МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ

ХЭРЭГЛЭЭНИЙ ШИНЖЛЭХ УХААН, ИНЖЕНЕРЧЛЭЛИЙН СУРГУУЛЬ

Пашкагын Мөнх-Болд

Гар утасны програм: Өгөгдлийн нууцлал, аюулгүй байдлын тусламж

Бакалаврын судалгааны ажил

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, Профессор Н.Оюун-Эрдэнэ

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээлэл компьютерийн ухааны тэнхим

Шүүмжлэгч : _____

Магистр Б.Магсаржав

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээлэл компьютерийн ухааны тэнхим

Гүйцэтгэсэн: _____

П.Мөнх-Болд

МУИС,Хэрэглээний шинжлэх ухаан, инженерчлэлийн сургууль

Мэдээллийн технологи 4

Гарчиг

Товчилсон үгийн жагсаалт

1.	МУИС	Монгол Улсын Их Сургууль
2.	ХШИУС	Хэрэглээний Шинжлэх Ухаан, Инженерчлэлийн Сургууль
3.	DB	Database
4.	GUI	Graphic User Interface
5.	API	Application Programming Interface
6.	DES	Data encryption standard
7.	TCP	Transmission Control Protocol
8.	IP	Internet Protocol
9.	HTTP	Hypertext Transfer Protocol
10.	RAID	Redundant Array of Independent Disks
11.	SQL	Structure Query Language
12.	SSL	Secure Socket Layer

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	Арга хэмжээ
14. Application	Програм
15. Gateway	Гарц
16. Proxy	Прокси
17. Packet	Пакет
18. Filter	Шүүлтүүр
19. Firewall	Галт хана
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

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 байдлын талаар асуудлууд үүсч байна. Иймд өгөгдлийн нууцлал, аюулгүй байдлын талаарх сэдвийг энэхүү баклаварын судалгааны ажилаараа сонгон авч судалгаа шинжилгээг шат дараалалтай хийж өгөгдлийн нууцлал, аюулгүй байдлын талаарх тусламж програмыг тодорхой хэмжээнд гүйцэтгэлээ.

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 програмынхаа 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.

Үндэслэл

Өгөгдлийн аюулгүй байдлыг хангах, өгөгдлийн нууцлалын асуудал чухлаар тавигдах болсонд өнөөгийн үед зарим хүмүс өгөгдлийн нууцлалыг хэрхэн хангах, түүний хор уршгийг мэдэхгүйн улмаас систем зарим хөгжүүлэгчид өгөгдлийн нууцлал, аюулгүй байдлыг үл тоон системээ хөгжүүлэх болсон билээ. Иймд оюутан сурагчдад өгөгдлийн нууцлал, аюулгүй байдлын талаар мэдлэг олгох хэрхэн хамгаалахад тус болох гэсэн үүднээс энэхүү програмыг хөгжүүллээ.

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 технолоийг судлах
- Хөгжүүлсэн програмаа туршиж сайжруулах үр дүнг дүгнэх
- Судалгааны үр дүнд тулгуурлан оюутан, сурагчдад зориулсан ухаалаг утасны програм, багшид зориулсан веб програм хангамжийг хөгжүүлэх

1. НЭГДҮГЭЭР БҮЛЭГ

1.1. 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.

1.2. 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.

1.2.1. Өгөгдлийн аюулгүй байдал

Өгөгдлийн аюулгүй байдал нь хулгай, буруу хэрэглэх, хүсээгүй халдлага болон дайралтаас өгөгдлийг хамгаалдаг тогтсон журам, стандарт болон тоног төхөөрөмжийн цогц юм. Өгөгдлийн сангийн аюулгүй байдал нь өгөгдлийн бүтэц байгууламж болон үүнд агуулагдаж байгаа өгөгдөлд нэвтрэх зөвшөөрлийг авч үздэг. Өгөгдлийн санг аюулгүй болгоход хэрэглэгдэх багаж хэрэгсэл 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 хангамжийг үйлдвэрлэгчид өгөгдлийн сангийн аюулгүй байдлыг хангах зорилгоор хамгийн түгээмэл ашигладаг аргууд нь хандалтыг хянах, гэрчилгээ болон өгөгдлийн нууцалж хадгалах юм.

