**3. Хаттама: сымды және сымсыз, арнайы және жан-жақты**

1-суретте осы құжаттың қоршаған ортасы көрсетілген алаңдаушылық. Пайдаланушылар біраз уақыт алуы мүмкін дәстүрлі сымдардан электрондық коммерцияға (веб-сайттарға) қол жеткізу

браузерлер (Netscape, Internet Explorer және т.б.). Пайдаланушылар сондай-ақ, жаңа сымсыз электрондық коммерция сайттарына қол жеткізе алады PDA және ұялы телефондар сияқты құрылғылар. Бұл бапта құрылғыда ұсынылатын қауіпсіздік қызметтері қарастырылады

дәстүрлі сымды шолғыш немесе одан да көп болсын, пайдаланушыны қарау жаңа сымсыз құрылғы. Мақалада да назар аударылады пайдаланушы браузерінен беру кезінде деректер қауіпсіздігі электрондық коммерция веб-сайтында. Байланысты қауіпсіздік мәселелері

веб-сайт (мысалы, несие карталарын сақтау) осы мақаланың шеңбері.

Қауіпсіздікті қамтамасыз ету үшін сымды және сымсыз әлемдегі электрондық коммерция транзакциялары кем дегенде келесі қызметтерді ұсыну қажет [3]:

\* Пайдаланушының аутентификациясы-бұл жүйенің дәлелі пайдаланушы өзін кім үшін береді.

\* Деректердің аутентификациясы-екі сервистен тұрады: деректердің тұтастығы және деректер көзінің аутентификациясы. Тұтастықпен деректерді алушы сенімді бола алады

бұл деректер жолда өзгерген жоқ. Деректер көзінің аутентификациясы алушыға деректердің бар екенін дәлелдейді шынында да, көрсетілген жіберушіден келді.

\* Деректердің құпиялылығы - деректердің құпиялылығы қорғайды тасымалдау кезінде кез келген деректерді жария етуден және деректерді шифрлаумен қамтамасыз етіледі.

\* Авторизация-авторизация-бұл акт (аутентификацияланған) мәні бар-жоғын анықтау

әрекетті орындау құқығы. Бұл жауапкершілік жүйені ұсынушы транзакциялар / электрондық коммерция қызметтері.

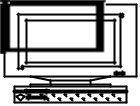
\* Аудит-аудиторлық қызмет тарихты ұсынады не (егер болса) анықтау үшін пайдаланылуы мүмкін әрекеттер -онда) қате болған кезде дұрыс болмады және ол не болды мұның себебі. Аудиторлық қызметтер де болуы мүмкін соңғы белгілі" жақсы " жағдайды анықтау үшін қолданылады

ақпарат.

Осы танымал қызметтерге қосымша мұны жиі күтуге болады электрондық коммерция мәмілелері бас тартуды қамтамасыз етеді. Бас тарту болып табылады пайдаланушы шынымен транзакцияны бастағанын дәлелдейді. Жауапкершіліктен бас тарту әдетте пайдаланушыдан талап ету арқылы жүзеге асырылады сандық қолтаңба транзакциялары. Сандық қолтаңбалар ерекше

пайдаланушылар және пайдаланушының бар екендігі туралы дәлелдер беру үшін қолданылады

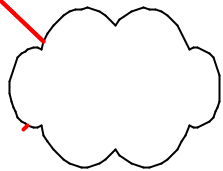
бұл транзакцияға қатысады. Егер атауды байланыстыру процесі болса пайдаланушының қолтаңба кілтіне (сандық қолтаңбаны жасау үшін) қауіпсіздік пен заңнаманың белгілі бір талаптарына жауап береді сандық қолтаңба пайдаланушының кейінгі кезеңдегі әрекеттерінен бас тартуға мүмкіндік беретін" жеткілікті күшті " болуы мүмкін.



