يريد إرسال رسالة مشفرة لحامل المفتاح الخاص. الطريقة الوحيدة لفك تشفير الرسالة تجري باستخدام المفتاح الخاص. بهذه الطريقة، يمكن إرسال الرسائل بدون الاتفاق سلفا على المفاتيح.

المشكلة الرئيسية في خوارزميات المفتاح العام هي البطئ. تُعتبر الخوارزميات المتناظرة أسرع من خوارزميات المفتاح العام نسبياً لأنها تتطلب مفاتيح أقصر. وهذا هو سبب استخدام الربط بين التشفير بالمفتاح العام والتشفير المتناظر مع تطبيقات العالم الحقيقي. يُعرّف الربط بين التشفير بالمفتاح العام والتشفير المتناظر بالغلاف الرقمي (Digital Envelope). الفكرة الأساسية هي استخدام التشفير بالمفتاح العام لإنشاء وإرسال مفتاح متناظر لمستقبل الرسالة. ثم يستخدم المفتاح المتناظر لتشفير وفك تشفير الرسالة.

6. التوقيع الرقمي:

1.6. مقدمة:

يشكل موضوع ضمان العقد الصحيح بين الطرفين واحدة من أهم القضايا التي يجب معالجتها في معاملات التجارة الالكترونية. ويعتبر تقييم صحة العقود في بيئة الانترنت أمراً غير معقد، كون العقود لا تكون ورقية مما يجعل أمر التقييم أسهل.



ولذلك تعتبر التواقيع الرقمية ضرورية للمساعدة في تعزيز التجارة الالكترونية لأنها تضمن دخول جميع الأطراف في اتفاق تعاقدي ملزم.

ويحدد استخدام تقانة التوقيع الرقمي بوضوح الأدلة اللازمة لسلامة العقد الالكتروني، فإذا قام أي طرف بتغيير أي جانب من جوانب وثيقة موقعة رقمياً، فإن عملية التحقق من صحة التوقيع الرقمي سوف تحدد فيما إذا تم تغيير الوثيقة منذ توقيعها، أو إذا لم يتم توقيعها من قبل الطرف الذي يدعي بأنها موقعة.

2.6. تعريف التوقيع الرقمي:

تعتبر قضية التواقيع الرقمية قضية مركزية لمشروع على شبكة الانترنت، لأنها تسمح لكل من المستهلكين والشركات بالدخول في اتفاقيات ملزمة عبر شبكة الانترنت. تحتاج المشاريع عبر الانترنت لضمان موثوقية ونزاهة وسرية توقيع الموقعين الذين يستخدمون هذه المشاريع عبر الانترنت، حيث أن طريقة تقديم أحد هذه المشاريع لنفسه على شبكة الانترنت تشكل مصدر قلق بالغ الأهمية. وتعتبر عملية تقييم صحة العقود أو الاتفاقات التي دخلت إلى الانترنت أمراً معقداً، نظراً لطبيعة الصفقة التي لا تعتمد على الورق، ولذلك كان من الضروري وجود معايير تم وضعها لضمان أمن ووثوقية التواقيع الرقمية.

يمكن تعريف التواقيع الرقمية بحسب قانون التجارة العالمية والوطنية، بأنه ختم أو رمز أو عملية إلكترونية مرتبطة منطقياً بعقد أو تقرير، وتكون منفذة أو معتمدة من قبل شخص على شبكة الانترنت بقصد التوقيع على العقد. ويكون للتوقيع الالكتروني بموجب هذا القانون قوة القانون نفسها لما يعادلها من توقيعات بخط اليد، وفي المقابل تكون التواقيع الرقمية محددة بدقة لتشمل التواقيع التي تستخدم آليات التشفير أو الترميز. ولا يحتوي التوقيع الرقمي خلافاً للتوقيع التقليدي على ترسيخ اسم شخص ما بالاعتماد على الحبر فوق قطعة من الورق.

3.6. آلية عمل التواقيع الرقمية:

تنطوي التواقيع الرقمية عادةً على استخدام تقانة التشفير. وتُعتبر أهم تقانات التشفير التي قد تستخدم للتوقيعات الرقمية هي التقانات المعتمدة على آليات التشفير غير المتناظر باستخدام المفتاح العام والمفتاح الخاص.

وينطوي هذا النوع من التشفير مزدوج المفتاح على الخطوات التالية:

الخطوة الأولى: يقوم الموّقع الذي يسعى للدخول في اتفاقية بتوليد مفتاحه الخاص ويمكن تخزين المفتاح الخاص على جهاز الحاسوب الخاص بالمستخدم ويتم الوصول إليه من خلال كلمة سر، ويعتبر هذا التوقيع الذي يتم توليده من خلال المفتاح الخاص، رقماً تم إنشاؤه بواسطة خوارزميات عددية.

