

**МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ**

**ХЭРЭГЛЭЭНИЙ ШИНЖЛЭХ УХААН, ИНЖЕНЕРЧЛЭЛИЙН СУРГУУЛЬ**

Пашкагын Мөнхболд

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

Бакалаврын судалгааны

Мэргэжил: D524300 Мэдээллийн технологи

**Улаанбаатар хот**

**2016 он**

**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

Мэдээллийн технологи 4

Гарчиг

[Гарчиг 3](#_Toc448171251)

[Товчилсон үгийн жагсаалт 5](#_Toc448171252)

[Орчуулсан үгсийн жагсаалт 6](#_Toc448171253)

[Зураг, хүснэгтийн жагсаалт 7](#_Toc448171254)

[АЖЛЫН ХУРААНГУЙ 8](#_Toc448171255)

[**НЭГДҮГЭЭР БҮЛЭГ** 10](#_Toc448171256)

[1. Онолын судалгаа 10](#_Toc448171257)

[1.1. Аюулгүй байдал 10](#_Toc448171258)

[1.2. Криптограф 12](#_Toc448171259)

[1.3. Хариу арга хэмжээ /Компьютерт суурьласан хяналт/ 17](#_Toc448171260)

[1.4. DBMS ба Вэбийн аюулгүй байдал 19](#_Toc448171261)

[1.5. Өгөгдлийн сангийн аюулгүй байдал ба админ 23](#_Toc448171262)

[1.6. SQL Injection 24](#_Toc448171263)

[1.7. Вэб програм хангамжийн судалгаа 24](#_Toc448171264)

[1.8. Гар утасны програм хангамжийн судалгаа 25](#_Toc448171265)

[1.9. Технологийн судалгаа 26](#_Toc448171266)

[1.10. Бүлгийн дүгнэлт 30](#_Toc448171267)

[2. ХОЁРДУГААР БҮЛЭГ 31](#_Toc448171268)

[**Төслийн хэсэг : Өгөгдлийн нууцлал, аюулгүй байдал гар утасны тусламж програм** 31](#_Toc448171269)

[2.1. Системийн шинжилгээ 31](#_Toc448171270)

[2.2. Системийн статик шинжилгээ 32](#_Toc448171271)

[2.3. Системийн динамик шинжилгээ 32](#_Toc448171272)

[2.4. Системийн зохиомж 37](#_Toc448171273)

[2.5. Бүлгийн дүгнэлт 38](#_Toc448171274)

[3. ГУРАВДУГААР БҮЛЭГ 38](#_Toc448171275)

[3.1. Ашигласан сангууд 38](#_Toc448171276)

[3.2. Өгөгдлийн сан 38](#_Toc448171277)

[3.3. Төслийн бүтэц 38](#_Toc448171278)

[ДҮГНЭЛТ 38](#_Toc448171279)

[НОМ ЗҮЙ 39](#_Toc448171280)

[ХАВСРАЛТ 40](#_Toc448171281)

Товчилсон үгийн жагсаалт

Орчуулсан үгсийн жагсаалт

1. Admin Админ
2. Data Өгөгдөл
3. Database Өгөгдлийн сан
4. Security Аюулгүй байдал
5. Confidentiality Нууцлалт
6. Availability Бэлэн байдал
7. Integrity Бүрэн бүтэн байдал
8. Control Хяналт
9. Access Хандалт
10. Flow Урсгал
11. Inference Дүгнэлт
12. Encryption Нууцлал
13. Measure Aрга хэмжээ
14. Application Програм
15. Gateway Гарц
16. Proxy Прокси
17. Packet Пакет
18. Filter Шүүлтүүр
19. Firewall Галтхана
20. Privacy Хувийн нууц
21. Authenticity Үнэн зөв байдал
22. non-Fabrication Дуураймал биш
23. non-Repudiation Татгалзалгүй
24. Journaling Тэмдэглэл
25. Backup Нөөц
26. View Харагдац
27. Privilege Давуу эрх
28. Threat Аюул занал
29. Framework Фрэймворк
30. Server Сервер
31. Client Клиент
32. Use case Ажлын явц
33. Sequence Дараалал
34. Activity Идэвхжилт
35. Layout Ерөнхий загвар
36. Open source Нээлттэй эхийн програм хангамж
37. Icon Шигтгээ зураг
38. Project Төсөл

Зураг, хүснэгтийн жагсаалт

АЖЛЫН ХУРААНГУЙ

1. **Оршил**

Мэдээлэл технологи харилцаа холбоо асар өндөр хөгжсөн өнөө үед хүний хэрэгцээнд нийцсэн програм хангамж болон техник хангамжуудыг бараг л бүгдийг үйлдвэрлэсэн байна. Үүнийг дагаад програм хангамжид ашиглагдах маш их өгөгдөл бий болсон бөгөөд түүний нууцлал болон аюулгүй байдалын талаар асуудлууд үүсч байна. Иймд өгөгдлийн нууцлал, аюулгүй байдалын талаарх сэдвийг энэхүү баклаварын судалгааны ажилаараа сонгон авч судалгаа шинжилгээг шат дараалалтай хийж өгөгдлийн нууцлал, аюулгүй байдалын талаарх тусламж програмыг тодорхой хэмжээнд гүйцэтгэж дууслаа.

Энэхүү боловсруулсан тайлан нь үндсэн 3 хэсгээс тогтох бөгөөд 1-р бүлэг Сэдвийн ерөнхий судалгаа, 2-р бүлэг Шинжилгээ зохиомж, 3-р бүлэг Хэрэгжүүлэлт гэсэн бүлгүүдээс тогтон.

**Нэгдүгээр бүлэг:** Энэ бүлэгт сэдвийн ерөнхий судалгааг хийсэн ба системийг хэрэгжүүлэхэд шаардлагатай технологиудыг нарийвчлан судалсан үр дүнг танилцууллаа.

**Хоёрдугаар бүлэг:** Дээрх судалгааны үр дүнд олж авсан мэдлэг дээр тулгуурлан программынхаа шинжилгээний бичиг баримтуудыг гаргасан. Шинжилгээний үр дүнд гарсан бичиг баримтууд болон харьцуулсан судалгаанаас олж авсан зүйлүүдээсээ ургуулан зохиомжоо хийсэн юм.

**Гуравдугаар бүлэг:** Энэ бүлэгт хэрэгжүүлэлтийг хийхдээ 2-р дугаар бүлэгт олж авсан шинжилгээ зохиомжийн бичиг баримтуудад тулгуурлан кодчиллыг хийж гүйцэтгэсэн

1. **Үндэслэл**

Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн нууцлалын асуудал чухлаар тавигдах болсонд өнөөгийн үед хүн бүхэн мэдээллийн нууцлалыг хэрхэн хангах талаар  цэгцтэй бөгөөд тодорхой хэмжээний ойлголттой байх хэрэгтэй.