1.2.2. Өгөгдлийн сангийн аюулгүй байдлын зорилго

Аюулгүй байдлын хэмжүүр нь мэдээллийг гаднаас үзэхээс нууц байлгах, өгөгдлийн тогтвортой байдлыг хадгалах, нөөцийг дээд төвшинд бэлэн баталгаатай байлгах юм. Үр ашигтай аюулгүй байдлын архитектур нь нууцлал (confidentiality), бүрэн бүтэн байдал (integrity), бэлэн байдал (availability) тулгуурладаг. Үүнийг C.I.A. гурвалжин буюу аюулгүй байдлын загвар гэж нэрлэдэг.

Зураг 1. Аюулгүй байдлын гурвалжин

1.2.2.1. Нууцлал

Нууц байдлыг хадгалах нь мэдээллийн нууцлалыг хамгаалж, хадгалах зорилгоор бодлого, журмын дагуу авсан арга хэмжээг хэлнэ. Учир нь системийн нууцлалыг

хангахын тулд энэ хоёр зүйлийг хийх хэрэгтэй:

1. Мэдээллийн нөөцөд хандах эрх бүхий боломжийг хязгаарлах замаар өөрийн хувийн нууцыг хадгалах.
2. Нөөцөд хандах зөвшөөрөлгүй хандалтыг хаах.

Өгөгдлийн 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 хязгаарлах замаар ашиглаж болно. Нууцлал нь аюулгүй байдлын хүчин чармайлтын хүрээнд хүрэх чухал зорилго юм. Нууцлалын цоорхой нь хэд хэдэн аюултай үр дүнд хүргэж болно.

1.2.2.2. Бүрэн бүтэн байдал

Бүрэн бүтэн байдал нь найдвартай, тогтвортой, иж бүрэн мэдээллийн тогтолцоог бий болгох болон дэмжих зорилгоор бодлого, журам 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 хууль бусаар эсвэл эрх бүхий өөрчлөлтөд аль альнаас 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 дутагдлыг олох шаардлагатай байдаг. Энэ үйл явц нь аудит гэж нэрлэдэг ба тиим мэдээллийн хуучин нөөцлөгдсөн хувилбарын эсрэг мэдээллийг шалгаж систем доторх ялгаа зөрүүг хайдаг ба аудитын ажилтныг татан оролцуулдаг юм. 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.

1.2.2.3. Бэлэн байдал

Бүрэн бүтэн байдал нь найдвартай, тогтвортой, иж бүрэн мэдээллийн тогтолцоог бий болгох болон дэмжих зорилгоор бодлого, журам 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 хууль бусаар эсвэл эрх бүхий өөрчлөлтөд аль алинаас 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 дутагдлыг олох шаардлагатай байдаг. Энэ үйл явц нь аудит гэж нэрлэдэг

ба тийм мэдээллийн хуучин нөөцлөгдсөн хувилбарын эсрэг мэдээллийг шалгаж систем доторх ялгаа зөрүүг хайдаг ба аудитын ажилтныг татан оролцуулдаг юм. Бүрэн бүтэн байдал нь мэдээллийн сангийн маш чухал шинж чанар бөгөөд хэрэв амжилтгүй хэрэгжүүлбэл, системийн гажуудал, найдваргүй өгөгдөл, гажигтай хөтөлбөр, муу гүйцэтгэлд хүргэж болох юм.

1.3. Криптограф

Криптограф гэдэг нь өгөгдлийн аюулгүй байдлыг хангах үүднээс өгөгдлийг нууцлах, өгөгдлийн бүрэн бүтэн байдал, түүний үнэн зөв өөрчлөлтгүй байдлыг хангах, зөвшөөрөлгүй хэрэглээнээс сэргийлэх зорилгоор өгөгдлийг 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. Криптографи нь өөртөө дараах үндсэн дөрвөн хүчин зүйлийг хамруулдаг. Үүнд:

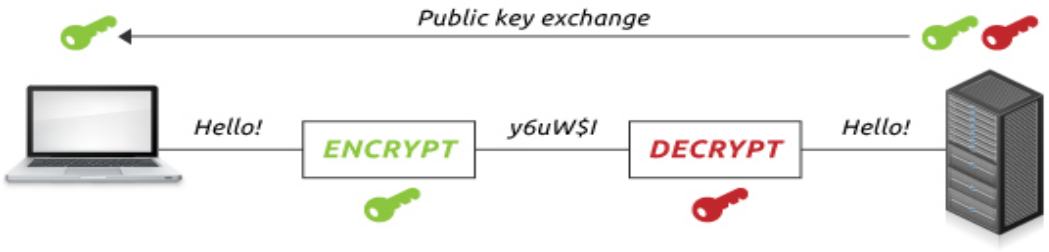
- Өгөгдлийг нууцлах
- Өгөгдлийг бүрэн бүтэн байдлыг хангах
- Өгөгдлийг тасралтгүй байдлыг хангах
- Өгөгдлийг баталгаажуулах

1.3.1. Тэгш хэмт бус криптографи гэж юу?

Тэгш хэмт криптографи 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 бусаагаад 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. Хамгийн түгээмэл тэгш хэмгүй шифрлэлтийн арга бол RSA юм. Тэгш хэмт бус түлхүүрүүд голдуу 1024 эсвэл 2048 бит байдаг.



Зураг 2. Тэгш хэмт бус криптографи

1.3.2. Тэгш хэмт криптограф гэж юу?

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:

1. Найдвартай кодлолын алгоритм хэрэглэх
2. Түлхүүрийн нууцллалыг маш сайн хангах

Тэгш хэмт кодлолын арга:

- **Орлуулах (substitution)** – энэ нь эх текстийн үсгүүдийг өөр үсэг, тоо, тэмдэгтээр орлуулан сольдог 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

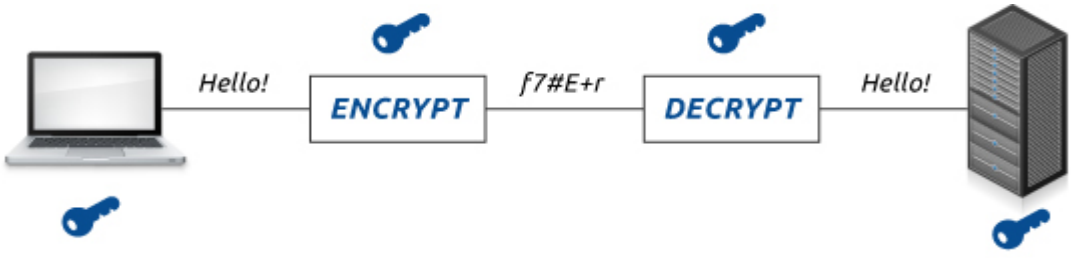
❖ **Block cipher algorithm** – багцын шифрийн алгоритм нь өгөгдлийг багц багцаар нь кодлодог бөгөөд мэдээллийн аюулгүй байдал болон нууцлалыг хангахад өргөн хэрэглэгддэг. Энэ нь өгөгдлийг 64 битээр кодлодог. Багцын шифрийн алгоритм нь Feisel –ийн cipher бүтэц дээр үндэслэн гарч ирсэн. Энэ нь тухайн бүтцээрээ 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.

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. Ye болгонд ялгаатай дэд түлхүүрийг ашигладаг. Тэгш хэмт түлхүүрүүд голдуу 128 эсвэл 256 бит байдаг.



Зураг 3. Тэгш хэмт криптографи

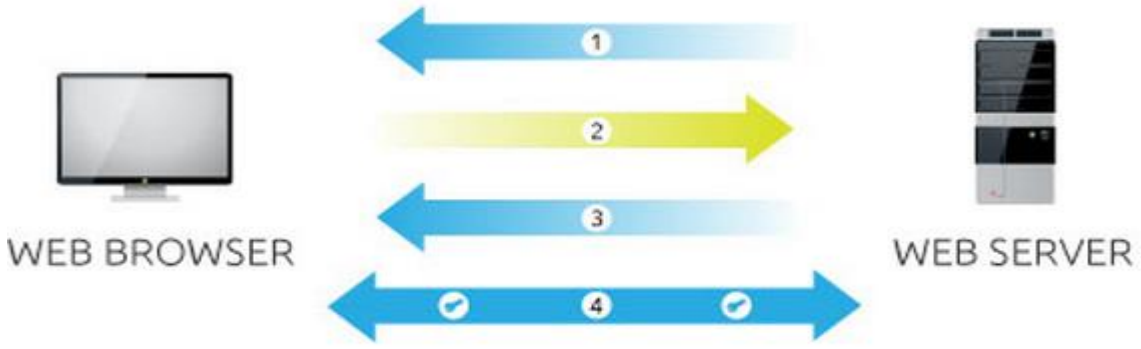
1.3.3. Аль нь илүү вэ ?