الخطوة الثانية: يقوم الموّقع أيضاً بتوليد المفتاح عام والمفتاح خاص بنفس الآلية بحيث يمكن لأي وثيقة تم تشفيرها أو توقيعها بالمفتاح الخاص، أن يتم فك تشفيرها بالمفتاح العام أو العكس. ويتوفر المفتاح العام على نطاق واسع لكل من يريد المصادقة على الوثائق التي تم توقيعها من قبله.

الخطوة الثالثة: عندما يقوم الموقّع بتشفير الرسالة أو جزء من معلوماته بمفتاحه الخاص ويقوم بإرسالها، يتم استخدام المفتاح العام من قبل المتلقي لفك التشفير وللتحقق من أن الرسالة تعود للشخص نفسه، كما يمكن استخدامه للتحقق من أن الرسالة التي تم استلامها مطابقة بالضبط للرسالة المرسلة، وطوال عملية تحديد الهوية هذه لا يتم كشف الهوية الفعلية للموّقع، ويكون الهدف هو التحقق من توافق المفتاح الخاص مع العام الذي يتم استخدامه من قبل المستقبل حتى يتأكد من مصدر الرسالة.

الخطوة الرابعة: يمكن استخدام سلطة تصديق لضمان دقة المفاتيح العامة والخاصة، وتكون وظيفة السلطة هي إثبات وثوقية المفاتيح، وتقوم سلطة التصديق بإصدار شهادة تضمن بأن حامل المفتاح العام هو نفسه حامل المفتاح الخاص. عندها يتوجب على الموقع أن يرسل الشهادة مع الرسالة الموقعة، ويقوم المستقبل بالتحقق من أن المرسل حقيقي وليس وهمي بالرجوع إلى سلطة إصدار هذه الشهادة.

4.6. التواقيع الإلكترونية وأنواعها:

على الرغم من أن استخدام مفتاح التشفير الخاص والعام هو أحد أكثر أنواع التواقيع الرقمية التي تم البحث فيها شيوعاً، إلا أنه يوجد هناك طرق أخرى من التواقيع التي يمكن استخدامها، وغالباً يمكن تمييز هذه الأنواع من خلال الإشارة إليهم بالتواقيع الإلكترونية بدلاً من التواقيع الرقمية، ولا تنطوي هذه التواقيع على استخدام مفتاح التشفير العام والخاص.

وفيما يلي بعض الأمثلة عن التواقيع الإلكترونية:

1. البطاقة الذكية التي يتم تمريرها من خلال جهاز الحاسوب الخاص بالمستخدم (تحتوي البطاقة الذكية على معلومات عن المستخدم يمكن التحقق منها)
2. كلمات السر
3. إرسال صور عن توقيعات بخط اليد عبر البريد الالكتروني
4. التواقيع على المنصات الرقمية باستخدام التقانة الحيوية (قزحية العين)

ويكون استخدام هذا النوع من التقانات مفيداً أيضاً للشركات على شبكة الانترنت، لأنه يساعد على ضمان نزاهة المعاملات، ويتم اعتماد تقانة محددة غالباً وفقاً لتشريعات معينة والتي يجري تمريرها في الحالة المحددة ضمن اختيار حكم القانون، وذلك لأن العديد من هذه القوانين تحد من تطبيقها على أنواع معينة من تقانة التوقيع الرقمي.

5.6. القيود التقنية / القانونية للتواقيع الرقمية:

يوجد قيود تقنية وقانونية لاستخدام التواقيع الرقمية على حد سواء.

تنطوي بعض القيود التقنية على التأكد من أن تقانة التشفير المستخدمة آمنة من التزوير والإختراق، وقد لا يتم نشر المفاتيح العامة في موقع مركزي مناسب، بل تكون مبعثرة بين سلطات التصديق المختلفة، وقد لا تكون سلطات التصديق هذه مرخصة، أو من جهة أخرى ألا تكون منظمة لحماية المستهلك، بالإضافة إلى أن الانتقال إلى نظام التواقيع الرقمية يتطلب كثير من الوقت والموارد على حد سواء، من جانب كل من الموّقع والمتلقي.

وقد يكون الموّقع في كثير من الحالات هو نفسه المستهلك الذي سيحتاج للإستثمار في بعض برامج التشفير، والدخول في اتفاق مع سلطة التصديق، ويكون استخدام التواقيع الرقمية التي تنطوي على تقانة التشفير أبطأ فيما إذا كانت تكاليف هذه الخدمات غالية، بالمقارنة مع استخدام أنواع أخرى من التواقيع الإلكترونية التي تنطوي على البطاقات الذكية أو كلمات السر.

كان عام 2000 بمثابة علامة فارقة في القضاء على العديد من القيود القانونية التي تعيق التواقيع الرقمية، ومع مرور التواقيع الإلكترونية في قانون التجارة العالمي والوطني في 30 حزيران من عام 2000، تم الإعتراف بالوضع القانوني للتواقيع بإعتبارها ملزمة بموجب قانون الولايات المتحدة الأمريكية.

