Өгөгдлийн сангийн аюулгүй байдал

Өгөгдлийн сангийн аюулгүй байдал : Санаатай болон санамсаргүй аюулаас өгөгдлийн санг хамгаалах механизм юм.

Аюулгүй байдлын асуудал нь дан ганц өгөгдлийн санд дахь өгөгдөлд хамаардаггүй :

Аюулгүй байдлын цоорхой нь системийн бусад хэсэг болон өгөгдлийн санд ч нөлөөлж болно.Иймд өгөгдлийн сангийн аюулгүй байдалд тоног төхөөрөмж , програм хангамж , хүмүүс , өгөгдлийн сан багтдаг. Аюулгүй байдлыг үр дүнтэйгээр хэрэгжүүлэхийн тулд зохих хяналт , системд тодорхой үүрэг зорилтуудыг тодорхойлсон байхыг шаарддаг. Аюулгүй байдлын энэ хэрэгцээг өмнө нь ихэнхдээ байгуулгууд үл тоогдог байсан бол одоо хүлээн зөвшөөрч сайжруулж байна.

Байгуулгын чухал өгөгдлийн сан зохих хяналтын дагуу хамгаалагдсан байх ёстой. Өгөгдлийн сангийн аюулгүй байдалтай холбоотой анхаарах зүйлс :

* Хулгай ба залилан
* Нууцлалын алдагдах
* Хувийн мэдээлэл алдагдах
* Бүрэн бүтэн байдал алдагдах
* Бэлэн байдал алдагдах

Эдгээр нөхцөл байдлууд нь хохирол болон гэмтэлд өртөх боломж буюу эрсдлийг буруулахыг байгуулагууд эрэлхийлэх хэрэгтэй тэр салбарууд өргөнөөр эзэлдэг байна. Зарим нөхцөл байдалд эдгээр салбарууд нь нэг салбарт хохирол учруулдаг нэг үйл ажилгаа нь магадгүй бусдад нь мөн хохирол учруулдаг тийм нарийн холбоотой юм. Үүнээс гадна залилан болон хувийн мэдээлэл алдагдал нь санаатай болон санамсаргүйгээр ч гарч болох үйлдэл бөгөөд мэдээллийн санд эсвэл систем гарсан өөрчлөлт хийгдэх бүрт заавал мэдээлэлж байна. Хулгай ба залилан нь зөвхөн мэдээллийн санд төдийгүй байгуулгад нөлөөлдөг. Ийм үйл ажилгааг хүмүүс үйлддэг учраас энэ боломжийг үүсгэхгүй байхад анхаарах хэрэгтэй. Хулгай болон залилангын мэдээллийг хэрэгцээгүйгээр өөрчлөх үйл ажилгааны үр дүн нууц эсвэл хувийн мэдээлэл алдагдана. Дутуу эсвэл гэмтсэн өгөгдлөөс өгөгдлийн бүрэн бүтэн байдал алдагдснаар байгуулгын ажилгаанд ноцтой нөлөөлж болно. Байгуулгууд 24/7 буюу тасралтгүй ажиллагааг эрилхийлж байна.(өдрийн 24 цаг , 7 хоногын 7 өдөр ) Өгөгдөл эсвэл системийн бэлэн байдал алдагдах нь байгуулгад санхүүд ноцтой нөлөөлж болно.Зарим тохиолдолд өгөгдлийн эвдрэл нь системийг ажилгааггүй болгож болно. Бэлэн байдал алдахдах гэдэг нь байгуулгын санхүүгийн гүйцэтгэлд ноцтойгоор нөлөөлж болох өгөгдөл , систем эсвэл хоёуланд хандаж чадахгүй байх явдал юм.Зарим тохиолдолд системийг ашиггүй байдалд хүргэдэг хэрэг явдлууд нь мөн магадгүй өгөгдлийг эвдрэлд хүргэж болох юм.Сүүлийн үед компьютерт суурилсан гэмт хэргийн үйл ажилгаа нэлээд өссөн ба дараагийн хэдэн жилүүдэд өсөлт нь үргэлжилэх урьдчилсан таамаг байна.

Аюул занал – Системд болон эцэст нь байгууллагад сөргөөр нөлөөлж болох ямар нэгэн санаатай болон санамсаргүй нөхцөл байдал буюу хэрэг явдал юм.

Байгууллагад хохирол учируулж болзошгүй хүн , үйл ажилгаа эсвэл нөхцөл байдалыг хамруулдаг хэрэг явдал нь аюул заналыг бий болгож болох юм. Хор хорхирол нь техник хангамж , програм хангамж өмн өгөгдлийн алдагдал гэх мэт мэдэгдэхүйц байж болно. Байгууллагын нүүр тулж буй асуудал нь бүх боломжит аюул заналыг илэрүүлэх юм.Тийм учраас наад зах нь тухайн байгууллага хамгийн ноцтой аюул заналыг тодорхойлоход цаг хугацаа , хүчин чармайлтаа гаргах хэрэгтэй .Өмнөх бүлэгт бид санаатай болон санамсаргүй үйл ажиллагаанаас үүдэлтэй алдагдалтай салбаруудыг тодорхойлсон. Зарим төрлийн аюул занал санаатай болон санамсаргүй байж болох ч үр дагавар нь хэвээрээ байна.Санаатай аюул заналхийлэл нь хүмүүстэй хамаатай ба байгууллагаас гадны хүн байж болох зөвшөөрөлгүй хэрэглэгчид болон эрх бүхий хэрэглэгчи аль аль нь үйлдэж болзошгүй юм.Ямар ч аюул заналыг хэрвээ амжиллттай болвол тодорхой нөлөө үзүүлэх аюулгүй байдлын болонжит цоорхой гэж үздэг. Хор нөлөө үзүүлж болох салбарын дор жагсаасан тул аюул заналын янз бүрийн төрлийн жишээг харуулж байна. Жишээ нь : Зөвшөөрөгдөөгүй өгөгдлийг аюул занал гэж үзээд илрүүлэх нь байгууллагын хувьд хувийн болон нууц хадгалах байдлын алдагдал , хулгай болон луйвард хүргэдэг байна.