W i r e d

E n v i r o n m e n t

P e r s o n a l C o m p u t e r



E - C o m m e r c e

P r o v i d e r



W i r e l e s s



 E n v i r o n m e n t



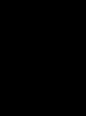
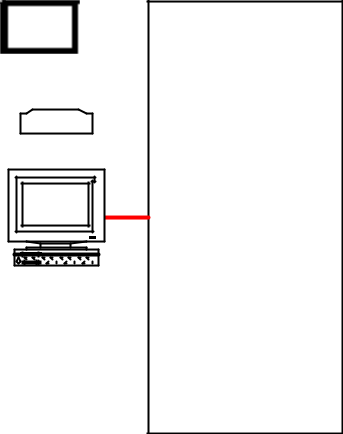
**Figure 1: E-Commerce Security**

**2 Желілік Орта**

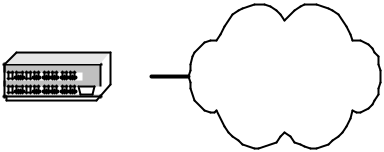
Бұл бөлімде біз желіні қысқаша сипаттаймыз сымды және сымсыз әлемдерге ортақ орта.

Біз сондай-ақ типтік Хаттамаларды және дәстүрлі сымды әлемде байқалатын қауіпсіздік талаптары. Бұл сымсыз әлемнің мүмкіндіктерімен салыстыру үшін негіз болады әрі қарай осы такрыпта.

Internet Service Provider



|  |  |
| --- | --- |
| Modem | ISP Servers |
|  |
|  | E-Commerce |
|  | Provider |
|  | ISP |
| Personal Computer Modem Bank | |



Router

**Figure 2: Traditional Wired Environment**

**2.1 Дәстүрлі Сымды Орта**

- Сур. 2 дәстүрлі сымды ортаны көрсетеді электрондық коммерция провайдеріне қол жеткізе алатын " үй " пайдаланушысы үшін (сонымен қатар браузерден back-end немесе Enterprise ретінде белгілі). Пайдаланушы өзінің жергілікті интернет-провайдеріне қосылады (ISP). Байланыс телефон желілері арқылы жүруі мүмкін, кабельді теледидар желісі,... Интернет-провайдер пайдаланушыға

Интернетке кіру және пайдаланушының сұрауларын жіберу. Пайдаланушы шолғышынан электрондық коммерция провайдеріне қолданылатын желілік протокол-TCP / IP

3-сурет суреттейді деп санауға болады WAP" дәстүрлі " желілік ортасы. Бұл

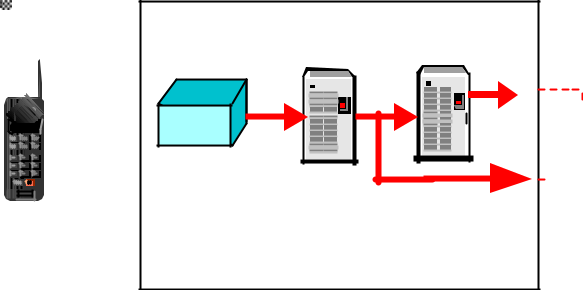
орта барлық қызметтер бар сымды ортаға ұқсас "типтес қосылыстар ұсынылады сымсыз желісімен.

Қызмет Көрсетуші. Бұл функцияның көп бөлігі сәйкес келеді қазіргі уақытта ұсынылатын функционалдылық телекоммуникация саласы. Біз күтеміз бұл функцияның көп бөлігі іске асырылады және сияқты телекоммуникациялық компаниялар басқарады

Сымсыз Қызмет Провайдерлері. WSP байланысты өңдеуді өңдейді кіріс WAP-байланыс, соның ішінде аударма wap құрылғысымен сымсыз байланыс беру мұнаралары арқылы модем банкіне және Қашықтан қатынау сервері (RAS) және одан әрі WAP Қақпа. Модем Банкі кіріс телефон қоңырауларын қабылдайды пайдаланушының мобильді құрылғысынан Ras сервері аударады