ولا يمكن التقليل من أهمية القوانين المختلفة التي صدرت من قبل المجالس التشريعية للولايات، على الرغم من أهمية القانون الإتحادي (الفيدرالي)، وقد انطوت هذه القوانين أيضاً على موضوع التواقيع الإلكترونية.
وتعتبر معالجة الخلافات الحالية الموجودة في قوانين الولاية أمراً مهماً، أن العديد من الولايات تفرض متطلبات مختلفة من أجل مطابقة التواقيع الإلكترونية.

6.6. أهمية التواقيع الرقمية:

تعتبر التواقيع الرقمية ضرورية لحماية موثوقية ونزاهة وخصوصية المعاملات عبر الانترنت، وتحتاج الشركات على الانترنت إلى ضمان حصولهم على معلومات دقيقة وقابلة للتحقق، بخصوص الشخص الذي يحاول استخدام خدماتها، حيث أن إحدى أهم المشكلات التي تواجه هذه الشركات هي التزوير والاحتيال.
وتسعى هذه الشركات من خلال استخدام بعض أنواع تقانات التوقيع الرقمي إلى حماية خدماتهم أو بضائعهم، التي يتم الحصول عليها عن طريق الاحتيال.
وعلى الرغم من أن موضوع التشفير غير المتناظر وكونه الوسيلة الأفضل أو الأكثر جدوى لتحقيق هذا الأمن لا يزال موضوعاً خلافياً، تحتاج الشركات على شبكة الانترنت إلى تحقيق واستثمار شكل من أشكال تقانة التوقيع الرقمي أو الإلكتروني من أجل حماية نفسها.
وتحمي تقانات التوقيع الرقمي المستهلكين أيضاً، وتوفر لهم حماية مشددة، بحيث يتم حماية معلوماتهم من خلال مفتاح خاص (أو بعض التقانات الأخرى)، والتي يعرفها الموّقع فقط، وبالتالي حماية المستهلكين من أن يكونوا ضحايا لسرقة الهوية.

7. الشبكات الخاصة الافتراضية Virtual Private Network:

لنفترض أن شركة ترغب بتزويد الموظفين البعيدين أو الجوالين بولوج آمن لبيانات الشركة والتي يجري الولوج لها بشكل طبيعي من خلال شبكة LAN. توجد بعض البيانات في صفحات الوب، ولكن معظم البيانات موجودة في ملفات معيارية (مثل ملفات Word) وأنظمة معلومات الشركة (مثل قواعد البيانات الكبيرة المترابطة). تقليدياً، يلج العمال البعيدون أو الجوالون من خلال بنك من المودمات (Modems) أو مُخدّم RAS (Remote Access Server) للولوج البعيد والذي يسمح لهم بالاتصال بشبكة محلية LAN (Local Area Network) عبر الخطوط الهاتفية. فرصة استراق السمع أثناء النقل معدومة ولكنها طريقة مكلفة للقيام بالعمل بسبب تكاليف الاتصالات الهاتفية بعيدة المدى. يوجد بديل أقل كلفة وهو الشبكة الخاصة الافتراضية VPN (Virtual Private Network).

تربط VPN بين التشفير، والمصداقية، وبروتوكول فتح أقنية خاصة (Tunneling) لتوفير نقل آمن للاتصالات الخاصة عبر الإنترنت العامة حيث تصبح الإنترنت وكأنها جزء من مشروع شبكة WAN (Wide Area Network) أكبر. تنخفض بهذه الطريقة تكاليف النقل بشكل كبير لأن الموظفين يستطيعون الولوج لبيانات الشركة بالقيام باتصال محلي إلى ISP بدلا من القيام باتصال بعيد المسافة. يمكن أن يكون التوفير كبيراً إذا اعتمد الموظفون على ISPs بمعدلات رسوم أخفض بدل الاتصال بشبكة. بالإضافة إلى ذلك ومن أجل دعم الموظفين البعيدين والجوالين، يمكن استخدام VPNs أيضاً لدعم اتصال موقع – إلى – موقع. مثلاً، يمكن وصل المكاتب الفرعية بمراكز القرار المشتركة من خلال أنفاق تنقل الاتصالات عبر الإنترنت. بشكل مشابه، يمكن وصل الشركة بمزوديها وموزعيها بواسطة VPN وبالنتيجة توفر إكسترانت آمنة. مرة أخرى، يمكن أن يكون توفير التكاليف كبيراً، خاصة إذا كانت المكاتب الفرعية، والمزودون، أو الموزعون موجودون حول العالم.

التحدي الحقيقي لشبكة VPN هو التأكد من وثوقية وسلامة البيانات المرسلة عبر الإنترنت، من خلال القناة المفتوحة. عند فتح القناة، يجري أولا تشفير البيانات ثم تجري تجميعها في رزم يمكن إرسالها عبر الإنترنت. يجري فك تشفير الرزم المشفرة بواسطة مضيف أو موجه خاص في العنوان الهدف. يدعم بروتوكول فتح القناة أيضاً الشبكة متعددة البروتوكولات.