1. **Зорилго, зорилт**

Энэхүү дипломын ажлын зорилго нь дээр дурдсан өгөгдлийн нууцлал, аюулгүй байдлын тусламж програмыг хөгжүүлэх бөгөөд зорилгодоо хүрэхийн тулд дараах зорилтуудыг тавилаа. Үүнд:

* Програм хөгжүүлэхэд ашиглах технолигиудыг судлах
* Хөгжүүлсэн програмаа туршиж сайжруулах үр дүнг дүгнэх
* Судалгааны үр дүнд тулгуурлан оюутан, сурагчидад зориулсан ухаалаг утасны програм, багшд зориулсан веб програм хангамжийг хөгжүүлэх

# **НЭГДҮГЭЭР БҮЛЭГ**

1. Онолын судалгаа

Энэ бүлэгт сонгож авсан сэдвийнхээ дагуу тулгарч болох асуудлуудаа нарийвчлан тодорхойлж, юунд хүрэх ямар систем хийх гэж зорьж буйгаа дэлгэрүүлэн судалсан юм. Мөн гар утас болон вэб програмыг хийж гүйцэтгэхийн өмнөх шаардлагатай технологи болон ойлголт онолуудыг судалсан тухай юм

* 1. Аюулгүй байдал

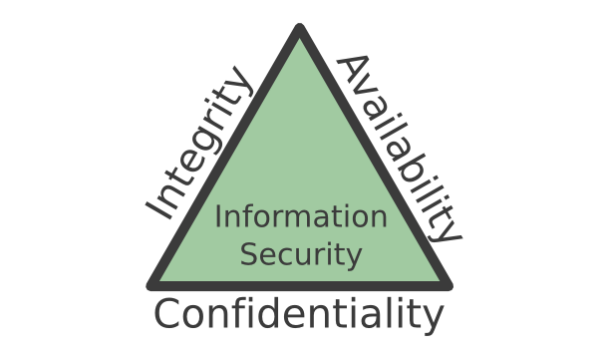
Аюулгүй байдал гэдэг нь хор хохирлоос хамгаалах эсвэл эсэргүүцэх чадварын чанар юм. Энэ нь хүн, орон гэр, эд зүйл, улс үндэстэн болон байгуулга гэх мэт эмзэг, үнэ цэнэтэй бүх зүйл дээр хэрэглэгддэг.

* + 1. Өгөгдлийн 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.

* + 1. 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.



Зураг 1 Аюулгүй байдлын загвар

* + - 1. Нууцлал

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.

* + - 1. Бүрэн бүтэн байдал

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.

* + - 1. Бэлэн байдал

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 ба саад болох зүйлийг төлөвлөж 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 нэвтэрч 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.

* 1. Криптограф

Криптограф гэдэг нь мэдээллийн аюулгүй байдлыг хангах үүднээс мэдээллийг  нууцлах, мэдээллийн бүрэн бүтэн байдал, түүний үнэн зөв өөрчлөлтгүй байдлыг хангах, зөвшөөрөлгүй хэрэглээнээс сэргийлэх зорилгоор мэдээллийг кодлох буюу хувиргах кодлолын арга зарчмыг судалдаг нэгэн төрлийн шинжлэх ухааны салбар юм. Криптограф нь нууцлалын өндөр зэрэглэлтэй санхүүгийн болон хувийн гэх мэт өгөгдлүүдийг хадгалахад өргөн хэрэглэгддэг.Криптограф нь өөртөө дараах үндсэн дөрвөн хүчин зүйлийг хамруулдаг. Үүнд:

* Мэдээллийг нууцлах
* Мэдээллийн бүрэн бүтэн байдлыг хангах
*  Мэдээллийн тасралтгүй байдлыг хангах
*  Мэдээллийг баталгаажуулах

Түлхүүр ойлголтууд:

Plaintext буюу эх текст – Энэ нь нууцлах гэж байгаа үндсэн мэдээлэл

Ciphertext – Энэ нь кодлогдсон буюу нууцлагдсан мэдээлэл

Encipher (encrypt) - Криптографд мэдээллийн нууцлалыг хангахын тулд түүнийг энкриптлэх(encrypt) буюу хөрвүүлэх гэсэн үндсэн ойлголт байдаг. Энэ нь мэдээллийн эх буюу энгийн текстийг энкриптлэсэн текстрүү хөрвүүлэх процесс юм.

Decipher (decrypt) - Энкриптлсэн текстийг буцааж эх текстрүү нь хөрвүүлэх процессийг декриптлэх гэнэ.

Ciper буюу алгоритм – Криптографд кодлох процессийг явуулахад тодорхой кодлолын алгоритмуудыг хэрэглэдэг.

Кеу буюу түлхүүр – Энкриптлэх болон декриптлэхэд ашиглагддаг түлхүүр.

Кодлолын алгоритмууд нь тусгай түлхүүрээр удирдагддагбөгөөд энэхүү нууц түлхүүр нь тухайн мэдээллийг хөрвүүлэхэд хамгийн чухал үүрэгтэй.

Криптоанализ – Энэ нь түлхүүрийг нь мэдэлгүйгээр кодлосон мэдээллээс эх мэдээллийг нь олж авах арга замын судалгаа юм. Өөрөөр үүнийг attack гэж хэлж болно.

Криптологи – Кодлол зүйн ухаан. Энд Криптограф болон Криптоанализыг хоёуланг нь судалдаг.

Криптоанализ үүнийг явуулах хоёр арга байдаг.

* Cryptoanalytic attack – алгоритмыг өөрийнх нь шинж чанар дээр тулгуурлаад эх мэдээллийг гаргаж авах
* Ciphertext  only – алгоритм болон шифрлэсэн текстээс эх мэдээллийш гаргах
* Known plaintext – эх текстийн хэсэг болон шифрлэсэн текстийн тусламжтай
* Chosen plaintext – эх текстийг сонгож
* Chosen ciphertext – шифрлэсэн текстийн тодорхой хэсгийг ашиглаад
* Chosen text – эх болон кодлосон текстийн хэсгийг ашиглаад
* Brute force attack – бүх боломжит түлхүүрийг туршиж үзэх, энэ нь хамгийн суурь аттак бөгөөд түлхүүрийн хэмжээнээс шууд хамааралтай байдаг.

Криптографийн системийг дотор нь хэд хэдэн зүйлээр ялгаж үздэг:

* Кодлох процессыг явуулж байгаа төрлөөр нь
* Substitution буюу орлуулах
* Transposition буюу шилжүүлэх
* Product буюу хосолсон
* Хэрэглэгдэж байгаа түлхүүрийн тоогоор нь
* Private key буюу нэг түлхүүр ашигладаг
* Public key буюу хос түлхүүр ашигладаг
* Эх текстийг хэрхэн боловсруулж байгаа аргаар нь
* Block – мэдээллийг блокуудад хуваасны дараа боловсруулдаг
* Stream – мэдээллийг бит битээр нь эсвэл байт байтаар нь боловсруулдаг

Тэгш хэмт буюу Symmetric кодлолын арга (private key)

Энэ кодлолын алгоритмд кодлох болон кодыг тайлах процесст нэг ижил түлхүүрийг

ашигладаг. Өгөгдлийг энкриптлэх ба декриптлэх хоёр талууд ашиглах шифлэлтийн

түлхүүрээ урьдчилсан тохирдог. Симметрик түлхүүрийн шифрлэлт нь ассиметрик

түлхүүрийн шифрлэлтээс хурдан боловч түлхүүрийг солилцох шаардлагатай байдаг учир эмзэг байдлын түвшин өндөр байна.

Тэгш хэмт кодлолын алгоритмд аюулгүй байдлын хоёр шаардлага байдаг:

Найдвартай кодлолын алгоритм хэрэглэх

Түлхүүрийн нууцллалыг маш сайн хангах

Тэгш хэмт кодлолын арга:

* Классик – өмнөх үеийн кодлолын алгоритм

Орлуулах (substitution) – энэ нь эх текстийн үсгүүдийг өөр үсэг, тоо, тэмдэгтээр орлуулан солидог арга юм.