сымды сымсыз пакеттік форматтан кіріс қоңыраулар пакеттік формат, ал маршрутизатор бұл пакеттерді келесіге бағыттайды қажетті орын

WAP GW



Int

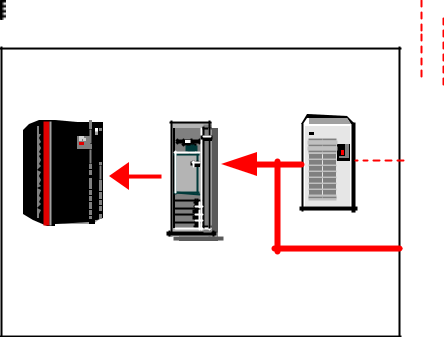


Modem Router

Bank &

RAS

Service Provider



WAP GW

|  |  |
| --- | --- |
| Server | Web Server |
|  |

Enterprise

**Figure 3: “Traditional” WAP Networking Environment**

WAP шлюзі WAP протоколдарын аудару үшін қолданылады ( үшін оңтайландырылған

өткізу қабілеті, төмен қуат тұтыну, шектеулі экран өлшемі және жадының төмен көлемі) Дәстүрлі интернет-хаттамаларға (TCP/IP). WAP шлюзі мыналарға негізделген прокси-сервер технологиялары. Типтік WAP шлюздері келесі функцияларды қамтамасыз етеді

мүмкіндіктер:

\* DNS қызметтерін ұсыну, мысалы, рұқсат алу үшін URL мекенжайларында қолданылатын Домен атаулары.

\* Алаяқтық пен пайдалануды басқару үшін бақылау пунктін қамтамасыз етіңіз қызмет.

\* Wap Протокол бумасын Протокол бумасына аудару арқылы прокси-сервер ретінде әрекет етіңіз

Internet. Көптеген шлюздерге "кодтау" мүмкіндігі де кіреді”, гипермәтінді белгілеу тілін аударатын

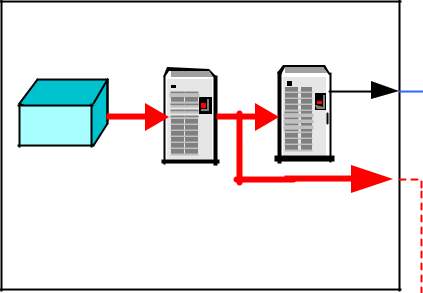
(HTML) сымсыз белгілеу тіліндегі бет (WML) құрылғының белгілі бір түріне сәйкес келетін бет (мысалы, Ұялы телефон Nokia 6120 немесе Motorola Timeport). Корпоративтік кеңістікте ішкі веб-серверлер мен серверлер бар қамтамасыз ететін қосымшалар кәсіпорынның транзакциялары.

Бұл сымсыз қызмет үшін "табиғи" болып көрінеді WAP қызмет көрсету және басқару провайдері

- шлюз-бұл жағымсыз жағдайлар. Бұл шифрлаудың "үзілуінің" болуына байланысты

сымсыз көлік деңгейінің қауіпсіздігі (WTLS) шлюз сеансы. Деректер уақытша ашық олар SSL сеансында қайта шифрланғанға дейін шлюздегі мәтін , кәсіпорынның веб-серверімен орнатылған. Бұл мәселе 5.3 бөлімінде егжей-тегжейлі талқыланады.