يمكن استخدام بروتوكولات متنوعة لتنفيذ عملية فتح القناة. حتى هذه اللحظة لا يوجد معيارٌ متفق علية. وبدلا من ذلك يوجد بروتوكولات متنافسة.

8. متطلبات إنشاء المخازن الإلكترونية:

توفر بروتوكولات الإنترنت ومتصفحات الوب ومُخدّمات الوب التجارية، والتشفير، أساساً لإنشاء مواقع الوب التي تستطيع بسهولة دعم التسويق والفعاليات الخدمية.

عموماً، يجب أن يدعم المخزن الإلكتروني المهمات والخطوات نفسها التي يدعمها المخزن المادي (الفيزيائي). إذا يحتاج المخزن الإلكتروني لأن يقدم للمشتري القدرة على:

- الاكتشاف والبحث عن، ومقارنة المنتجات من أجل الشراء
- تحديد المنتج الذي سيجري شراؤه والمفاوضة أو تحديد سعره الكلي
- التقدم بطلب لشراء المنتجات المرغوبة
- تأكيد طلب الشراء، والتأكد من صلاحية المنتج المرغوب
- دفع ثمن المنتجات التي جرى طلبها (غالباً على شكل ائتمان)
- التحقق من الائتمان ومن المصادقة على الشراء
- معالجة الطلبات
- التحقق من شحن المنتج
- الاستعلام عن دعم الدفع البريدي أو توفير تغذية خلفية للبائع

بهدف توفير هذه القدرات، يجب على المخزن الإلكتروني أن يحتوي على ثلاثة أنظمة مترابطة على الأقل:

- واجهة لإضافة المنتجات، والأسعار، والمساعدة في الترويج
- نظام مناقلات لمعالجة الطلبات وعمليات الدفع وأنشطة المناقلة الأخرى
- بوابة دفع توجه عمليات الدفع بشكل رئيسي من خلال الأنظمة المالية الموجودة

يملك تجار الوب وبشكل مماثل التجار التقليدين عدد من الخيارات لإنشاء وتشغيل المخازن الإلكترونية. السؤال الأول الذي يوجهه التاجر هو هل سيتعاقد مع شركة خارجية لإنشاء وتشغيل المخزن الإلكتروني أو هل سيقوم ببنائه وتشغيله داخلياً. يعتمد الخيار على عوامل مثل حجم الشركة، وتجربتها السابقة على الوب وفي التجارة الإلكترونية وقدرات موظفي IT في الشركة.

تجري خدمة الشركات صغيرة ومتوسطة الحجم والتي تملك القليل من موظفي المعلوماتية وذات الميزانيات الصغيرة، بشكل جيد بواسطة متعاقدين خارجيين. أثبت المتعاقدون الخارجيون أيضاً بأنهم خيار جيد للشركات الكبيرة التي ترغب *بتجربة* التجارة الإلكترونية بدون توظيف استثمارات ضخمة كبيرة، لحماية شبكاتهم الداخلية، أو الاعتماد على الخبراء لتأسيس مواقع والتحكم بها لاحقا. يجري تشغيل بعض مواقع B2C الأكثر شهرة على الوب بواسطة بائعي طرف – ثالث. يوجد ثلاثة أنواع من المزودين الذين يقدمون خدمات لإنشاء وتشغيل المخازن الإلكترونية:

1. مخازن الإنترنت الكبيرة (Internet malls). يوجد أكثر من 3.000 مخزن على الوب. يتألف مخزن الإنترنت مثله مثل المخزن الحقيقي من مخزن واحد للدخول إلى مجموعة من المخازن الإلكترونية. بالمقارنة مع المخازن السيبرية المبكرة، تملك مخازن اليوم هيئة وإحساس مشترك. يقدم المخزن جيد التشغيل بيع مختلط من مخزن لآخر ويوفر بنية دفع مشتركة حيث يستطيع المشترون استخدام بطاقة ائتمان واحدة لشراء المنتجات من عدة مخازن. نظرياً، يقوم المخزن الكبير بتسويق أوسع من الموقع الثابت، بالنتيجة، توليد حركة أكبر. الجانب السلبي هو وجوب المشاركة بالدخل مع مالك المخزن. تتنوع مخازن الإنترنت في الأحجام والأشكال والأنواع كالمخازن الإقليمية والمخازن التخصصيه وتختلف أجورها من استضافة وصيانة الخدمات وغيرها.

2. مزودو خدمة الإنترنت (Internet Service Providers). بالإضافة إلى تزويد الشركات والأفراد بالولوج للإنترنت، يقدم عدد كبير من ISPs خدمات استضافة للتجارة الإلكترونية. يركز ISPs وبشكل كبير على تشغيل بيئة مناقلات آمنة وليس على محتوى المخزن. هذا يعني بأنه يجب على التجار الذين يستخدمون خدمات ISPs الاستمرار في تصميم الصفحات الخاصة. مرة أخرى، يمكن توكيل هذه المهمة إلى طرف ثالث.