Шилжүүлэх (transposition) – энэ аргад тухайн текстийн үсгүүдийг хооронд нь байрыг нь сольдог алгоритм бөгөөд энэ үед тухайн үсгийн давтамжийн тархалт хэвээр хадгалагддаг.

* Rail fence
* Мөрөөр шилжүүлэх арга гэх мэт

Хосолсон (product) – энэ нь орлуулах болон шилжүүлэх алгоритмуудыг дарааллан хэрэглэх замаар кодлодог. Ингэснээр давтамжийн тархалтыг багасгадаг бөгөөд эндээс орчин үеийн кодлолын алгоритмууд гарсан.

* Rotor machine
* Steganography
* Data encryption – орчин үеийн кодлолын алгоритм

Block cipher algorithm – багцын шифрийн алгоритм нь өгөгдлийг багц багцаар нь кодлодог бөгөөд мэдээллийн аюулгүй байдал болон нууцлалыг хангахад өргөн хэрэглэгддэг. Энэ нь өгөгдлийг 64 битээр кодлодог. Багцын шифрийн алгоритм нь Feisel –ийнcipher бүтэц дээр үндэслэн гарч ирсэн. Энэ нь тухайн бүтцээрээ өгөгдлийг кодлоод түүгээрээ тайлах боломжтой систем байсан. Feisel-н бүтцийн суурь чанар нь product шифр юм. Мөн Feisel-н шифр нь Claude Shannon –ы санаан дээр үндэслэсэн.Энэ хүн нь кодлолын техникт ашиглагддаг 2 гол аргыг(орлуулах болон шилжүүлэх) ашигласан сүлжээг ашиглах замаар кодлодог. (S&P network)

Энэ бүтцийг ашиглаад 2 ойлголт гаргасан:

1.      Diffusion буюу сарниулах – энэ нь сүлжээгээр кодлогдсон мэдээлэл болон эх

мэдээллийн хоорон дахь статистик хамаарлыг алга болгодог, өөрөөр хэлбэл давтамжийн тархалтыг алга болгодог

2.   Confusion буюу будлиулах – энэ нь кодлосон мэдээлэл болон түлхүүр хоорондын хамаарлыг алга болгодог

Эдгээр санааг ашиглан Feisel өөрийн шифрийн бүтцийг санал болгосон. Feisel нь эх

текстийг зүүн баруун хоёр хэсэгт хуваагаад n үеэр кодлодог. Үе болгонд ялгаатай дэд түлхүүрийг ашигладаг.

 Data encryption standard (DES) – энэ нь Feisel-н шифр дээр тулгуурлан гарч ирсэн

стандарт. 1977 онд стандарт болсон. Өгөгдлөө 64 битээр, түлхүүрээ 56 битээр сонгож авсан. 64 бит байсныг 56 байхаар сонгосон нь түлхүүрийг нэг чипэд багтдаг байхаар сонгосон.  16 үетэй бөгөөд мөн үед бүртээ ялгаатай түлхүүртэй. Баруун зүүн 2 хэсэгтэй бөгөөд эхлэхдээ битүүдээ сэлгэлт хийдэг, дууссаны дараа мөн хоёр талыг хооронд нь сэлгэлт хийдэг.

Triple DES – энэ нь DES –г гурван удаа гурван өөр түлхүүртэйгээр гүйцэтгэдэг алгоритм.

    AES (Advanced Encryption Standard ) – Triple DES-н дараагийн стандарт

Тэгш хэмт бус буюу Asymmetric кодлолын арга (public key)

Хос түлхүүрт кодлолын алгоритм нь тэгш хэмт кодлолын алгоритмыг арилган гарч ирсэн. Тэгш хэмт кодлолын алгоритмд хэрэглэгчид хоорондоо түлхүүрээ солилцдог дутагдалтай талтай бөгөөд тухайн мэдээлэл нь баталгаатай эх сурвалжаас ирсэн гэсэн мэдээллийг баталгааг хангах боломжгүй байдаг. Хос түлхүүрт кодлолын алгоритмд хүлээн авагч болон дамжуулагч нь ялгаатай түлхүүрийг хэрэглэдэг учраас илүү найдвартай болсон.Нийтийн түлхүүрт алгоритмд баталгааг хангахдаа хувийн түлхүүрээр кодлог дамжуулж нийтийн түлхүүрээр тайлж болдог.

Түлхүүр:

Private key(хувийн түлхүүр): тухайн хэрэглэгч л мэдэх түлхүүр

Public key(нийтийн түлхүүр): хүн болгонд тараадаг түлхүүр

Тэгш хэмт бус кодлолын алгоритмыг гурван категорт хэрэглэдэг:

 Мэдээллийн нууцлалыг хангахад

Тоон гарын үсгийг хэрэгжүүлэх буюу мэдээллийн баталгааг хангах

Түлхүүр солилцох – тэгш хэмт алгоримтын үед түлхүүрээ аюулгүй дамжуулахад ашигладаг.

Баталгаа болон нууцлалыг зэрэг хангаж болох бөгөөд ингэхдээ эхлээд хувийн түлхүүрээр кодлож дараа нь хүлээн авагчийн нийтийн түлхүүрээр кодлож дамжуулна. Дутагдалтай тал нь тооцоолол хийхэд удаан байдаг.

·         RSA – Rivest Shamir & Adleman

Энэ нь томоохон хэмжээний бүхэл тоонуудын тооцоолол дээр үндэслэн гаргаж авсан алгоритм юм. Түлхүүрийн хэмжээ нь1000bit-ээс илүү байдаг.Энэ алгоритм нь том хэмжээний тоонуул дээр тооцоолол хийдэг учраас Brute Force-н attack-д тэсвэртэй байдаг.

* Diffie – Hellman

Нууц түлхүүрийг солилцоход ашиглагддаг public key алгоритмуудын нэг.

* HASH – нэг чиглэлтэй функц. Аргументдаа янз бүрийн урттай мессеж авч болдог. Hash-н хэмжээ нь тогтмол байна.
  1. Хариу арга хэмжээ /Компьютерт суурьласан хяналт/
     1. Эрх олгох

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

* + 1. Хандалтыг хянах

Өгөгдлийн сангийн системд хандалтын хяналтыг хангах нийтлэг арга зам нь эрх олгох , давуу эрхийг хүчингүй болгох юм.

* + 1. Харагдац

Харагдац бол нэг эсвэл олон харилцаан дээр оператор үйл ажилгагаа явуулж динамик үр дүн авдаг.

* + 1. Нөөц

Тогтмол хугацаанд өгөгдлийн сангийн хуулбар болон бүртгэлийн файлыг офлайн агуулахад хадгалах үйл явц юм.

* + 1. Нууцлал

Өгөгдлийг онцгой алгоритм ашиглан шифрлэлтийг буцаах түлхүүргүйгээр ямар ч програмд өгөдлийг уншигдахгүй болгоно

* + 1. RAID технологи

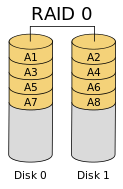
RAID (redundant array of independent disks) гэдэг нь нэг ижил мэдээллийг хэд хэдэн хатуу дискэд зэрэг хуулах технологийг хэлдэг. RAID-ийг үндсэн хоёр зорилгоор ашигладаг.