Мұндай жағдайларда wap шлюзіне суретте көрсетілгендей кәсіпорында қызмет көрсету керек. 4.WAP шлюзіне қызмет көрсету ешқандай телекоммуникациялық дағдыларды қажет етпейді; шлюз тұрақты UDP пакеттерін алады. Бұл шешімдегі мәселе мобильді құрылғыда DNS клиентінің болмауы болып қала береді, бұл мобильді құрылғыда әр мақсат үшін профильдерді сақтауды қажет етеді. Сондай-ақ, бұл кәсіпорыннан қызмет провайдерімен қарым-қатынас орнатуды талап етеді, оған сәйкес кәсіпорынға арналған барлық кіріс пакеттері (IP мекенжайы бойынша анықталады) дереу WSP тікелей кәсіпорынға жіберіледі және ешқашан WSP шлюзіне жіберілмейді.



WAP GW



Int



Modem Router

Bank &

RAS

Service Provider



WAP GW

|  |  |
| --- | --- |
| Server | Web Server |
|  |

Enterprise



To Other Content Providers

**Figure 4: e-Commerce Specific WAP**

**Networking Environment**

**iMode желілік ортасы**

iMode-бұл жеке меншік NTT DoCoMo протоколы Жапония. iMode дербес деректерді пайдалана отырып, интернет-сервисті ұсынады. Сандық ұялы пакет (PDC-P) және HTML жиынтығы

3.0 мазмұнды сипаттау үшін [19]. iMode жеткізушілерге мүмкіндік береді бағдарламалар / мазмұн бағдарламалық жасақтаманы тарату (Java- апплеттер) ұялы телефондарға, сондай-ақ пайдаланушыларға апплеттерді жүктеу (мысалы, ойындар). iMode сымсыз бөлікке арналған packetswitched технологиясын қолданады және сымды байланыс үшін TCP/IP протоколы арқылы беріледі байланыс бөліктері. Жіберу және қабылдау пакеттерін коммутациялау жүйелері

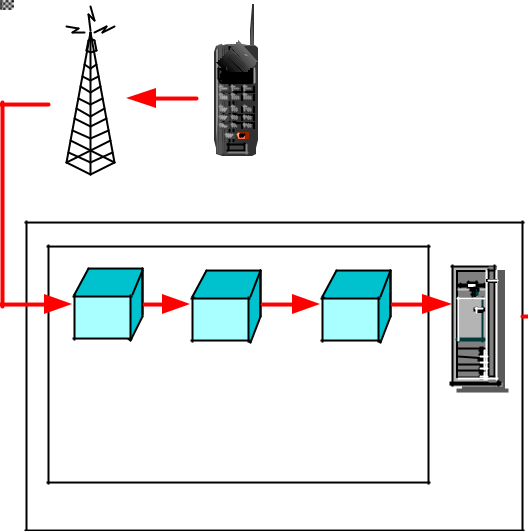
хабарламаларды кішігірім блоктарға бөлу арқылы ақпарат және әр пакетке адрестік және басқару элементтері бар тақырыптарды қосу ақпарат. Бұл мүмкіндік береді бірнеше

Жалпы арна бойынша байланыс. Бұл төмен құны бар арнаны тиімді пайдалануға мүмкіндік береді.

Бөлінген "DoPa" Docomo деректер қызметі жергілікті желіге қосылуды ұсынады және

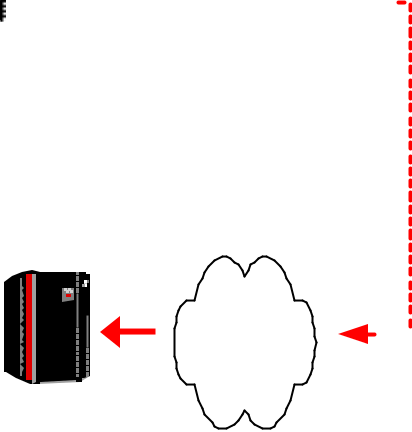
Осы қағиданы қолдана отырып, Интернет-провайдерлер пакеттік коммутация, сондай-ақ сымсыз секцияға. Жүйесі ұялы пакеттік байланыс желілік пакеттік байланыс болатын конфигурация

Docomo жеке кабинетіне қосылған және біріктірілген функция Сандық ұялы байланыс (PDC) - бұл сандық жүйе портативті және автомобиль телефондары.