3. شركات الاتصالات (Telecommunication Companies). وسعت شركات الاتصالات الكبرى وبشكل متزايد خدماتها في الاستضافة لتشمل مجال حلول التجارة الإلكترونية الكامل. على الرغم من وجود شركات الاتصالات ومن كل الأحجام، إلا أن التركيز يكون على الشركات الكبيرة التي تستخدم خدماتها في الاتصالات بعيدة المسافة.

على الرغم من وجود عدد من التعقيدات التسويقية والتقنية المرفقة ببناء وتشغيل مخزن الصدارة الإلكتروني، إلا أن معظم الشركات اختارت القيام بذلك بنفسها. يجب أن يجري توجيه تطوير المخزن الإلكتروني وفقا للممارسة وللمعايير المعلوماتية الموجودة في الشركة..

9. المحادثة على الوب:

تجاهلت معظم الشركات الربح الاقتصادي المحتمل من الاتصالات على الوب. باستثناء البريد الإلكتروني، وجرى التعامل مع الإنترنت والوب كوسط إرسال ضيق مع تدفق للمعلومات باتجاه واحد (سحب من قبل المستخدم النهائي أو دفع المعلومات له). لكن الشركات بدأت لاحقاً بإدراك أن الإنترنت والوب تقدمان القدرة على إشغال الزبائن في حوار وعلى إنشاء مجتمعات افتراضية يستطيع الزبائن من خلالها الاتصال بعضهم ببعض وتأسيس وتعزيز الاتصال بين الناس.

تُستخدم اليوم منتديات الوب ومجموعات المحادثة والشبكات الاجتماعية لأهداف متنوعة في التجارة الإلكترونية. منتديات الوب مكافئة لمجموعات Usenet الإخبارية (ولكن بواجهة أفضل)، ومجموعات المحادثة مشابهة إلى الـ IRC (Internet Relay Chat). جرى تصنيف الاستخدامات المتنوعة لهذه المنتديات ومجموعات المحادثة بالطريقة التالية:

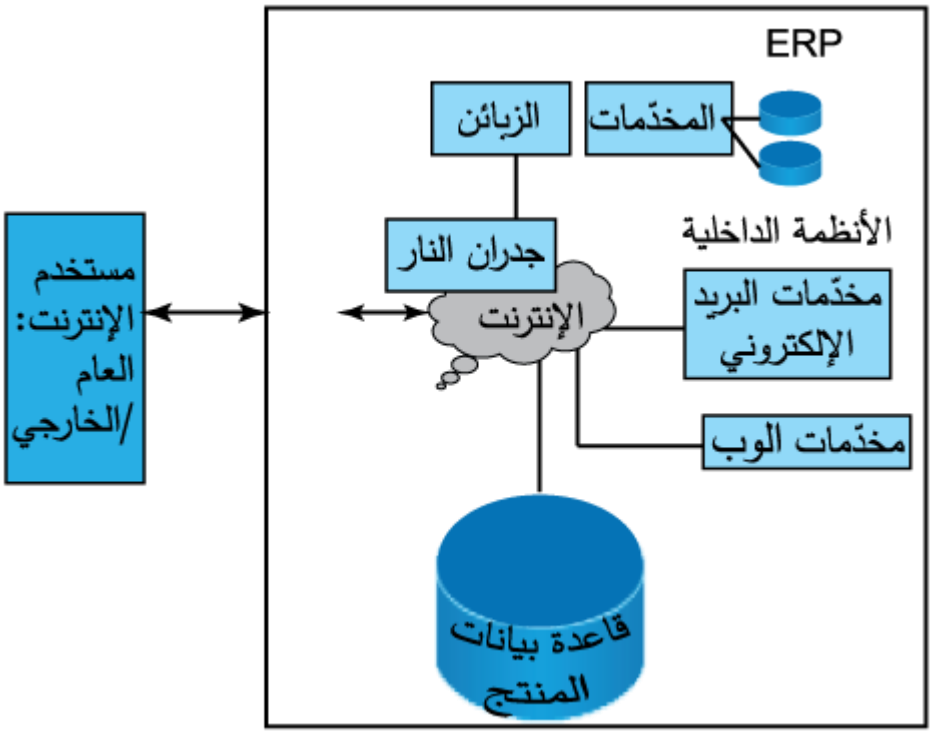
- مراكز الاتصال – الشركات التي وظيفتها الرئيسة تأمين مكان لقاء افتراضي حيث يمكن إجراء الاتصالات بين المشاركين. يجري توليد العائد من خلال رسوم الاشتراك أو عوائد الإعلان.
- خدمة الزبون – يقدم العديد من المواقع الدعم لخدمة الزبون على الوب حيث يستطيع الزبائن التحادث مع موظفي المساعدة على الخط (Help–Line) والتحادث مع الزبائن الآخرين. يتركز معظم النقاش حول الأسئلة عن المنتج، المشاكل، والنصائح. جرى تصميم معظم مراكز الدعم على الوب كمنتديات أكثر منه كمجموعات محادثة.
- نقاش اجتماعي – توفر عدة مواقع تجارة إلكترونية منتديات وخدمات محادثة وفق نظرة تسويقية باتجاه تطوير مجتمع من المستخدمين الأوفياء، التابعين والمدافعين. تشكل المنتديات التي يوفرها العديد من شركات الاستثمار المالية على الوب مثالاً جيداً لهذه الاستراتيجية.