1. Хэрэв компьютерт маш чухал, үнэ цэнэтэй мэдээллүүд байгаа бол тэдгээрийг давхар нөөц байдлаар байнга хадгалж байх
2. Зэрэг хэд хэдэн хатуу диск ашигласнаар өгөгдөл хуулах, дамжуулах хурдыг нэмэгдүүлэх явдал юм. Өөрөөр хэлбэл нэг бол мэдээллийг нөөцөлж хадгалах, эсвэл компьютерийн мэдээлэл хуулах, зөөх хурдыг нэмэгдүүлэх зорилгоор ашиглана.

Хэд хэдэн хатуу дисктэй бол энэ хоёрыг аль алиныг нь дэмждэг байхаар ч хийж болно. RAID-ийг үүсгэсний дараа үйлдлийн систем RAID-ийг нэг хатуу диск байдлаар танидаг байна.Ерөнхийдөө маш чухал мэдээллүүдтэй харьцдаг эмнэлэг, цэргийн байгууллагын компьютерууд, сервер компьютеруудад RAID-ийг өргөнөөр ашигладаг бөгөөд одоохондоо энгийн хэрэглээний компьютеруудад нэг их шаардлагагүй.  RAID нь нилээд хэдэн төрлийн байх бөгөөд энгийн хэрэглээнд ихэвчлэн хэрэглэгддэг төрлүүдийнх нь талаар тайлбарлая.

**RAID-0 :**

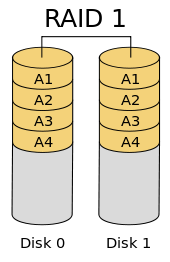
Мэдээллийг хатуу дискүүдэд давхар бичих боловч нөөцлөх гэсэн ойлголт байхгүй. Өөрөөр хэлбэл хоёр хатуу дискийг RAID-0 байдалтай холбоход үйлдлийн системд нэг хатуу диск байдлаар харагдах бөгөөд мэдээллийг хоёр хатуу диск хуваан хуулдгаараа мэдээллийн бичих болон унших хурдыг бараг 2 дахин ихэсгэх боломжтой юм. Харамсалтай нь хатуу дискний аль нэг дээрх эвдрэл нь нийт мэдээллийг ажиллагаагүй болгох аюултай.

****

**Зураг 2 RAID-0**

**RAID-1 :**

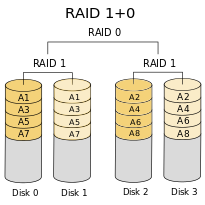
Disk mirroring  буюу “Диск хуулбарлах” гэж мөн нэрлэгдэх бөгөөд 2 болон түүнээс дээш хатуу дискүүдийг RAID-1 байдлаар холбох боломжтой. Мэдээллийг унших хурд нэмэгдэх бөгөөд бичих хурдны хувьд дан ганц дискний хурдтай ижил байна. Бичих явцад мэдээллийг нөөцөлж явдаг учраас мэдээлэл гэмтэх, устгагдах гэх мэтийн алдаа гарна гэсэн ойлголт бараг байхгүй.

****

**Зураг 2 RAID-1**

**RAID-10 :**

RAID-0 болон RAID-1-ийг хослуулан хэрэглэснийг RAID-10 гэх бөгөөд ерөнхийдөө RAID-0 болон RAID-1-ээс илүү өндөр хурдтай, найдвартай ажиллагаатай боловч өндөр зардал шаарддаг. Дотроо RAID-0+1, RAID-1+0 гэсэн төрлүүдтэй.

****

* 1. 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, JavaScript / VBScript , эсвэл нэг буюу хэд хэдэн Java апплет хяналтыг агуулж болно. 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
    1. Прокси сервер

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
   * 1. Галт хананууд

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 :
* Програмын гарц :

Тодорхой програмууд FTP болон Telnet гэх мэт аюулгүй байдлын механизмыг хэрэглэнэ. Энэ нь маш үр дүнтэй боловч үйл ажилгааг бууруулдаг

* Circuit түвшний гарц:

TCP эсвэл UDP холболт тогтоосон үед аюулгүй байдлын энэ арга замыг мөрдөнө. Холболт хийгдсэний дараа , пакетуудыг шалгалгүй хоструу урсгаж чадна.

* + 1. Зурвас эмхэтгэл алгоритмууд ба дижитал гарын үсэг
       1. Тоон гарын үсэг гэж юу вэ?

Цахим баримтад зурагдсан гарын үсэг буюу тоон гарын үсэг нь хэвлэмэл материалд үзгээр зурсан гарын үсэгтэй ижил үүрэг, зорилготой баталгаажуулалтын нэг арга, хэлбэр бөгөөд дараах 2 зүйлийг баталгаажуулдаг мэдээлэл юм. Үүнд:

* Цахим баримт буюу файлд гарын үсэг зурсан этгээд буюу эзэн, хариуцагч нь хэн бэ гэдгийг,
* Тухайн файлд гарын үсэг зурагдсанаас хойш санаатай болон санамсаргүй байдлаар ямар нэгэн өөрчлөлт ороогүй эсвэл эвдрээгүй гэдгийг,

Зарим тохиолдолд, энэ мэдээллийг тухайн файлаас нь салгах боломжгүйгээр түүнд хавсаргасан байдаг. Өөрөөр  хэлбэл, ямар нэгэн файл үүсгэхэд түүний нэр, хэмжээ, төрөл, үүсгэсэн, өөрчилсөн огноо зэрэг мэдээлэл нь файлын агуулгад биш гэхдээ дайвар байдлаар тухайн файлтайгаа хамт байдагтай адил зүйл.

Дараах зүйлсийг тоон гарын үсэгт тооцохгүй. Жишээлбэл:

* Ямар нэгэн материал дээр үзгээр гарын үсгээ зураад тухайн материалаа скайнэрдэж эсвэл фото зургийг нь авч цахим хэлбэрт оруулсан хуулбар
* Зурмал гарын үсэг бүхий факс
* Ямар нэг баримтын агуулга дотор скайнэрдаж оруулсан, зурмал гарын үсгийн зураг
* Цахим шууданд хавсаргасан, зурмал гарын үсгийн зураг гэх мэт

Эдгээр нь тоон гарын үсэгтэй ямар ч хамааралгүй, зүгээр л нэг файл, дүрс, тэмдэгт бөгөөд хүмүүсийн ихэнхи нь эдгээр хэлбэрийг тоон гарын үсэг гэж бодож төөрөлддөг. Харин эдгээр арга, хэлбэрийг тоон гарын үсгийн мөрөөдлийн, зөгнөлт хэлбэр гэж үзэх нь бий. Үнэн хэрэгтээ, эдгээр мэдээлэл нь тухайн баримтын үнэн худал болон хариуцагчийг бүрэн баталгаажуулдаггүй тул хүчин төгөлдөр гарын үсэг хэмээн тооцож ашиглах боломжгүй юм.

* + - 1. Тоон гарын үсэг нь яагаад чухал гэж вэ?

Цахим баримт бичиг буюу файлд гарын үсэг зураагүй тохиолдолд хэзээ ч тухайн файлыг албан ёсны хэмээн тооцох боломжгүй, учир нь тухайн файл жинхэнэ хувь нь мөн эсэхэд болон жинхэнэ эзэн, хариуцагч нь хэн гэдэгт итгэх боломжгүй. Өөрөөр хэлбэл, хүн төрөлхтөн цахим тооцоолуур, цахим систем болон цахим баримт үүсгэн ашиглаж байгаа хэдий ч хэвлэмэл цаасан материалаас үргэлж хамааралтай, албан хэрэглээндээ ашигласан хэвээр байх бөгөөд учир нь өөрсдийн үүсгэсэн цахим зүйлсдээ бүрэн итгэл хүлээлгэхгүй байгаад оршино. Энэ нь бид хэзээ ч албан болон хувийн хэрэгцээндээ цаасгүй цахим системийг бүрэн байгуулах боломжгүй гэсэн утгатай.