Тэгш хэмгүй түлхүүрүүд тэгш хэмт түлхүүрүүдээс илүү том, тэгш хэмгүй шифрлэгдсэн өгөгдөлийг эвдэх нь тэгш хэмтэй шифрлэгдсэн өгөгдлөөс илүү хүнд байдаг. Гэхдээ энэ тэгш хэмгүй түлхүүрүүд илүү гэсэн үг биш. Тэдний хэмжээгээр харьцуулснаас илүүтэйгээр дараах шинжээр тэдгээр түлхүүрүүдийг харьцуулах хэрэгтэй: тооцооллын дарамт болон түгээлтийн хялбар.

Тэгш хэмт түлхүүрүүд тэгш хэмгүй түлхүүрүүдээс бага ба түүгээрээ ч илүү бага тооцооллын ачааллыг шаарддаг. Гэсэн хэдий ч тэгш хэмт түлхүүрүүдэд гол сул тал байдаг – ялангуяа тэднийг мэдээллийг зөөх үеийн аюулгүй байдлыг хангахаар ашиглаж байгаа тохиолдолд. Яагаад гэвэл шифрлэх болон тайлахдаа ижил түлхүүр ашигладаг нь илгээгч болон хүлээн авагчид хоёуланд нь түлхүүр хэрэгтэй.

Тэгш хэмгүй шифрлэлтэнд энэ асуудал хамаагүй. Хэдий хугацаагаар хувийн түлхүүрийг нууцлаж чадна тэр хэмжээгээр илгээгчийн мессежийг тайлж чадахгүй гэсэн үг.

Тэгш хэмт болон тэгш хэмт бус шифрлэлтийн хамтын ажиллагаа



Зураг 4. Тэгш хэмт болон тэгш хэмт бус шифрлэлтийн хамтын ажиллагаа

1. Сервер өөрийн тэгш хэмгүй нийтийн түлхүүрийг илгээнэ.
2. Хөтөч тэгш хэмт сейшн түлхүүрийг , серверийн тэгш хэмгүй нийтийн түлхүүрийн хамт шифрлэн үүсгэнэ.
3. Сервер тэгш хэмт сейшн түлхүүрийг авахын тулд өөрийн хувийн тэгш хэмгүй түлхүүрээр тэгш хэмгүй нийтийн түлхүүрийг задалж уншина.
4. Ингэснээр хөтөч , сервер хоёр тэгш хэмт нийтйин сейшн түлхүүрийг ашиглан бүх дамжуулж буй өгөгдлүүдийг шифрлэж, задалж солилцоно.

1.3.4. 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.

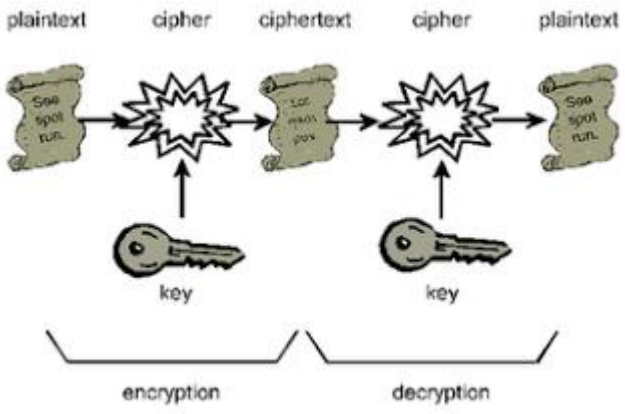
Ciper буюу алгоритм – Криптографд кодлох процессийг явуулахад тодорхой кодлолын алгоритмуудыг хэрэглэдэг.

Key буюу түлхүүр – Энкриптлэх болон декриптлэхэд ашиглагддаг түлхүүр. Кодлолын алгоритмууд нь тусгай түлхүүрээр удирдагддаг бөгөөд 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.