Хариу арга хэмжээ /Компьютерт суурьласан хяналт/

Эрх олгох / authorization / : Тухайн зүйлийг олгох эрх буюу давуу эрх нь хууль ёсны хандах эрхтэй систем юм уу системийн обьеттэй байна.

Бататгал/ Authentication / : хэрэглэгч нь хэн болохыг тодорхойлох механизм

Хандалтыг хянах / access controls / : Өгөгдлийн сангийн системд хандалтын хяналтыг хангах нийтлэг арга зам нь эрх олгох , давуу эрхийг хүчингүй болгох юм.

Давуу эрх /privilege / : Давуу эрх нь үүсгэх эсвэл хандалт(унших , бичих , өөрчлөх) зарим өгөгдлийн санг(тухайлбал : холбоо , харагдац , индекс ) эсвэл DBMS-н тодорхой хэрэгслүүдийг ашиглах боломжийг олгодог.

Харагдац / views / : Харагдац бол нэг эсвэл олон харилцаан дээр оператор үйл ажилгагаа явуулж динамик үр дүн авдаг

Нөөц / backup / : Тогтмол хугацаанд өгөгдлийн сангийн хуулбар болон бүртгэлийн файлыг офлайн агуулахд хадгалах үйл явц юм.

Тэмдэглэл / Journaling / : Гэмтэл гарсан тохиолдолд өгөгдлийн сангийн бүх өөрчлөлтийг бүртгэлийн файлд (тэмдэглэлд) бичиж хадгалан , сэргээх үйл явц юм.

Бүрэн бүтэн байдал / integrity / :

Нууцлал / encryption / : Өгөгдлийг онцгой алгоритм ашиглан шифрлэлтийг буцаах түлхүүргүйгээр ямар ч програмд өгөдлийг уншигдахгүй болгоно

Майкрософт оффис ӨСМС хандалт болон Ораклийн ӨСМС (өгөгдлийн сангийн менежмент систем) нь системийн аюулгүй байдал болон өгөгдлийн аюулгүй байдал гэх аюулгүй байдлын хэмжигдэхүүний 2 хоёр төрлийг санал болгодог . Системийн аюулгүй байдал нь өгөгдлийн санг нээх нууц үгийн тохиргоог тааруулах мөн хэрэглэгч зөвхөн унших, өөрчлөх л боломжтой байх гэх мэтээр өгөгдлийн сангийн хэсгүүдэд тодорхой хязгаарлалтуудыг тавьж хэрэглэгчийн түвшинд өгөгдлийн аюулгүй байдлыг хангах.

Аюулгүй байдлын хэмжигдэхүүн нь Вэб дээрх ӨСМС-тэй уялдаатай байдаг энэ нь : итгэмжлэгдсэн серверүүд, галт хана, зурвас эмхэтгэх алгоритм болон тоон гарын үсэг, тоон сертификат, керберос, Аюулгүйн соккет давхарга (SSL) мөн Аюулгүйн HTTP (S-HTTP), Аюулгүйн Электрон Гүйлгээ (SET), Аюулгүйн Гүйлгээний Технологи (SST), Жава аюулгүй байдал болон АктивИкс аюулгүй байдал зэргийг багтаадаг

DBMS ба Вэбийн аюулгүй байдал

Интернэт холбооны үндсэн протокол гэж TCP / IP дээр тулгуурладаг. Гэсэн хэдий ч TCP / IP болон HTTP аюулгүй байдлыг хангах зорилготой зохиогдоогүй . Тусгай програм хангамжгүй бол интернэтийн урсгалыг хэнч уншиж бас хянаж чадна.

* Интернэтээр мэдээлэл авах болон дамжуулахад дарааах сорилыг хангана :
* Илгээгч ба хүлээн авагчаас өөр хэнч халдашгүй (Хувийн нууц /privacy/ )
* Дамжуулах явцад өөрчлөгдөхгүй (Бүрэн бүтэн байдал /integrity/ )
* Хүлээн авагч илгээгчээс ирсэнд итгэлтэй байж чадна (Үнэн зөв байдал/authenticity/ )
* Илгээгч хүлээн авагчд итгэлтэй байж чадна (Дуураймал биш /non-fabrication/ )
* Илгээгч нь явуулчихсангаа үгүйсгэж чадахгүй байгаа (Татгалзалгүй/non-repudiation/)

Гэсэн хэдий ч , Гүйлгээг хамгаалах нь асуудлын хэсгийг шийдэх цор ганц шийдэл юм. Нэгэнт мэдээлэл вэб сэрвэрт хүрсэн бол хамгаалагдсан байх ёстой.Өнөөдөр ийм архитектурын ихэнх хэсэг нь баталгаажсан байдаг , гэхдээ энэ нь ерөнхийдөө янз бүрийн бүтээгдэхүүн, механизмыг шаарддаг. Вэб орчинд авч үзэх ёстой аюулгүй байдлын өөр нэг асуудал хэрэглэгчийн машинруу дамжуулагдаж мэдээлэлийн утга юм. Жишээ : HTML хуудас ActiveX хяналтыг агуулж болно , JavaScript / VBScript , эсвэл нэг буюу хэд хэдэн Java апплет. Дараах хортой үйлдэлийг хийх боломжтой ба урьдчилан сэргийлэх арга хэмжээ авах хэрэгтэй :