Radio tower

|  |  |  |  |
| --- | --- | --- | --- |
| Int | Int | Int |  |
| Base | Packet | Mobile |  |
| Station | Processing | Message |  |
|  | Module | Packet | iMode |
|  |  | Gateway |
|  |  | Server |
|  |  | Module |
|  |  |  |
| PDC-P Network | |  |  |



Internet

Server

**Figure 5: DoCoMo iMode Wireless Networking Environment**

**3 сымды және сымсыз хаттамалар**

Бұл бөлімде екі сымсыз протоколға қысқаша кіріспе берілген-WAP және iMode. Біз сондай-ақ осы хаттамалардағы ұқсастықтар мен айырмашылықтарды талқылаймыз. Біз сымды протоколдарды, SSL/TLS [7], TCP/IP [4] және т.б. талқылауды қамтымаймыз, олар үшін көптеген сілтемелер бар.

3.1 планшеттің сипаттамасын тіркеусіз алуға болады

WAP ерекшелігі Интернетке сымсыз қосылуды жүзеге асыру үшін ашық, стандартты архитектураны және протоколдар жиынтығын анықтайды.

WAP ерекшелігі, басқалармен қатар, [1]:

\* Wireless Markup Language (WML) XML типті белгілеу тілі: WML және WMLScript сымсыз құрылғыларға жарамды белгілеу тегтерінің жиынтығын ұсынады. WML мазмұнына қол жеткізу (дәстүрлі) веб-серверде интернет арқылы Гипермәтінді беру протоколының стандартты сұраныстарын (HTTP 1.1) қолдана отырып жүзеге асырылады.

\* "Microbrowser" сипаттамасы: бұл WML және WMLScript сымсыз телефон тұтқасында қалай түсіндірілетінін анықтайды.

\* Жеңіл Протокол стегі: өткізу қабілеттілігінің талаптарын азайтуға арналған, ол әртүрлі сымсыз желілерге WAP қосымшаларын іске қосуға мүмкіндік береді. Сымсыз сессия ХАТТАМАСЫ қысылған форматтағы HTTP хаттамасына тең.

\* Сымсыз телефония қосымшаларына арналған шеңбер (WTA): ол WMLScript арқылы дәстүрлі телефония қызметтеріне (қоңырауларды бағыттау сияқты) қол жеткізуге мүмкіндік береді.

\* Инициализация: бұл қызмет жеткізушілеріне қысқа хабарламалар жүйесі (SMS) арқылы ұялы телефондарды қашықтықта қайта конфигурациялауға мүмкіндік береді (SMS GSM стандарты екенін ескеріңіз) [5].

WML: Wireless Markup Language

WSP: Wireless Session Protocol

WTP: Wireless Transport Protocol

WTLS: Wireless Transport Layer Security

WCMP: Wireless Control Management Protocol

WDP: Wireless Datagram Protocol

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| HTML, XML | |  | WML | |  |
| JavaScript, | |  | WBXML | |  |
|  |  |
| Java |  |  | WMLScript | |  |
| HTTP | |  | WSP | |  |
|  |  |
| SSL/TLS | |  | WTP | |  |
| TCP |  |  | WTLS | |  |
| IP | ICMP |  | WCMP |  |  |
|  |  |
|  |  |  | WDP & |  |  |
|  |  |  |  |
| Internet | |  | Adaptation | |  |
| Protocol | |  | WAP | |  |
| Stack | |  | Stack | |  |
|  |  |  |  |  |  |
| UDP |  |  | WCMP |  |  |
| IP | ICMP |  | WDP & | |  |
|  |  |  | Adaptation | |  |
|  |  |  |  |
| Internet | |  |  |  |  |
| Protocol | |  | WAP | |  |
| Stack | |  | Stack | |  |



**Figure 6: WAP Protocol Stack Specification**