Зураг 5. Криптологи

Криптоанализ явуулах хоёр арга байдаг :

Cryptoanalytic attack – алгоритмыг өөрийнх нь шинж чанар дээр тулгуурлаад эх мэдээллийг гаргаж авах.

- Ciphertext only – алгоритм болон шифрлэсэн текстээс эх мэдээллийг гаргах
- Known plaintext – эх текстийн хэсэг болон шифрлэсэн текстийн тусламжтай
- Chosen plaintext – эх текстийг сонгож аваад
- 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

1.4. Хариу арга хэмжээ /Компьютерт суурьласан хяналт/

1.4.1. Эрх олгох

Систем эсвэл системийн аливаа нэг зүйлийг хуулийн дагуу ашиглахыг зөвшөөрдөг эрх буюу онцгой эрх ямбын зөвшөөрөл юм.

1.4.2. Хандалтыг хянах

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

1.4.3. Харагдац

Өөр холбоо харилцааг бий болгохын тулд үндсэн харилцаа холбоон дээр ажилладаг нэг эсвэл илүү олон харилцан хамааралтай үйл ажиллагааны идэвхтэй үр дүнг хэлнэ. Өгөгдлийн санд үнэндээ оршдоггүй ч хүсэлт явуулах үед тусгай хэрэглэгчийн тус хүсэлт дээр бий болдог динамик үр дүн юм.

1.4.4. Нөөц

Сүлжээнд холбогдоогүй хадгалах хэрэгсэлд ажлын файл (магадгүй мөн програм) болон өгөгдлийн сангийн хуулбарыг тогтмол авах үйл явц юм.

1.4.5. Нууцлал

Код тайлах түлхүүргүйгээр ямар ч програмаар өгөгдлийг уншиж болохооргүй болгодог тусгай алгоритмаар өгөгдлийг шифрлэх.

1.4.6. RAID технологи

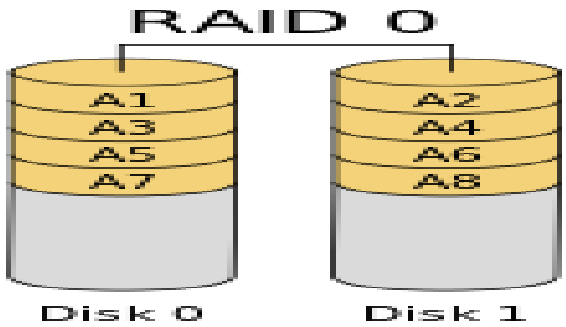
RAID гэдэг нь нэг ижил мэдээллийг хэд хэдэн хатуу дискэнд зэрэг хуулах технологийг хэлдэг. RAID-ийг үндсэн хоёр зорилгоор ашигладаг.

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 альныг нь дэмждэг байхаар ч хийж болно. RAID-ийг үүсгэсний дараа үйлдлийн систем RAID-ийг нэг хатуу диск байдлаар таньдаг 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 нэлээд хэдэн төрлийн байх бөгөөд энгийн хэрэглээнд ихэвчлэн хэрэглэгддэг төрлүүдийнх нь талаар тайлбарлая.

RAID-0:

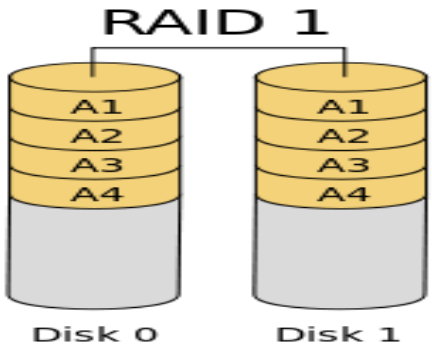
Мэдээллийг хатуу дискнүүдэд давхар бичих боловч нөөцлөх гэсэн ойлголт байхгүй. Өөрөөр хэлбэл хоёр хатуу дискийг RAID-0 байдалтай холбоход үйлдлийн системд нэг хатуу диск байдлаар харагдах бөгөөд мэдээллийг хоёр хатуу диск хуваан хуулдгаараа мэдээллийн бичих болон унших хурдыг бараг 2 дахин ихэсгэх боломжтой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



Зураг 6. RAID 0

RAID-1:

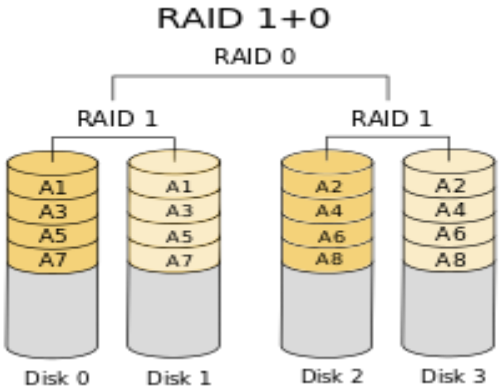
Disk mirroring буюу “Диск хуулбарлах” гэж мөн нэрлэгдэх бөгөөд 2 болон түүнээс дээш хатуу дискнүүдийг RAID-1 байдлаар холбох боломжтой. Мэдээллийг унших хурд нэмэгдэх бөгөөд бичих хурдны хувьд дан ганц дискний хурдтай ижил байна. Бичих явцад мэдээллийг нөөцөлж явдаг учраас мэдээлэл гэмтэх, устгагдах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



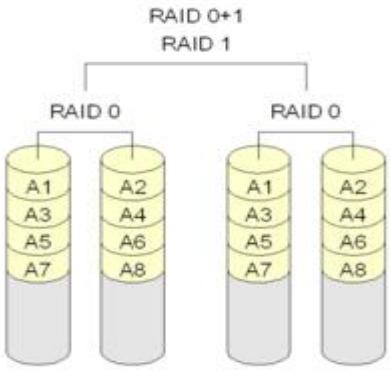
Зураг 7. RAID 1

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.



Зураг 8. RAID 10



Зураг 9. RAID 10

1.5. DBMS ба Вебийн аюулгүй байдал

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

Интернетээр мэдээлэл авах болон дамжуулахад дараах 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 авагчид итгэлтэй байж чадна (Дууриамал биш /non-fabrication/)
- Илгээгч нь илгээснээ үгүйсгэж чадахгүй байгаа (Татгалзалгүй/non-repudiation/)

Гэсэн хэдий ч, гүйлгээг хамгаалах нь асуудлын хэсгийг шийдэх цор ганц шийдэл юм. Нэгэнт мэдээлэл веб серверт хүрсэн бол хамгаалагдсан байх ёстой. Өнөөдөр ийм архитектурын ихэнх хэсэг нь баталгаажсан байдаг, гэхдээ энэ нь ерөнхийдөө янз бүрийн бүтээгдэхүүн, механизмыг шаарддаг. Веб орчинд авч үзэх ёстой аюулгүй байдлын өөр нэг асуудал хэрэглэгчийн машин руу дамжуулагдаж мэдээллийн утга юм.

Жишээ: HTML хуудас ActiveX, JavaScript / VBScript, эсвэл нэг буюу хэд хэдэн Java апплет хяналтыг агуулж болно. Дараах хортой үйлдлийг хийх боломжтой ба урьдчилан сэргийлэх арга хэмжээ авах хэрэгтэй:

- Бохир өгөгдөл эсвэл програмын 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 төхөөрөмжид зохисгүй нөлөө үзүүлдэг

1.5.1. Прокси сервер

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

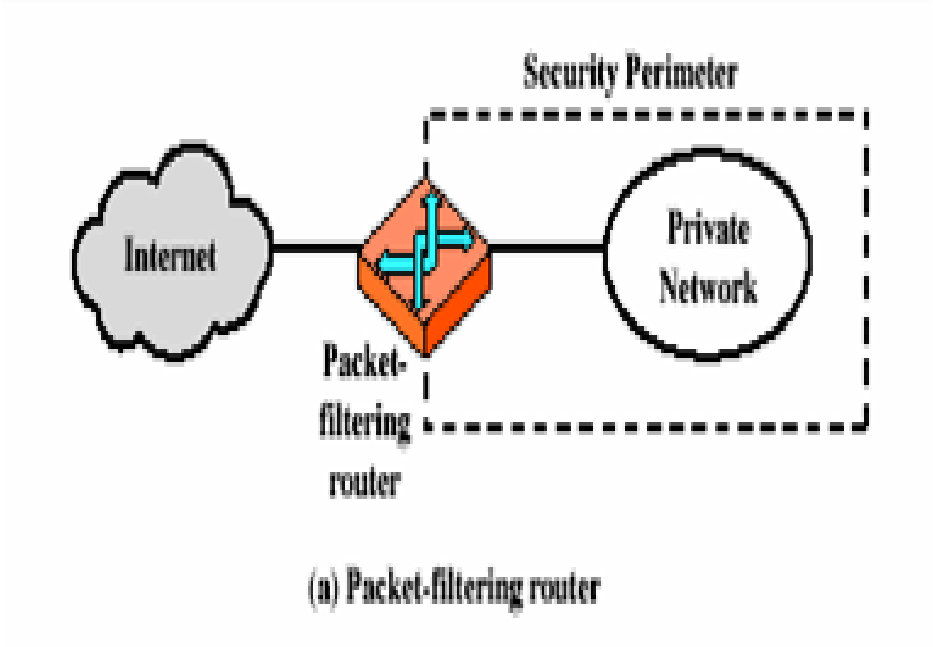
1. хүсэлт шүүх
2. үйл ажилгааг сайжруулах