Жишээлбэл, хэрвээ та төрийн ямар нэгэн байгууллагатай харьцах шаардлага үүсээд баримт, материалаа онлайнаар илгээгээд дараа нь тухайн материалынхаа цаасан хэлбэрийг нь өөрийн биеэрээ хүргэж өгсөн ч таны цахим материалын эзэн-хариуцагч нь та өөрөө мөн гэдэгт, таны материалын утга агуулга үнэн зөв гэдэгт итгэх боломжгүй. Өөр нэг жишээ, тухайлбал та зээлийн материалаа цахим шуудангаар банк руу илгээсэн тохиолдолд таны зээлийн материалд банк итгэх боломжгүй учир нь тухайн баримт, материалын эзэн-хариуцагч нь хэн болох мөн мэдээлэл нь луйврын эсэх нь баталгаагүй.Ямар нэгэн цахим баримт бичгийн эзэн-хариуцагч нь хэн гэдэг бодит бие хүн болохыг тогтоож, тэрхүү бодит бие хүн болон цахим баримт бичиг хоорондын салшгүй хамаарлыг зөвхөн тоон гарын үсэг л баталгаажуулж чадна. Иймээс, цахим ертөнцөд итгэлцэл, аюулгүй байдлыг бий болгох, цахим нийгэм (цахим засаглал, цахим бизнес, цахим боловсрол, цахим эмнэлэг, цахим сургууль гэх мэт)-ийг байгуулахад чиглэсэн, бие хүнийг бүрэн төлөөлөх тоон мэдээллийг үүсгэх, хөгжүүлэх үндсэн арга, хэрэгсэл нь тоон гарын үсэг юм.

* + - 1. Хайш функц гэж юу вэ?

Энэхүү функцын ажиллагаа нь цахим баримтыг өөрийн аргаар уншиж шинжлээд түүнээс бичил мэдээлэл үүсгэнэ. Хялбаршуулан адилтгаж ойлговол, энэхүү функцын үйлдэл нь ямар нэгэн юмнаас сорьц, дээж авч орц, найрлагыг нь тогтоох үйлдэл, тухайлбал ДНК-ын шинжилгээ авч, хариуг нь гаргахтай төстэй зүйл юм.  Файлын хэмжээнээс үл хамаарч “найрлага”-ны хэмжээ нь ижил байна. Ялгаатай 2 файл ижил найрлага үүсгэх боломжгүй. Нэг тэмдэгт өөрчилсний дараа хайш функцээр шинжлэхэд “найрлага” нь өөрчлөгдсөн байна. Харин өөрчилсөн тэмдэгтээ буцааж хэвэнд нь оруулаад хайш функцээр уншуулахад “найрлага” анхны байдалдаа орно. Энэ функцын гол онцлог нь “найрлага” буюу хайшаас эх мэдээллийг нь гарган авах боломжгүй буюу нэг чиглэлтэй үйлдэл бөгөөд ямар нэгэн нууцлагч, нууц тайлагч түлхүүр ашигладаггүй.

* + - 1. Тэгш хэмт бус криптограф гэж юу?

Тэгш хэмт криптограф нь нууцлах, нууцыг тайлах үйлдэлдээ ижил буюу нэг түлхүүр ашигладаг бол тэгш бус хэмт нь хоорондоо математик хамааралтай хос түлхүүртэй ба алийг нь ч ашиглан нууцлаж болно. Гол онцлог нь нууцлахад ашигласан түлхүүрээрээ буцаагаад нууцаа тайлах боломжгүй ба зөвхөн нууцлагч түлхүүрийн нөгөө түлхүүрээр нь нууцыг тайлдаг. Хүн бүрт нууцлагч хос түлхүүр байх бөгөөд нэгийг нь хувийн буюу нууц түлхүүр гэх ба зөвхөн тухайн хүн л мэднэ, нөгөөг нь нийтийн буюу нээлттэй түлхүүр гэх ба түүнийг нь бүх хүн мэднэ. Хос түлхүүрийн аль нэгнээр нь нууцлагдсан мэдээллийг зөвхөн тэр хос түлхүүрийн нөгөөг нь ашиглаж л нууцыг тайлна. Хүн бүрийн мэддэг нийтийн буюу нээлттэй түлхүүрээс нь хувийн буюу нууц түлхүүрийг олж авах боломж бараг үгүй.

Нууц болон нээлттэй түлхүүрийн хосыг үүсгэх, мэдээллийг нууцлах, нууцыг тайлах арга буюу алгоритм нь математик тооцоолол дээр үндэслэгддэг. Алгоритмыг ойлгох нь хүндрэлтэй биш ч энэ тухай энд дурдахгүй бөгөөд тэгш бус хэмт криптограф нь нууцлалын хувьд илүү гэдгийг мэдэхэд үндсэн санаа оршино.

* 1. Өгөгдлийн сангийн аюулгүй байдал ба админ

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.

* 1. SQL Injection
  2. 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
  1. 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.

* 1. Технологийн судалгаа

Энэхүү хэсэгт системийн хэрэгжүүлэлтэд ямар технологиудыг ашиглах тэдгээр технологиудын давуу болон сул талуудыг харьцуулж харуулахыг зорьсон болно. Мөн зарим нэг шинэ технологиудыг ашигласан ба тэдгээрийн талаарх дэлгэрэнгүй мэдээллийг орууллаа.

* + 1. Андройд системийн судалгаа

Андройд бол мэдрэгчтэй дэлгэцтэй ухаалаг гар утас ба таблет зэрэг хөдөлгөөнт хэрэгслүүдэд зориулан бүтээгдсэн, Линукст тулгуурласан үйлдлийн систем юм. Андройд үйлдлийн систем бол нээлттэй эх бөгөөд Жава програмчлалын хэлд үндэслэгдэн хийгдсэн. Андройдыг Android, Inc хөгжүүлдэг ба Google 2005 оноос худалдан авч хөгжүүлж эхэлсэн. Андройд нь 2007 он хүртэл олон нийтэд ил гараагүй байсан ба нээлттэй гэрээний ачаар харилцаа холбооны компаниуд гар утсанд үйлдлийн систем болгон ашиглаж эхэлсэн. 2008 оны аравдугаар сард анхны андройд утас худалдаанд гаран зарагдаж байсан. Андройд нь нээлттэй эх бөгөөд Google нь Apache License-н доор гарган авсан. 2015 оны 10-р сард 1100000 андройд апликейшн байгаа бөгөөд Google Play-с эдгээр апликейшнүүд нь 25 тэр бум удаа татагдсан байна.