* + Бохир өгөгдөл эсвэл программын ажиллах бүтэц
  + Бүтэн дискнүүдийг дахин форматлах
  + Бүх системийг унтраах
  + Нууц үг , файл , нууц мэдээлэл татаж авах болон цуглуулах
  + Хэрэглэгчийн дүрд тоглон хэрэглэгчийн компьютерийн сүлжээгээр хууль бусаар эзлэх довтлох
  + Ялангуяа аюулгүй боловч гаралтын төхөөрөмжинд зохисгүй нөлөө үзүүлдэг

Прокси сервер / Proxy Servers /

Вэб орчинд нь прокси сервер нь Вэб браузер болон вэб серверийн хооронд суудаг компьютер юм. Энэ хүсэлтийг нь өөрөө биелүүлж чадах эсэхийг тодорхойлохын тулд вэб сервер нь бүх хүсэлтийг ялгадаг. Хэрэв тийм биш бол, энэ нь Вэб сервер рүү хүсэлтийг дамжуулдаг. Прокси сервер хоёр гол зорилготой юм :

1. хүсэлт шүүх
2. үйл ажилгааг сайжруулах
3. Үйл ажилгаа сайжруулах

Прокси сервер нь тодорхой хугацаанаас хойш бүх хүсэлтийн үр дүнг хадгалах нь хэрэглэгчдийн бүлгийн үйл ажилгааг мэдэгдэхүйц сайжруулдаг. Жишээ нь А ба Б хэрэглэгч нь вэбээр дамжуулан прокси серверд ханддаг. Эхлээд А хэрэглэгч вэб хуудасд хүсэлт явуулна үүний дараагаар Б хэрэглэгч ижил вэб хуудсанд хүсэлт явуулна. Харин хүсэлтийг вэб сервер рүү хүсэлтийг дамжуулна,прокси сервер нь ердөө А хэрэглэгчийн дуудсан байсайн хуудсыг кэш хийн буцаана.

1. Хүсэлт шүүх

Прокси сервер нь мөн хүсэлт шүүж ашиглаж болно.

Галт хананууд / Firewalls /

Галт хана нь зөвшөөрөлгүй хандалт эсвэл хувийн сүлжээнээс сэргийлэх зорилготой. Галт хана тоног төхөөрөмж болон програм хангамж эсвэл аль алиныг нь хослуулан хэрэгжүүлж чадна. Интернэтэд холбогдсон хувийн сүлжээнд зөвшөөрөлгүй хэрэглэгчид нэвтрэхээс урьдчилан сэргийлэх тулд ашиглаж байна. Галт хана хэд хэдэн төрөл байдаг :

Пакет шүүлт / Packet filter / :

Програмын гарц / Application gateway / : Тодорхой програмууд FTP болон Telnet гэх мэт аюулгүй байдлын механизмыг хэрэглэнэ. Энэ нь маш үр дүнтэй боловч үйл ажилгааг бууруулдаг

Circuit түвшний гарц / Circuit-level gateway / : TCP эсвэл UDP холболт тогтоосон үед аюулгүй байдлын энэ арга замыг мөрдөнө. Холболт хийгдсэний дараа , пакетуудыг шалгалгүй хоструу урсгаж чадна.

Прокси сервер / Proxy server / : Сүлжээгээр орж , гарж буй бүх мэдээллийг ялгадаг. Прокси сервер нь үнэн сүлжээний хаягийг нуудаг.

Зурвас эмхэтгэл алгоритмууд ба дижитал гарын үсэг

Зурвас эмхэтгэл алгоримт эсвэл нэг мөр хэш функц : Дурын хэмжээтэй мөр (зурвас)авч тогтмол урттай мөр(хэш эсвэл эмхэтгэл) үүсгэдэг.Товч дараах шинжүүдтэй байна :

* Өөр зурвас олох тооцооллын хувьд биелэшгүү байх нэг эмхэтгэл бий болгоно
* Эмхэтгэлээс зурвасын талаар юу ч мэдэж чадахгүй.

Дижитал гарын үсэг нь хоёр хэсгээс бүрдэнэ : Хувь хүн болон байгууллагыг хувийн түлхүүр , гарын үсэгтэй нь хамт тооцоолол хийнэ. Гарын үсэг нь мэдээлэл хувь хүн эсвэл байгууллагаас ирсэн эсэхийг шалгаж чадна. Гараар бичсэн гарын үсэг шиг дижитал гарын үсэг нь олон ашигтай шинж чанартай байдаг :

* Жинхэнэ эсэхийг олон нийтийн түлхүүрээр харгалзах тооцооллыг ашиглан шалгаж чадна
* Энэ хуурамч байж чадахгүй
* Гарын үсэг зурсан мэдээлэл бол гарын үсэг нь цаашид хүчинтэй байх ба мэдээллийг шалгаж болно, өөрчилж чадахгүй.

Хамгаалалтын төрлүүд /Types of Security /:

Өгөгдлийн сангийн аюулгүй байдал нь олон асуудлуудыг тусгасан өргөн цар хүрээг хамардаг.

* Тодорхой мэдээлэл олж авах эрхийн тухай хууль эрх зүйн болон ёс зүйн янз бүрийн асуудлууд

Жишээ нь : АНУ-д мэдээллийн нууцлалыг зохицуулах олон хууль байдаг.

* Төрийн бодлого , аж ахуй байгуулгын түвшинд олон нийтэд хүргэж болохгүй мэдээл байдаг.