من وجهة نظر تقنية، فإنه من الممكن بالنسبة لشركة أن تؤسس مجموعاتها الإخبارية الخاصة بها أو مُخدّم IRC بهدف توفير منتدى أو مجموعة محادثة على الوب. المشكلة هي أن هذه التسهيلات تتطلب زبائن خاصين وكذلك مُخدّمات خاصة، وتكامل شفاف على الوب. كما أن الطبيعة غير المتزامنة في "خزن – و – توجيه" المنتدى، تجعل بالإمكان إنشاء لوحة إعلانية حيث يمكن خزن تشكيلات من الرسائل حول مواضيع خاصة وذلك في قاعدة بيانات، ويمكن تحويلها ديناميكياً إلى صفحات HTML للإجابة على استعلامات المستخدم.

بسبب الصعوبات التقنية المرافقة لتنفيذ كل من منتديات الوب ومجموعات المحادثة، يوفر عدد من البائعين البرمجيين الآن أنظمة مصممة فقط لهذه الأهداف. تُعتبر المنتجات التي تدعم المحادثة في الزمن الحقيقي مختلفة قليلاً. تستخدم معظم المنتجات متصفح الوب كهيكل وتعتمد على برامج خاصة كواجهة للزبون. يمكن لهؤلاءالاتصال مع مُخدّم الوب بواسطة HTTP أو من خلال مع مُخدّم IRC عبر بروتوكول IRC.

10. الإنترانت:

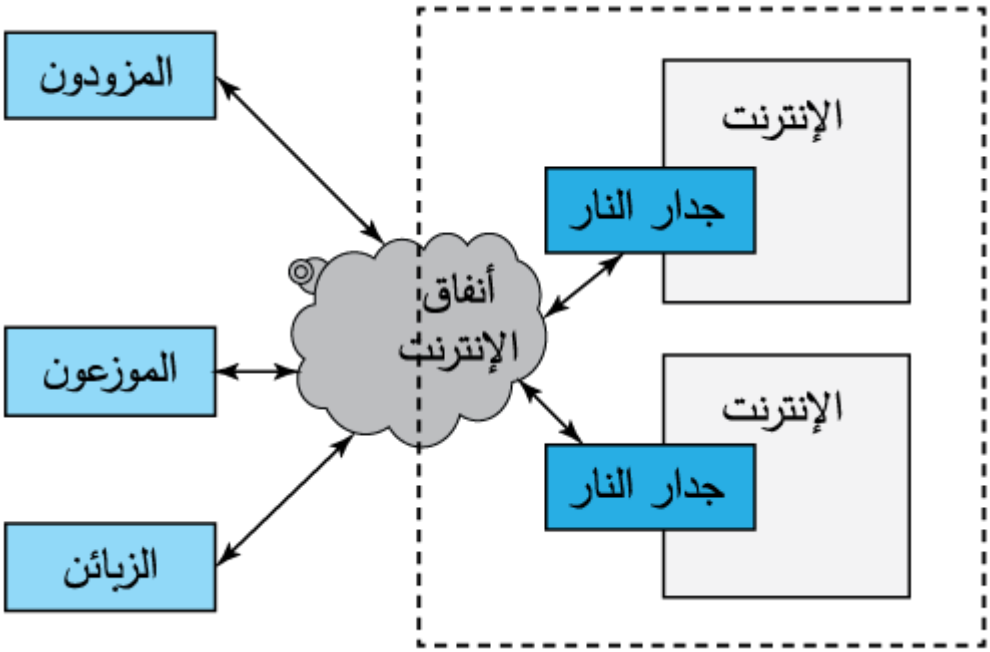
الإنترانت هي شبكة LAN مشتركة أو شبكة (WAN) محيطيه، تستخدم تكنولوجيا الإنترنت خلف مخدمات الحماية الخاصة بالشركة. تربط الإنترانت بين مُخدّمات متنوعة، وزبائن، وقواعد بيانات، وبرامج تطبيقية مثل ERP (Enterprise Resource Planning).