Андройд хувилбарууд :

* Cupcake (1.5)
* Donut (1.6)
* Ecliar (2.0-2.1)
* Froyo (2.2-2.2.3)
* [Gingerbread](https://en.wikipedia.org/wiki/Android_Gingerbread) (2.3–2.3.7)
* [Honeycomb](https://en.wikipedia.org/wiki/Android_Honeycomb) (3.0–3.2.6)
* [Ice Cream Sandwich](https://en.wikipedia.org/wiki/Android_4.0) (4.0–4.0.4)
* [Jelly Bean](https://en.wikipedia.org/wiki/Android_Jelly_Bean) (4.1–4.3.1)
* [KitKat](https://en.wikipedia.org/wiki/Android_KitKat) (4.4–4.4.4, 4.4W–4.4W.2)
* [Lollipop](https://en.wikipedia.org/wiki/Android_Lollipop) (5.0–5.1.1)
* [Marshmallow](https://en.wikipedia.org/wiki/Android_Marshmallow) (6.0)
  + 1. 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

Андройд хөгжүүлэлтийн амьдралын цикл



* + 1. 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

* + 1. 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.

* + 1. 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

* + 1. MySQL

MySQL нь өгөгдлийг удирдах менежментийн систем юм. MySQL хэмээх нэрний хувьд уг системийг санаачлан хөгжүүлэгч Micheal Widenius-ын охины нэр My + SQL(Structed Query Language) гэсэн утгатай ажээ. Энэ систем нь GNU (General Public License) буюу нээлттэй эхийн систем учир хүссэн хэн бүхэн хөгжүүлэлтэнд оролцож, үнэгүй хэрэглэж болох юм. Эзэмшигч нь алдарт Java-г хөгжүүлсэн Sun MicroSystems компани байсан ба, одоогоор Sun-г Oracle корпорац эзэмших болсон билээ. Үнэгүй програм хангамжийн өгөгдлийн санг удирдах системд ихэвчлэн MySQL-ийг хэрэглэдэг бөгөөд тэдгээрийн сонгодог жишээ гэвэл Joomla, Drupal, Wordpress, phpBB гэх мэт агуулга удирдах системүүд (CMS-Content Management System), Wikipedia, Facebook, Google гэх мэт гигантууд юм. Хөгжүүлэлт нь C/C++ хэл дээр хийгдсэн ба AIX, BSDi, FreeBSD, HP-UX, i5/OS, Linux, Mac OS X, NetBSD, Novell NetWare, OpenBSD, OpenSolaris, eComStation, OS/2 Warp, QNX, IRIX, Solaris, Symbian, SunOS, SCO OpenServer, SCO UnixWare, Sanos, Tru64, Microsoft Windows гэсэн олон үйлдлийн системүүд дээр ажилладаг.

* + 1. 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
  1. Бүлгийн дүгнэлт

Энэ бүлэгт системээ хэрэгжүүлэхэд зайлшгүй хэрэгтэй зүйлсийн талаарх технологи болон мэдээллийн судалгаа хийлээ. Энэхүү судалгаанаас ашиглах гэж байгаа технологиудынхаа бусад технологиудаас юугаараа давуу, юугаараа сул, хоорондоо яаж зохицож ажилладаг зэргийг мэдэж авлаа.

1. ХОЁРДУГААР БҮЛЭГ

## **Төслийн хэсэг : Өгөгдлийн нууцлал, аюулгүй байдал гар утасны тусламж програм**

* 1. Системийн шинжилгээ

Системд хэрэглэгч, админ гэсэн 2 төрлийн тоглогч байх ба тус бүрдээ өөр өөр эрх, өөр өөр хийх үйлдэлтэй байна. Хэрэглэгч нь гар утасны програмыг ашиглах бол админ нь веб програмыг ашиглах юм.

* + 1. Хэрэглэгчийн функциональ шаардлага

**Хэрэглэгч :**

Хэрэглэгч нь гар утасны програм ашиглах бөгөөд дараах үйлдлүүдийг хийнэ.

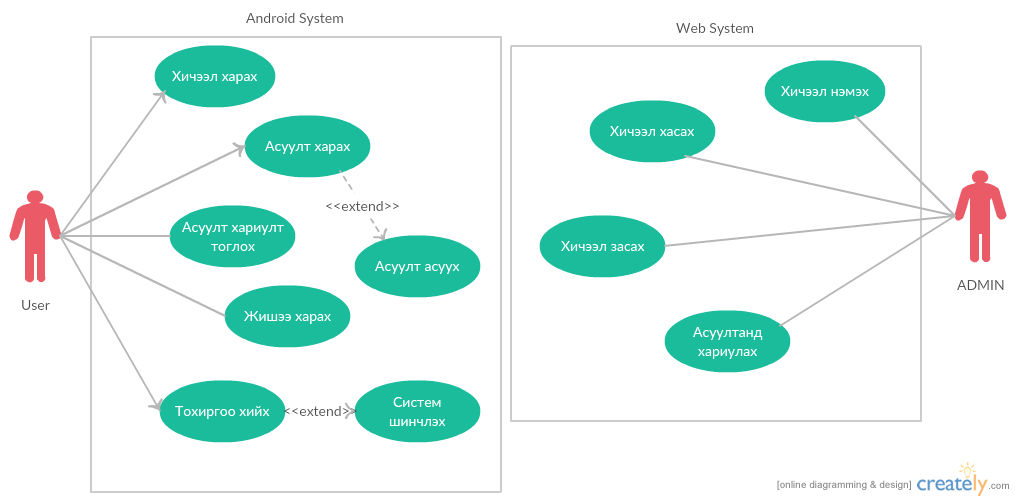
* Хичээл харах
* Асуулт харах
* Асуулт асуух
* Асуулт хариулт тоглох
* Жишээ харах
* Тохиргоо хийх
* Шинчлэл хийх

**Админ :**

Системийг админ веб програмыг ашиглан удирдах бөгөөд админ нь дараах эрх үүргүүдтэй байна.

* Хичээл нэмэх
* Хичээл хасах
* Хичээл засах
* Асуулт нэмэх
* Асуулт хасах
* Асуултанд хариулах
  + 1. Хэрэглэгчийн функциональ бус шаардлага
* Үйл ажиллагааны
* Хэрэглэгчид зориулсан програм нь ямар ч төрлийн андройд үйлдлийн системтэй төхөөрөмж нь дээр ажилладаг байна.
* Админий систем нь уян хатан загвар бүхий гар утсанд ээлтэй(mobile friendly)зарчмыг хангасан байна.
* Гүйцэтгэл
* Энэхүү систем нь энгийн , ойлгомжтой цөөн үйлдлүүдтэй байх
* Хамгаалалт нууцлал
* Зарим чухал нууцлалтай мэдээллүүдийг нууцлал(encryption) хийж хадгална.
* Соёл
* Мэдээлэл үнэн байх
  1. Системийн статик шинжилгээ
     1. Классын диаграм
     2. Обьектын диаграм
     3. Туршилтын загвар
  2. Системийн динамик шинжилгээ
     1. Ажлын явцын диаграм

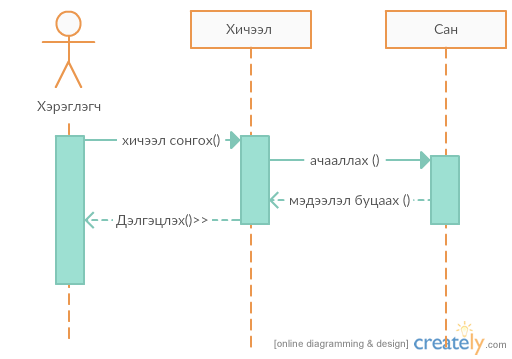
Тус системд хэрэглэгч нь хичээл харах, асуулт харах, асуулт асуух, асуулт хариулт тоглох, жишээ харах, программыг шинчилдэг байна. Админ хэрэглэгч нь хичээл нэмэх, хасах, засах ба хэрэглэгчээс ирсэн асуултанд хариулдаг байна. Системийн үйлдлүүдийг ажлын явцын диаграммаар дүрсэлбэл доорх диаграммд үзүүлсэн хэлбэрээр дүрслэгдэнэ.