Жишээ нь : Зээлийн зэрэглэл, хувийн эрүүл мэндийн бүртгэл гэх мэт.

* Системтэй холбоотой асуудлыг системийн түвшинд төрөл бүрийн аюулгүй байдлын үйл ажилгааг хэрэгжүүлдэг байх ёстой.

Жишээ нь : Аюулгүй байдлын үйл ажиллагаа физик тоног төхөөрөмжийн түвшинд, үйлдлийн системийн түвшинд, эсвэл DBMS түвшинд шийдэх шаардлагатай эсэх.

* Зарим байгууллагад шаардлагатай аюулгүй байдлын түвшин , өгөгдөл болон хэрэглэгчид суурьласан хэд хэдэн ангилал тодорхойлж ангилдаг.

Жишээ нь : Маш нууц , нууц болон ангилагдаагүй. Мэдээллийн янз бүрийн ангилалд хандах хандалтыг зөвшөөрөхтөй холбоотой байгуулгын бодлого хэрэгжүүлдэг байх ёстой.

Хяналтын арга хэмжээ / Control Measures / :

Мэдээлэлийн сангийн аюулгүй байдлыг хангахад дөрвөн гол хяналтын арга хэмжээг ашигладаг.

* Хандалтыг хянах /Access control /
* Урсгалын хяналт / Flow control /
* Дүгнэлтийг хяналт / Inference control /
* Өгөгдлийн нууцлал / Data encryption /

Компьютерийн системүүдэд нийтлэг байдаг аюулгүй байдлын асуудал нь системд зөвшөөрөлгүй этгээд хандах , мэдээлэл олж авах эсвэл мэдээллийн санд хортой өөрчлөлт оруулхаас урьдчилан сэргийлэх юм.

Жишээ : Статик өгөгдлийн сангаас хүн амын насны бүлэг,орлогын түвшин , өрхийн тоо , боловсролын түвшин болон бусад шалгуурт үндэслэн статик мэдээлэл өгч болно. Ийм өгөгдлийн сангийн хэрэглэгчид нь засгийн газрын статикч эсвэл зах зээлийн судалгааны компаниуд нийт хүн амын тухай статик мэдээлэл авахын тулд өгөгдлийн санд хандах эрхтэй боловч тодорхой хувь хүмүүсийн дэлгэрэнгүй нууц мэдээллийг авч чадахгүй. Статик өгөгдлийн сангийн аюулгүй байдал нь хувь хүний мэдээлэл хандаж чадахгүй байна.!!!!. Энэ асуудал, статистикийн мэдээллийн сангийн аюулгүй байдал гэж нэрлэдэг. Холбогдох хяналтын арга хэмжээ дүгнэлт хяналтын арга гэж нэрлэдэг.

Өгөгдлийн сангийн аюулгүй байдал ба админ / Database security and DBA / :

Өгөгдлийн сангийн администратор (DBA) нь өгөгдлийн сангийн системийг удирдах гол мэргэжилтэн юм. DBA-ийн үүрэг, хариуцлага системийг ашиглах хэрэгтэй хэрэглэгчдэд давуу эрх олгох, байгууллагын бодлогын дагуу хэрэглэгчид болон мэдээллийг ангилах зэрэг юм. Админ нь өгөгдлийн санд админ бүртгэлтэй байна заримдаа супер хэрэглэгчийн бүртгэл гэж нэрлэдэг. Энэ нь ердийн мэдээллийн санд хэрэглэгчдэд хүртээмжтэй биш хүчирхэг боломжуудыг олгодог.

1. Бүртгэл үүсгэх / Account creation / : DBMS-д хандах эрхтэй хэрэглэгч эсвэл хэрэглэгчдийн бүлэгт шинэ бүртгэл , нууц үг үүсгэх үйлдэл юм .
2. Эрх олгох / Privilege granting / : Энэ арга хэмжээ нь тодорхой дансанд тодорхой давуу эрх олгохыг админ зөвшөөрөх үйлдэл юм.
3. Эрх цуцлах / Privilege revocation / : Урьд нь тодорхой дансанд өгсөн тодорхой давуу эрхийг цуцлах админ зөвшөөрөх үйлдэл юм.
4. Аюулгүй байдлын түвшин дэхь хэрэглээ / Security level assignment / :

Аюулгүй байдлын цэвэрлэгээний түвшинд хэрэглэгчийн бүртгэлийг зааж бүртгэх үйлдэл юм.

Админ нь өгөгдлийн сангийн системийн ерөнхий аюулгүй байдлыг хангах үүрэгтэй.

1-р үйлдэл : Жагсаалтыг бүхэлд нь DMBS-д хандах хандалтыг хянахад ашиглана. 2 ,3 -р үйлдэл : Өгөгдлийн санг дур зоргоороо ашиглахаас хянахад ашиглана.

4-р үйлдэл : Зөвшөөрөл хянахад ашиглана.

Андройд дээр mysql-тэй холбож insert ,update , delete , select хийсэн textlinked болгож үзсэн

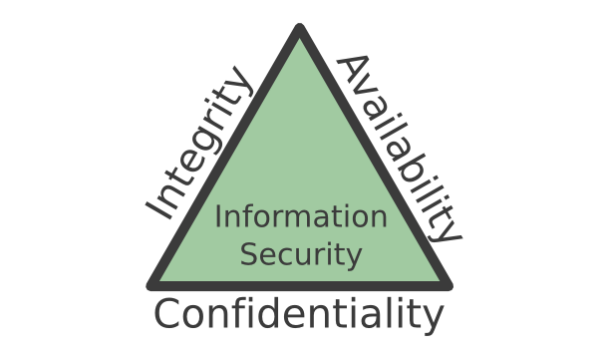
!!!