على الرغم من أنه قد جرى تطوير شبكات الإنترانت على البروتوكول نفسه الذي جرى تطوير الإنترنت عليه وهو TCP/IP إلا أنها تعمل كشبكة خاصة بولوج محدود حيث يستطيع الموظفون المفوضون فقط استخدامها. تقتصر شبكات الإنترانت على المعلومات ذات الصلة الوثيقة بالشركة وتحوي على معلومات حصرية وغالباً ما تكون المعلومات مملوكة وحساسة. تحمي جدران النار (وهي عبارة عن برمجيات و/ أو عتاد يسمح للمستخدمين الخارجيين الذين لديهم تصاريح محددة بالولوج للشبكة المحمية) شبكات الإنترانت من الولوج الخارجي الغير مسموح له؛ يمكن استخدام الإنترانت لتعزيز الاتصال والتعاون بين الموظفين المفوضين، والزبائن، والمزودين، وشركاء العمل الآخرين. يجري الولوج إلى الإنترانت عن طريق الإنترنت، وبسبب ذلك، لا تتطلب الإنترانت استئجار شبكات إضافية. توفر شبكات الإنترانت البنية التحتية للعديد من التطبيقات التجارية للشركة المحيطية.
نحتاج عند بناء شبكة إنترانت إلى مُخدّمات وب، ومتصفحات، وأدوات نشر على الوب، وقواعد بيانات خلفية، وشبكات TCP/IP (WAN أو LAN)، وجدران نار.

11. الإكسترانت:

تستخدم الإكسترانت أو "الإنترانت الموسعة" بروتوكول شبكات الإنترنت TCP/IP لربط شبكات الإنترانت المتواجدة في مواقع مختلفة كما هو موضح في الشكل الموجود في الشريحة. ويجري عادةً قيادة عمليات الإرسال على الإكسترانت عبر الإنترنت التي تقدم خصوصية أو أمن إرسال أقل، لذلك نجد من الضروري عند استخدام الإكسترانت تحسين أجزاء الربط مع الإنترنت حيث يجري ذلك بإنشاء أقنية ربط لتدفق البيانات بشكل أمن باستخدام خوارزميات التفويض والتشفير وفك التشفير (Cryptography).



تُعرف الإنترنت المزودة بتكنولوجيا الأقنية (Tunneling) بالشبكة الخاصة الافتراضية VPN (Virtually Private Network). توفر شبكات الإكسترانت اتصال آمن بين شبكات إنترانت الشركات وبين شبكات شركائها في العمل، ومزودي المواد، والخدمات المصرفية، والحكومة، والزبائن، وغالباً ما يكون الولوج لشبكات الإكسترانت مقيداً باتفاقات الأطراف المشتركة وهو متاح ومتحكم به فقط من قبل أشخاص مفوضين. تسمح البيئة المحلية في الإكسترانت، للمجموعات بالتعاون، والمشاركة بالمعلومات حصراً وتبادلها بشكل أمن. تُعتبر الإكسترانت منصة مرنة ومفتوحة وآمنة لإدارة سلسلة التجهيز لأنها تسمح بالاتصال بين الشركات من خلال الإنترنت.

يبني العديد من الشركات، لزيادة الأمن، نُسخ طبق الأصل عن قواعد البيانات التي يريدون المشاركة بها مع شركائهم ويفصلونها بشكل ملموس عن شبكات الإنترانت العادية، ولكن حتى البيانات المفصولة تحتاج للحماية حيث يجري توفير هذه الحماية ببنية خاصة.

12. تطبيقات شبكات الإنترانت والإكسترانت:

نعاين تطبيقات شبكات الإنترانت والإكسترانت من وجهات نظر ثلاثة: الوظائف العمومية، مجالات التطبيق، وحلول الإنترانت الصناعية.

1.12. الوظائف العمومية للإنترانت والإكسترانت:

تستطيع شبكات الإنترانت توفير الوظائف العمومية التالية:

- صفحات وب مشتركة فردية / مؤسساتية / تخصصية
- الولوج لقاعدة البيانات: قاعدة بيانات معتمدة على الوب
- محركات البحث والأدلة: تساعد على البحث المعتمد على الكلمات المفتاحية
- الاتصال التفاعلي: المحادثة، الصوت، فيديو عن بعد
- توزيع الوثائق وسير العمل: نسخ وتوجيه الوثائق بالاعتماد على الوب
- العمل الجماعي: لوحة إعلانية وبريد إلكتروني ممتاز
- النظام الهاتفي(Telephony): تُعتبر شبكات الإنترانت قناة مثالية للنظام الهاتفي المعتمد على الحاسوب
- التكامل مع التجارة الإلكترونية: واجهة للمبيعات والمشتريات الإلكترونية المعتمدة على الإنترنت
- ربط الفروع الموزعة جغرافياً، والزبائن، والمزودين بالأجزاء المفوضة في شبكات الإنترانت لجعل الزبائن أكثر سعادة وجعل المزودين أكثر فعالية وتخفيض تكاليف الموظفين

يجري توفير هذه الوظائف لعدد كبير من التطبيقات.