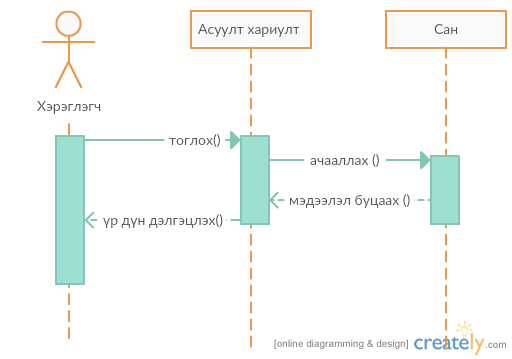
Зураг Ажлын явцын диаграм

* + 1. Дарааллын диаграм

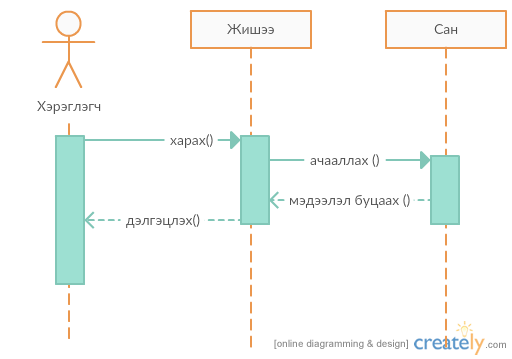
Дарааллын диаграмыг ажлын явц бүрийн хийгдэх үйлдлийн дараалал болон тэдгээрт оролцох обьектуудыг тодорхой нарийвчилж гаргаж өгдөг. Мөн тухайн обьектийн үүсэх хугацаа, устах хугацааг нарийвчлан харуулдаг диаграм юм. Иймд дарааллын диаграмыг ажлын явц бүрд нарийвчилж зурж өгөх нь тохиромжтой байдаг. Дараах диаграмуудыг чухал гэсэн ажлын явцуудыг нарийвчлан дарааллын диаграммыг тус бүрд нь зурлаа



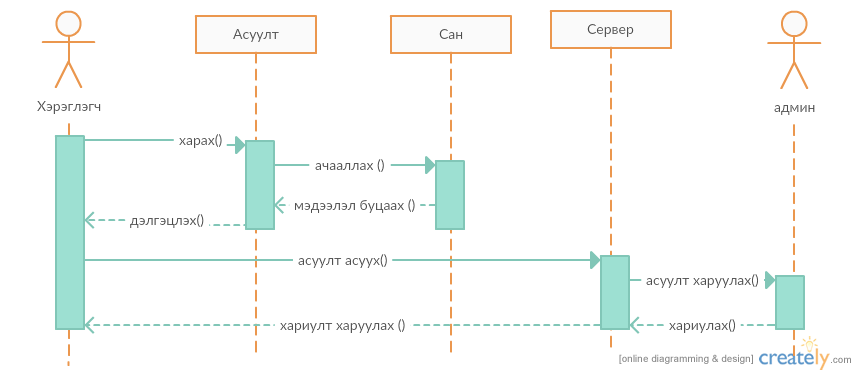
Зураг Хичээл харах дарааллын диаграм



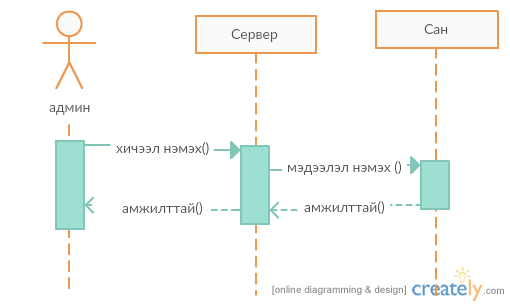
Зураг Асуулт хариулт тоглох дарааллын диаграм



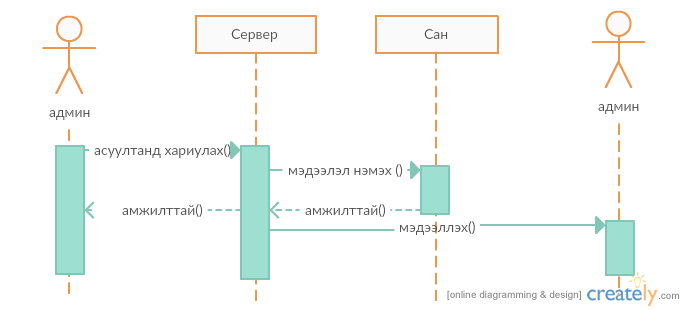
Зураг Жишээ харах дарааллын диаграм



Зураг Асуулт асуух дарааллын диаграм



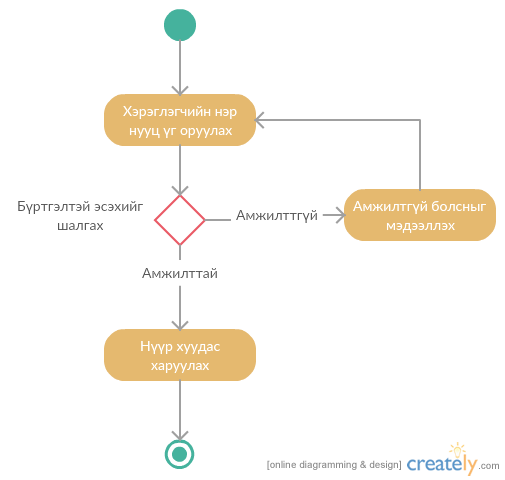
Зураг Админ хичээл нэмэх дарааллын диаграм



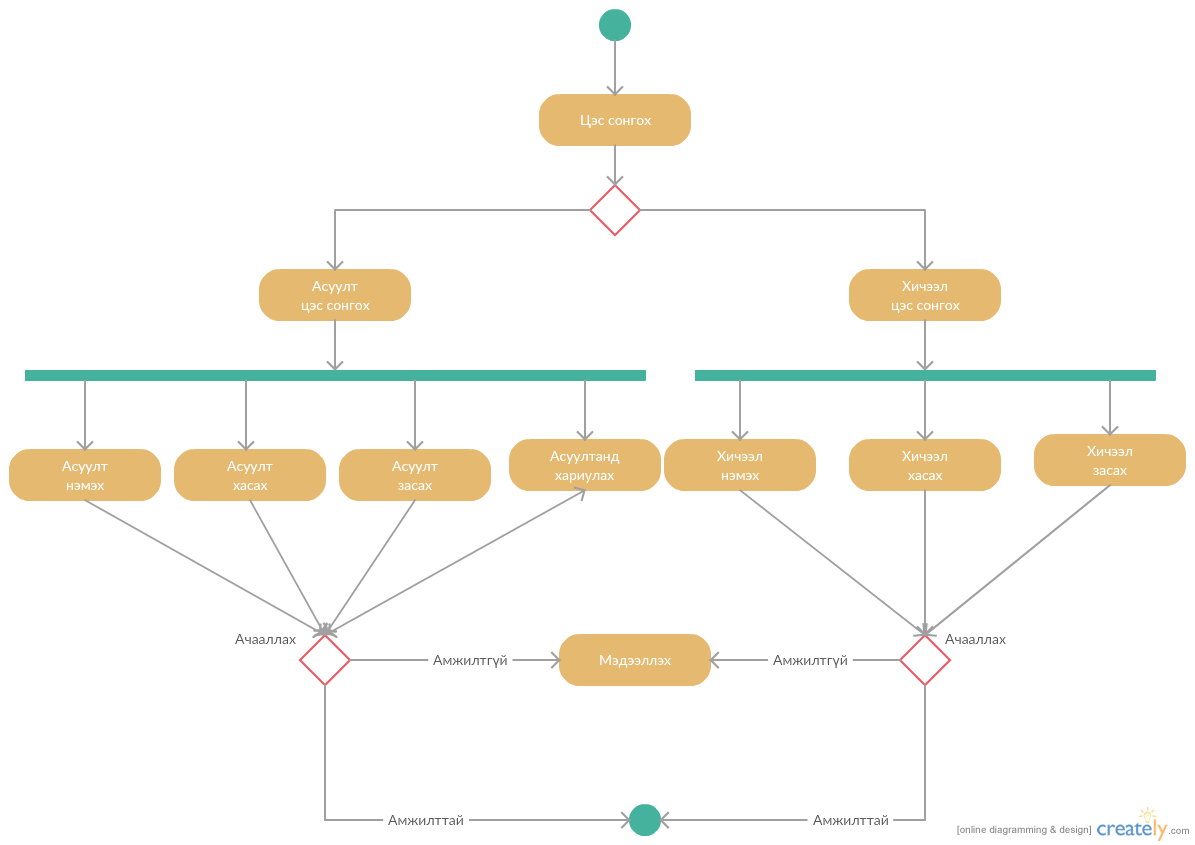
Зураг Админ асуултанд хариулах дарааллын диаграм