Аюулгүй байдал гэдэг нь хор хохирлоос хамгаалах эсвэл эсэргүүцэх чадварын чанар юм. Энэ нь хүн, орон гэр, эд зүйл, улс үндэстэн болон байгуулга гэх мэт эмзэг, үнэ цэнэтэй бүх зүйл дээр хэрэглэгддэг.

Өгөгдлийн сангийн аюулгүй байдал :

Өгөгдлийн сангийн аюулгүй байдал нь хулгай, буруу хэрэглэх, хүсээгүй халдлага болон дайралтаас өгөгдлийг хамгаалдаг тогтсон журам, стандарт бодлого болон тоног төхөөрөмжийн цогц юм.Өгөдлийн сангийн аюулгүй байдал нь өгөгдлийн бүтэц байгууламж болон үүнд агуулагдаж байгаа өгөгдөлд нэвтрэх зөвшөөрлийг авч үздэг.Өгөгдлийн санг аюулгүй болгоход хэрэглэгдэх багаж хэрэгцэл нь ихэвчлэн өгөгдлийн сангийн програм хангамж дотор нь суулган тохируулагдсан байдаг ба үйлдвэрлэгчид нь Oracle, MySQL, Microsoft SQL Server гэх мэт өөр өөр байна. Өгөгдлийн сангийн програм хангамжыг үйлдвэрлэгчид өгөгдлийн сангийн аюулгүй байдлыг хангах зорилгоор хамгийн түгээмэл ашигладаг аргууд нь хандалтыг хянах, гэрчилгээ болон өгөгдлийн нууцлаж хадгалах юм.

Өгөгдлийн сангийн аюулгүй байдлын зорилго :

Үр ашигтай аюулгүй байдлын архитектүр нь нууцлал (confidentiality), бүрэн бүтэн байдал (integrity), бэлэн байдал(availability) тулгууралдаг. Үүнийг C.I.A. гурвалжин буюу аюулгүй байдлын загвар гэж нэрлэдэг. 

Asd

Нууцлал (Confidentiality) :

Учир нь системийн нууцлалыг хангахын тулд, энэ хоёр зүйлийг хийх хэрэгтэй :

* 1. Мэдээллийн нөөцд хандах эрх бүхий боломжийг хязгаарлах замаар өөрийн хувийн нууцыг хадгалах.
  2. Нөөцд хандах зөвшөөрөлгүй хандалтыг хаах.

Өгөгдлын сангийн систем нь нөөцийн нууцлалыг гэрчилгээ болон хандалтыг удирдах замаар хамгаалдаг. Жишээ нь : Администратор нь хэрэглэгчийн нэвтрэх эрхийн мэдээллийг ашиглан мэдээллийн сан эсвэл мэдээллийн сангийн орчинд эрхийг хязгаарлаж замаар ашиглаж болно. Нууцлал аюулгүй байдлын хүчин чармайлтын хүрээнд хүрэх чухал зорилго юм. Нууцлалын цоорхой нь хэд хэдэн аюултай үр дүнд хүргэж болох юм.

Бүрэн бүтэн байдал (Integrity) :

!

Бэлэн байдал (Availability) :!

## 1 Андройд системийн судалгаа

## Андройд аппликейшний судалгаа

Андройд үйлдлийн систем нь олон хэрэглэгчийн хандалттай линукс, нээлттэй эхийн систем ба энд аппликейшн болгон тусдаа нэгэн хэрэглэгч болдог. Андройд дээрх аппликейшнүүд нь жава програмчлалын хэлээр бичигддэг. Андройд SDK түүлүүд нь бичсэн кодыг хамт хавсрагдах нөөц файлууд, өгөгдлүүдтэй хамт хөрвүүлэгдэж .apk өргөтгөлтэй файл болдог. Энэхүү файлыг андройд үйлдлийн системтэй утсан дээр аппликейшнээ суулгахад ашиглана. Утсан дээр суулгасан аппликейшн нь бие даан өөрийн хүрээнд ажиллах ба үндсэн тохиргоогоор систем аппликейшн болгонд давтагдашгүй нэг ID өгдөг. Мөн аппликейшн бүр өөрийн гэсэн виртуал орчинг үүсгэж ажиллах ба ингэснээрээ бусад аппликейшнүүдээс хамааралгүй ажиллах боломжтой юм. Зарим тохиолдолд хэд хэдэн аппликейшн өөр хоорондоо мэдээлэл солилцох, ашиглах шаардлага гардаг. Энэ тохиолдолд хоёр аппликейшн нь дундаа процесс ID –тай байх ба ингэснээр нэг нь нөгөөгийнхөө хандах эрхтэй файл, хэсгүүд рүү хандах боломжтой болно. Аппликейшн тодорхой мэдээлэл, хэсгүүд рүү хандахдаа зөвшөөрөл авч болно. Эдгээр эрх болон хязгаарлалтуудыг аппликейшн суулгахдаа тохируулна. Андройд аппликейшн бүтээх гол хэсгүүд нь компонентүүд гэж ойлгож болно. Компонент бүр нь системээс аппликейшн рүү хандах нэг хандалтын цэг юм. Хэрэглэгчийн хувьд компонент бүр нь хандах цэг гэсэн үг биш ба зарим нь бусдаасаа хамаарч ажилладаг. Мөн компонент бүр бие даан орших ба тодорхой үүрэг рольтой байна. Хэсэг тус бүр аппликейшний ерөнхий ажиллах зарчмыг тодорхойлдог. Дөрвөн аппликейшний хэсэг, компонентүүд :

* Activity
* Service
* Content
* Broadcast receiver

Эдгээр нь тус бүрдээ өөр өөр зорилготой бөгөөд хэрхэн бий болох, устгагдахыг тодорхойлох амьдралын хугацаатай байдаг.