1.5.2. Галт хананууд

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

- Пакет шүүлт (Packet Filter):

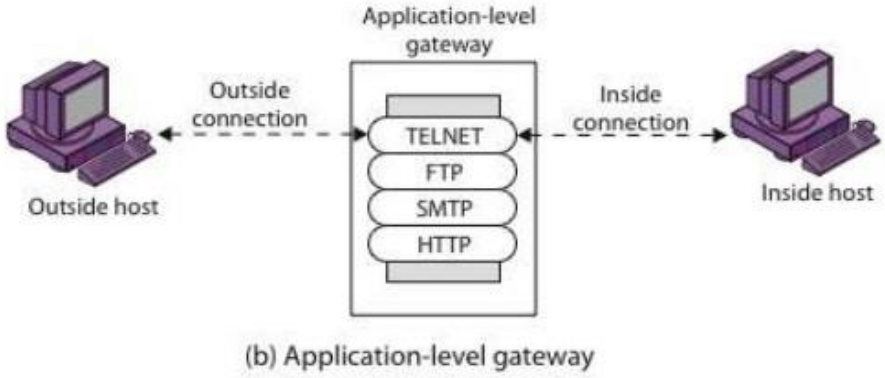
Интернетээр ямар нэгэн файлыг илгээхэд TCP/IP протокол уг файлыг жижиг, жижиг хэсгүүдэд хувааж байж дамжуулдаг. Тэдгээр олон жижиг хэсгүүдийн нэгийг пакет гэдэг. Пакетууд тус бүрдээ дугаарлагддаг ба очих газрынхаа IP хаягийг агуулсан байдаг. Тэгээд интернетээр дамжихдаа заавал нэг замаар дамжих албагүй өөр өөр замаар дамжиж болох ба хүрэх газраа очсон хойноо нийлж эргээд нэг файл болдог. Тэгэхээр энэ арга бол пакетуудыг шүүх шүүлтүүр бөгөөд тохируулж, тогтоож өгсөн шүүлтүүрийн хэм хэмжээний дагуу дүн шинжилгээ хийдэг. Пакетууд шүүлтүүрээр чөлөөтэй нэвтэрсний дараагаар очих ёстой газраа саадгүй хүрдэг.



Зураг 10. Пакет шүүлт

- Програмын гарц (Application gateway) :