* + 1. Үйл идэвхжилтийн диаграм

Үйл идэвхжилтийн диаграм нь тухайн системийн төлөв байдал болон тэдгээрийн идэвхжилт, шилжилтийг харуулдаг диаграм юм. Энэхүү диаграм нь дүрслэх шаардлагатай нөхцөлүүдийг дүрслэх боломжтой бөгөөд нөхцөл бүрээс хамааран гарах үр дүнг тодорхой харуулдаг. Дараах диаграмуудыг чухал гэсэн ажлын явцуудыг нарийвчлан үйл идэвхжилтийн диаграммыг тус бүрд нь зурлаа.

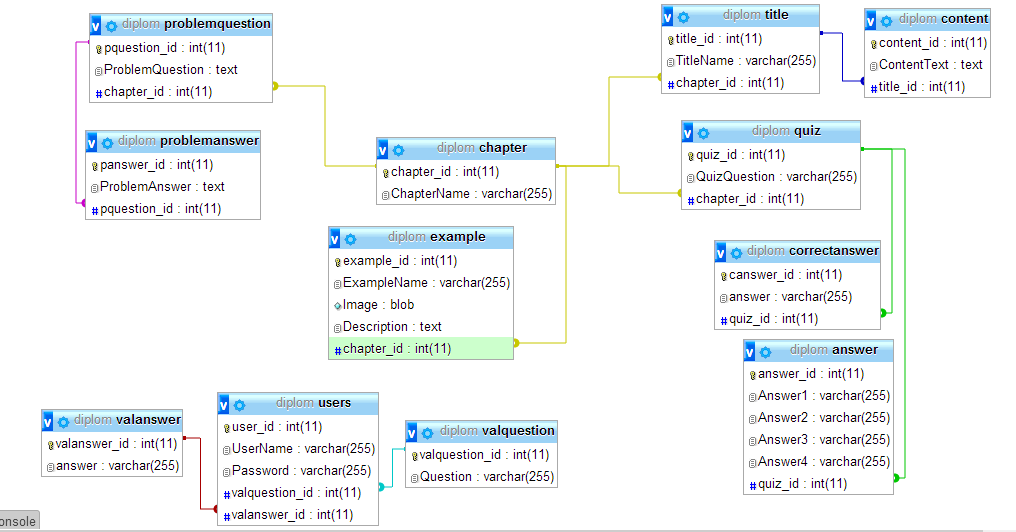


Зураг Админ системд нэвтрэх хэсгийн идэвхжилтийн диаграм



Зураг Админий хийх үндсэн үйлдлүүдийн идэвхжилтийн диаграм

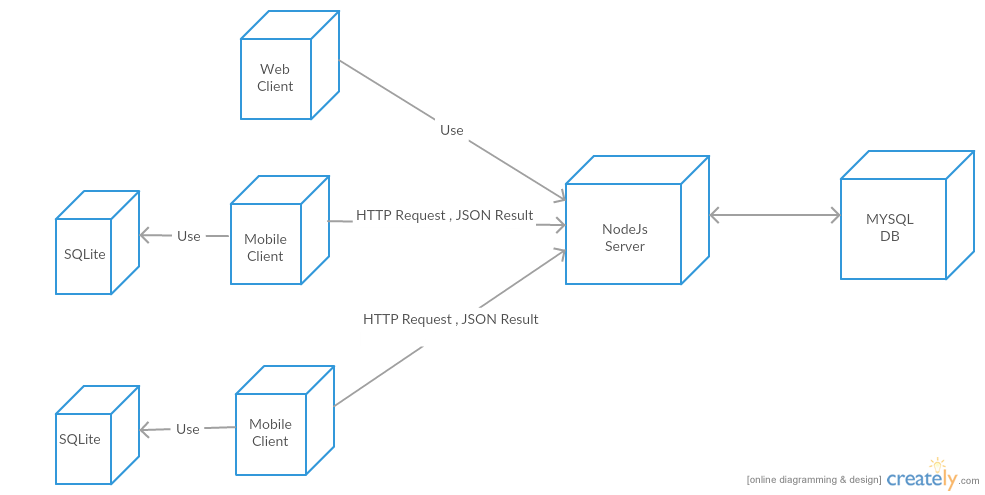
* 1. Системийн зохиомж
     1. Өгөгдлийн сангийн зохиомж



Зураг Харьцаат өгөгдлийн сангийн зохиомж

* + 1. Архитектүрын зохиомж

Системд гар утасны клиент болон вэб клиент-ууд байх ба NodeJS сервертэй харьцаж ажилна. Вэб сервер нь МуSQL өгөгдлийн сангийн системээс өгөгдлөө авна. Мөн гар утасны систем нь оффлайн горимд файлд суурилсан өгөгдлийн сан болох SQLite-аас өгөгдлөө аван ажиллана.



Зураг Архитектурийн диаграм

* + 1. Хэрэглэгчтэй харьцах хэсгийн зохиомж
       1. Шилжилтийн диаграм
       2. Уян хатан загвар
       3. Туршилтын загвар
       4. Шигтгээ зураг зурах
  1. Бүлгийн дүгнэлт

1. ГУРАВДУГААР БҮЛЭГ
   1. Ашигласан сангууд
   2. Өгөгдлийн сан
   3. Төслийн бүтэц

ДҮГНЭЛТ

НОМ ЗҮЙ

1. Доктор, Проф. Ж.Пүрэв, Улаанбаатар 2004 он, Ажлын төсөл бичих аргачлал
2. Database Security (Alfred Basta and Melissa Zgola)
3. Database system, 4th Edition
4. Fundamentals of Database Systems, 6th Edition
5. https://nodejs.org/en/
6. https://jquery.com/
7. http://getbootstrap.com/
8. https://www.sqlite.org/

ХАВСРАЛТ