**Вэб програм хангамжийн судалгаа**

Вебийн түүх 1980-аад оны сүүл үеэс эхлэлтэй. 1989 онд Европийн Цөмийн Физикийн Судалгааны Төвд (CERN) дэлхийгээр нэг тархсан судлаач эрдэмтдийг компьютерын сүлжээний тусламжтайгаар өөр хооронд нь холбож, санаа оноогоо солилцож байх боломжийг олгох “WWW” төсөл хэрэгжиж эхлэсэн нь бидний мэдэх вебийн үүсэл юм. WWW-г интернетэд байрлах асар том “номын сан”-тай зүйрлэж болно. “Номын сан” нь үй олон “ном”-оос тогтоно. Ийм “ном”-ыг веб сайт (web site) гэнэ. Веб сайт нь өөрөө хуудаснуудаас тогтоно. Ийм хуудсыг веб хуудас (web page) гэнэ. Веб хуудас хөгжихийн хэрээр веб аппликейшн гэх ойлголт чимээгүйхэн даган хөгжиж ирсэн гэж үздэг. Учир нь бүх зүйл веб гэх зүйлрүү чиглэхийн хэрээр Desktop програмууд шахагдан вэбрүү шилжин веб аппликейшнийн суурийг тавьж өгсөн. Веб аппликейшн гэдэг нь веб хөтөч дээр ажиллаж байгаа програм хангамжуудыг хэлнэ. Энэ нь дэлгэрэнгүй тайлбарлавал (Javascript, HTML, CSS) гэх зэрэг хөтөч дэмжлэгтэй програмчлалын хэл дээр тулгуурлан бий болсон програм хангамжуудыг хэлнэ. Цаг хугацаа өнгөрөхийн хэрээр веб аппликейшнийн хөгжил маш хурдацтай өсөж байна. Хурд хүч сайтай компьютерүүд гарч ирэхийн хэрээр тэдгээрийг дэмжин ажиллах өндөр хүчин чадалтай сервер, серверийн үйлчилгээ явуулдаг компаниуд олширч байна. Мөн үүнийгээ дагаад веб аппликейшнүүд нь бүх мэдээллээ өндөр хүчин чадал бүхий сервер дээрээ байршуулж мөн хэрэглэгчид ч гэсэн өндөр хүчин чадалтай компьютерууд ашиглан сервер хэрэглэгчийн компьютер хоёрын хооронд том асуудал болоод байсан хүлээлт гэдэг зүйл бараг арилж байна. Энэнь маш том давуу тал бөгөөд тухайн веб хэрэглэгчийн веб дээр ачаалахын тулд маш олон шат дамжлагыг дамждаг байсан бол энэ нь эсрэгээрээ өөрчлөгдсөн байна. Веб програмын давуу талууд  Ямар ч суулгац (install) хэрэггүй бөгөөд веб хөтөч байхад л хангалттай  Төвлөрсөн мэдээллийн сан, нөөцтэй, аюул бага, амар хялбар  Хурдан шуурхай, шинэчлэл хийхэд хялбар  Дэлхийн хаана ч хэнд ч хүрч чадна.  24 цаг, 7 хоногийн турш ч ачааллаж чадна.  Бага үзүүлэлттэй компьютер, гар утас гээд бүх л технологи дээр ажиллах боломжтой.  Үргэлж хамгийн сүүлийн хувилбар хэлбэрээр хэрэглэгчид хүрнэ.  Хамгийн сүүлийн үеийн мэдээллээр хангах чадвартай.

Веб програмын сул талууд  Удаан сүлжээнд байгаа нөхцөлд ажиллуулах боломж хүндрэлтэй  Интернет нь үргэлж 100% байх нь баталгаатай биш  Харагдах байдал байнга төгс биш  Зарим зүйл дээр төвөгтэй асуудлууд гарч ирэхэд хөгжүүлэхэд цаг их орох  Зарим хөтчүүд тухайн аппликейшнийн хувилбарыг дэмжихгүй байх  Аюулгүй байдлын эрсдэл зарим аппликейшн дээр ихээр хөндөгдөх  Сүлжээ тасарсан тохиолдолд ажиллах боломжгүй

**Гар утасны програм хангамжийн судалгаа**

Гар утасны хөдөлгөөнт холбооны дэвшилтэт технологи бүхий төхөөрөмж юм. Тухайн утасны төрлөөс хамаараад системийн програм хангамж нь өөр өөр байдаг.Түүнээс гадна тухайн системийн тасралтгүй ажиллагааг хангах, мэдээллийг боловсруулах хадгалах, техник хангамжийн хэсгийг бүхэлд нь удирдах гол үүргийг програм хангамж гүйцэтгэдэг. Өөрөөр хэлбэл техник хангамж /hardware/, програм хангамж /software/ нь хоорондоо салшгүй холбоотой ажилладаг. Гар утасны програмын гэмтэл нь олон төрөл байх бөгөөд байнга тохиолдож байдаг нэлээд түгээмэл гэмтэлд ордог.

**SQLite**

SQLite нь эмбэдэд төхөөрөмжид зориулсан өгөгдлийн сангийн хөдөлгүүр юм. Бусад SQL өгөгдлийн сангуудаас ялгаатай нь тусдаа сервер байдаггүй тухайн ажилж буй төхөөрөмжийн диск дээр сангаа үүсгэн ажилладаг. SQLite нь маш авсаархан сан юм. Багтаамж бага эзэлдэг учраас ихэнх жижиг багтаамж багатай төхөөрөмжүүд дээр түлхүү ашиглагддаг. Жишээ нь андройд, iOS гэх мэт. SQLite өгүүлбэр зүйн хувьд бусад SQL суурьтай хэлүүдтэй төстэй юм.