2.12. مجالات تطبيق الإنترانت والإكسترانت:

تتضمن شبكات الإنترانت إجرائيات وخطط، ووثائق تشاركيه، ودليل هاتف مشترك، وموارد بشرية، وبرامج تدريبية، وقواعد بيانات للزبائن، وكتيبات وكتالوجات للمنتجات، ومعلومات لدخول المخزن، وأرشيف مصور، وطلبات شراء، ومجموعة من المشروعات البديلة، وخدمات حجز السفر. نجد أن كلاً من قواعد بيانات الزبائن، والكتيبات والكتالوجات المنتجات، وطلبات الشراء، وخدمات الحجز السفر، تتعلق مباشرة بالشراء والتسويق الإلكتروني.

يمكن وضع شبكات الإنترانت والإكسترانت في موضع التطبيق في المناحي التالية:

- خدمة الزبون
- تعزيز المشاركة المعرفية
- تعزيز قرار المجموعة وإجرائية العمل
- المنظمات الافتراضية
- التوزيع البرمجي

- إدارة الوثائق
- التدريب
- تسهيل معالجة المناقلات
- إلغاء الأعمال المعتمدة على الورق
- دعم العملية الإدارية

3.12. حلول الأعمال المعتمدة على الإنترنت والإنترانت والإكسترانت:

أصبح تطوير نماذج العمل أصبح الشأن الحاسم للنجاح الإداري وساعد استخدام الإنترنت والإنترانت والإكسترانت في تطوير نماذج ناجحة يمكن تصنيفها ضمن:

- الخدمات المالية: العمل المصرفي، وخدمات الوساطة والخدمات المالية الأخرى، والتأمين
- خدمات تكنولوجيا المعلومات
- خدمات التصنيع: الصناعات النفطية والكيميائية، والبضائع الاستهلاكية، والطعام والشراب، والصناعات العامة، والصناعات الصيدلانية
- خدمات البيع بالتجزئة
- خدمات البناء الهندسية، والتعليمية، والبيئية، والعناية الصحية، والإعلامية، والترفيهية، وخدمات الاتصالات، والنقل، والمرافق العامة

13. التمارين:

1. يجري تشغيل الأعمدة الفقرية بواسطة مزودي خدمة الشبكة NSP (Providers Network Service). وتدار شبكات التسليم الفرعية من خلال مزودات خدمة الإنترنت ISP (Internet Service Providers) المحلية والإقليمية
   A. صح
   B. خطأ

2. وتحتوي البروتوكولات التي جرى تصميم الإنترنت عليها على مجموعة من مبادئ التصميم، واحد مما يلي ليس منها:
   A. السرعة
   B. قابلية التشغيل
   C. الطبقية
   D. البساطة

3. يشكل موضوع كيفية ضمان العقد الصحيح بين الطرفين من أهم القضايا التي يجب معالجتها في معاملات التجارة الالكترونية:
   A. صح
   B. خطأ

4. يعرف التشفير بالمفتاح العام أيضاً بالتشفير المتناظر، الذي يستخدم زوجا من المفاتيح – واحد عام واحد خاص
   A. صح
   B. خطأ

5. التوقيع الرقمي هو دمغة الكترونية أو رمز أو عملية ملحقة أو مرتبطة منطقياً بعقد أو تقرير، وتكون منفذة أو معتمدة من قبل شخص على شبكة الانترنت بقصد التوقيع على المحضر:
   A. صح
   B. خطأ

6. تنطوي التواقيع الرقمية عادةً على استخدام تقانة التشفير:
   A. صح
   B. خطأ

7. واحد مما يلي يعتبر من التواقيع الإلكترونية:
   A. البطاقة الذكية
   B. كلمات السر
   C. التواقيع على المنصات الرقمية باستخدام التقانة الحيوية
   D. جميع الإجابات صحيحة

8. تنطوي بعض القيود التقنية لاستخدام التواقيع الرقمية على التأكد من أن تقانة التشفير المستخدمة آمنة من التزوير والإختراق:
   A. صح
   B. خطأ

9. تعتبر التواقيع الرقمية ضرورية لـ :
   A. لحماية موثوقية ونزاهة وخصوصية المعاملات عبر الانترنت
   B. ضمان الحصول على معلومات دقيقة وقابلة للتحقق، بخصوص الشخص الذي يحاول استخدام الخدمات، حيث أن إحدى أهم المشكلات التي تواجه الشركات هي التزوير والاحتيال.
   C. تحمي تقانات التوقيع الرقمي المستهلكين أيضاً، وتوفر لهم حماية مشددة، بحيث يتم حماية معلوماتهم من خلال مفتاح خاص
   D. جميع الإجابات صحيحة

رقم التمرين	الإجابة الصحيحة
1	(A)
2	(A)
3	(A)
4	(B)
5	(A)
6	(A)
7	(D)
8	(A)
9	(D)