**Jquery**

JQuery бол жаваскриптийн фрэймворк бөгөөд клиент талд код бичиж байгаа веб хөгжүүлэгчдэд хэрэг болох маш олон зүйлүүдийн жаваскрипт функцийн санг бэлтгэсэн байдаг. Өөрөөр хэлбэл JQuery нь хэрэглээг хөнгөвчлөх зорилготой веб хөтөч хамааралгүй

(Cross browser) клиент талын жаваскрипт сангийн цуглуулга юм. Эдгээр сан нь дараах зүйлүүдийг хамардаг.

 HTML элементийн сонгуур  HTML элементүүдийг удирдах  CSS хөгжүүлэх  HTML-ийн үзэгдлийн функцүүд  Жаваскриптын эффект болон анимэйшинүүд  HTML DOM-оор гүйх болон өөрчлөлтүүд  AJAX  Utilities зэрэг байдаг.

JQuery нь бидний мэдэх Жаваскрипт санг хөгжүүлэгчдэд хялбар болгож илүү боломжийг олгож өгсөн сан бөгөөд өмнөх бүлэгт дурдагдсан фрэймворкын нэг хэлбэр гэж ойлгож болно. Сүүлийн жилүүдэд веб програм хөгжүүлэгчид веб програмын клиент, сервер хоёуланг чухалчлан үздэг болсон ба энэ нь хэрэглэгчийн харьцах хэсгийг илүү хялбар, сонирхолтой болгож хэрэглэгчид ажиллах хүсэл төрүүлнэ.

Үүнийг хэрэгжүүлэх шилдэг технологи нь JQuery бөгөөд нэг үгээр жаваскрипт функцуудыг тодорхойлж өгсөн сан юм. Одоогийн байдлаар JQuery сүүлийн хувилбар v2.0.0 гараад байна. Дипломын төсөл хэрэгжүүлэхэд JQueryv2.0.0 хувилбарыг сонгон авч судаллаа.

Ажиллагааны үндсэн зарчим:

 Тухайн дуудагдах хуудсанд JQuery файлыг шигтгэж өгсөн байна  Хуудсан дээр клиент код буюу жаваскрипт функцээр дамжуулан хүссэн JQuery-ийн функцийг дуудаж өгнө.  JQuery нь тодорхой бичиглэлийн дүрэмтэй.

jQuery –йин үндсэн 3 төрлийн хэрэглээ түгээмэл байдаг. HTML document–д, CSS файлд стиль өгөх, мөн JavaScript файлтай харьцах.

**Bootstrap** Вэб програм нь гар утас, таблет зэрэг дээр ажиллах учир тухайн төхөөрөмжийн хэмжээнээс үл хамаараад ямар нэгэн эвдрэлгүй ажиллах ёстой. Энэ асуудлыг ‘Twitter Bootstrap’ CSS фрэймворкийг ашиглан зохиомжилсон. Twitter Bootstrap нь нээлттэй эх бүхий веб сайт болон веб аппликэйшн хөгжүүлэхэд зориулагдсан хэрэгслүүдийн цуглуулга юм. Энэ нь дотроо HTML, JS болон CSS дээр суурилсан форм, товчлуур, диаграмм зэрэг клиент талын програм хангамжийн интерфейсийн загварыг гаргах бүрэлдэхүүн хэсгүүдийг агуулсан.Бүүтстрип 2.0 хувилбараас хойш уян хатан вэб дизайныг (responsive web design) дэмжин ажилладаг болсон.

Bootstrap нь вэб хөтөч дээр ажиллахаас гадна ухаалаг гар утас болон таблет дээр ажиллах боломжтой. Дотоод CSS зохиомжийнх нь бүтэц нь 12 багана бүхий grid системтэй. Энэ нь тухайн төхөөрөмжийн хэмжээнээс үл хамааран вэб аппликэйшнийн дизайныг хийхэд хялбар болгож өгнө. Грид систем гэдэг нь хуудасны бүтцийг 2 хэмжээст хүснэгтэд хуваан зохиомжлохыг хэлнэ.

**MySQL**

**NodeJS**

NodeJS бол сервер талд жава-скрипт кодоор програмчилдаг нээлттэй эхийн, бүх платформуудад ажилладаг веб програм хөгжүүлэхэд зориулсан технологи юм. NodeJS нь үзэгдэл удирдлагад суурилсан архитектуртай болон бодит цаг хугацааны веб програм хөгжүүлэхэд илүү тохиромжтой технологи юм. NodeJS нь Chrome хөтчид бүтээгдсэн Google-ийн V8 engine дээр ажилладаг. Мөн олон бэлэн модулиудтай ирдэг учир бүх зүйлийг эхнээс бичих шаардлагагүй. Өөр хүмүүсийн бичсэн олон сангууд үнэгүй татахаар бэлэн байдаг. Бас Node.JS технологи дээр төрөн гарч, уялдаж ажилладаг авсаархан хирнээ хүчирхэг хэрэглээтэй багц системүүд тоо томшгүй байгаа нь:

 NPM - Node.JS-ийн багц системүүдийн удирдлага

Node.JS дээр ажиллуулах ба боломжгүй бол ajax, flash зэргээр орлуулах технологи  Express.js - Вэб апп фрэймворк 

LESS - Динамик CSS фрэймворк 

Jade - Динамик HTML фрэймворк 

Mongoose - MongoDB-гийн Node.JS сан

Бүрэн бүтэн байдал нь найдвартай, тогтвортой, иж бүрэн мэдээлэл, тогтолцоог бий болгох болон дэмжих зорилгоор бодлого, журам, зураг төслөөр дамжуулан авсан хүчин чармайлт дээр үндэслэдэг.

Мэдээллийн сан дахь бүрэн бүтэн байдал нь мэдээллийн сангаас эргүүлсэн авсан болон дотор нь хадгалсан өгөгдлийн найдвартай, үнэн зөв, тууштай байдлыг хэлнэ. Мэдээллийн сангийн багтаамж эсвэл эргүүлэн авах нь найдваргүй болон нийцэхгүй байж болзошгүй, санамсаргүй буюу санаатайгаар эсэх нь хууль бусаар эсвэл эрх бүхий өөрчлөлт аль аль нь урьдчилан сэргийлэхээр өгөгдлийн сангийн бүрэн бүтэн байдлыг хамгаалдаг байна. Бүрэн бүтэн байдал нь эвдэрсэн мэдээлэл нь заавал алга болсон биш зүгээр л өөрчлөгдсөн учраас хэмжихэд хамгийн хэцүү зүйл нь юм.

Хэд хэдэн шалгалт болон тэнцвэрт байдал нь мэдээллийн сан даяар байдаг өөрчлөлт болон алдаа дутагдалыг олох шаардлагатай байдаг. Энэ үйл явц нь аудит гэж нэрлэдэг ба тиим мэдээлэлийн хуучин нөөцлөгдсөн хувилбарын эсрэг мэдээллийг шалгаж систем доторх ялгаа зөрүүг хайдаг аудитын ажилтаныг татан оролцуулдаг юм. Өгөгдлийн сан аудитын тухай дараа нь номонд нарийвчлан хэлэлцэх боловч, та төсөөлж байгаачлан мэдээллийн сан илүү нарийн төвөгтэй байна, аудитын зорилт тэр чинээгээр илүү их байдаг. Бүрэн бүтэн байдал нь мэдээллийн сангийн маш чухал шинж чанар бөгөөд хэрэв амжилтгүй хэрэгжүүлвэл, системийн гажуудал, найдваргүй өгөгдөл, гажигтай хөтөлбөр, муу гүйцэтгэлд хүргэж болох юм.

Бэлэн байдал нь сүлжээн дээрх эсвэл мэдээллийн сан доторх нөөцийн хүртээмжтэй байдлыг хэвээр байлгахын тулд бодлого, журам, зураг төслөөр дамжуулан авсан аргыг хэлнэ. Эдгээр нөөц агуулдаг боловч мэдээлэл, өргөдөл, бусад мэдээллийн сан, компьютер, сервер, програм, файл, удирдаж байгаа програм, хувьцаа, болон сүлжээний хандалт зэргээр хязгаарлагдахгүй байна.

Манай нөөцийг хамгаалахын тулд бид мэдээллийн сангийн бэлэн байдалд аюул занал учруулж буй зүйлийг тодорхойлох болон тиймээс тэд саад болох зүйлийг төлөвлөдөг болон мухардалд оруулдаг тийм аюул түвшинг үнэлэх ёстой. Нийтлэг аюул уруулч чадах зүйлс нь техникийн алдаа (жишээ нь, мөрдөгч, эсвэл эвдэрсэн төхөөрөмж, гажигтай хөтөлбөр, програм хангамжийн хэсэг), байгалийн гамшиг (жишээ нь, үер, эсвэл гал түймэр), халдлага (жишээ нь, вирус, Трожан, хорхойнууд) болон хэрэглэгч (жишээ нь, санамсаргүй буюу санаатайгаар аюул занал) зэргийг багтаадаг.

Нууц хадгалах байдал болон бүрэн бүтэн байдлаас ялгаатай нь бэлэн байдалгүйгээр ямар ч үйл ажиллагаа явуулж чадахгүй.учраас бизнесийн хамгийн чухал хэрэгсэлрүү нэвтурч чадахгүй байх нь ажлуудын хамгийн энгийн дуусгах боломжгүй буюу гэмтэлтэй болгодог. Зөвшөөрөгдөхийн тулд нөөцийн бэлэн байдлыг авдаг хүмүүс олон байдаг. Алга болсон файл болон өргөдөл нь энэ цаашдаа боломжтой байхаа болих хүртэл бүтээмжтэй байж болдог нөлөөг тэд ойлгодоггүй. Хамгийн шилдэг төлөвлөгөөтэй байсан ч хэн ч ямар ч үед бүх сүлжээний нөөцийг 100% бэлэн байдалаар хангаж чаддаггүй. Юу тодорхой байна вэ гэвэл сүлжээний эсвэл өгөгдлийн нөөц нь хэр удаан хүртээмжгүй байна тэр хэрээр гарах алдагдал нь их байна. Зөв тодорхойлолт, зөв төлөвлөлт нь сүлжээ бэлэн байлгах, бизнес цэцэглэн хөгжих гол түлхүүр юм.

**МЭДЭЭЛЭЛ КОМПЬЮТЕРИЙН УХААНЫ ТЭНХИМ**

**Гар утасны програм : Өгөгдлийн нууцлал, аюулгүй байдлын тусламж**

Бакалаврын судалгааны ажил

Удирдагч: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Доктор, дэд профессор Н.Оюун-Эрдэнэ

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээлэл компьютерийн ухааны тэнхим

Шүүмжлэгч : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээлэл компьютерийн ухааны тэнхим

Гүйцэтгэсэн: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

П.Мөнхболд

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээлэл компьютерийн ухааны тэнхим