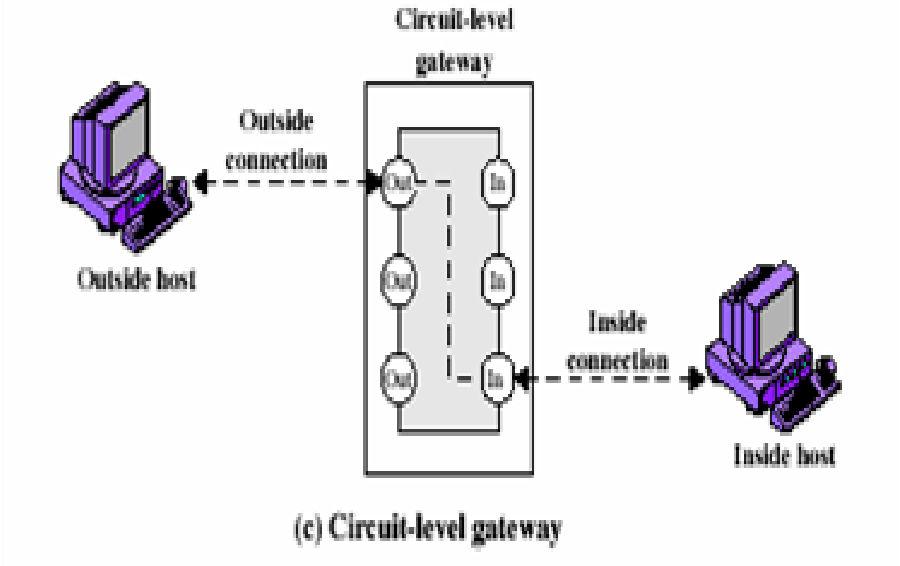
  Тодорхой програмууд FTP болон Telnet гэх мэт аюулгүй байдлын механизмыг хэрэглэнэ.Энэ нь маш үр дүнтэй боловч үйл ажилгааг бууруулдаг.



Зураг 11. Програмын гарц

- Circuit төвшний гарц:

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



Зураг 12. Circiut төвшний гарц

1.5.3. SSL гэж юу вэ?

SSL /secure socket layer/ гэдэг нь сервер болон хэрэглэгчийн төхөөрөмжийн хоорондох шифрлэгдсэн холбоосыг байгуулах аюулгүй байдлын стандарт технологи юм. Голдуу веб сервер /веб сайт/ болон веб хөтөч эсвэл цахим шуудангийн сервер болон цахим шуудангийн хэрэглэгчийн програмын / Outlook / хооронд ажиллана.

SSL нь кредит картны дугаар, нийгмийн хэрэгцээний нууц дугаар гэх мэт эмзэг мэдээллүүд мөн аюулгүй дамжих ёстой итгэмжлэгдсэн мэдээллүүдийн аюулгүй байдлыг хангах боломжийг олгодог. Веб хөтчүүдийн хооронд илгээгдсэн өгөгдөл мөн веб серверийн илгээсэн энгийн текстүүд нь нууцаар сонсох /мэдэх/ эмзэг аюулгүй байдлыг үүсгэж байдаг. Хэрэв халдагч нь веб хөтчүүд болон веб серверийн хооронд илгээгдсэн мэдээллүүд рүү нэвтэрч чадах юм бол тэдгээр мэдээллүүдийг чөлөөтэйгээр харж , ашиглаж чадна.

Тодруулбал, SSL нь аюулгүй байдлын протокол юм. Протоколууд нь алгоритмууд хэрхэн ашиглагдаж байгааг тайлбарладаг. SSL протокол нь дамжуулагдсан мэдээлэл болон холбоосыг хоёуланг нь шифрлэсэн хувьсагчуудыг тодорхойлдог.

SSL нь интернетээр өдөр бүр олон сая хүмүүсийн мэдээллийг хамгаалж байдаг, ялангуяа цахим гүйлгээний болон нууц мэдээллийг дамжуулж байх үеүд хамаарна. Интернет хэрэглэгчид веб хөтчийн хаяглалтын хэсэг дахь ногоон дүрс эсвэл цоожны дүрсээр SSL- ээр хамгаалагдсан веб сайтыг таньж болно. SSL-ээр хамгаалагдсан веб сайтууд мөн http ээс илүү https ээр эхэлсэн байдаг.

1.5.3.1. SSL гэрчилгээ гэж юу вэ?

Бүх веб хөтчүүд SSL протоколыг ашиглан хамгаалагдсан веб серверт хандах чадамжтай байдаг. Гэсэн хэдий ч бүх веб хөтчүүд болон серверт аюулгүй холболтыг үүсгэх SSL гэрчилгээ хэрэгтэй байдаг.

SSL гэрчилгээнүүд нь нийтийн болон хувийн түлхүүр гэсэн хос түлхүүртэй байдаг. Эдгээр түлхүүрүүд хамтдаа ажиллаж байж баталгаажсан аюулгүй холболтыг үүсгэдэг. Мөн гэрчилгээнүүд нь гэрчилгээ болон веб сайтын эзэмшигчийг таних “объект”-ыг агуулдаг.

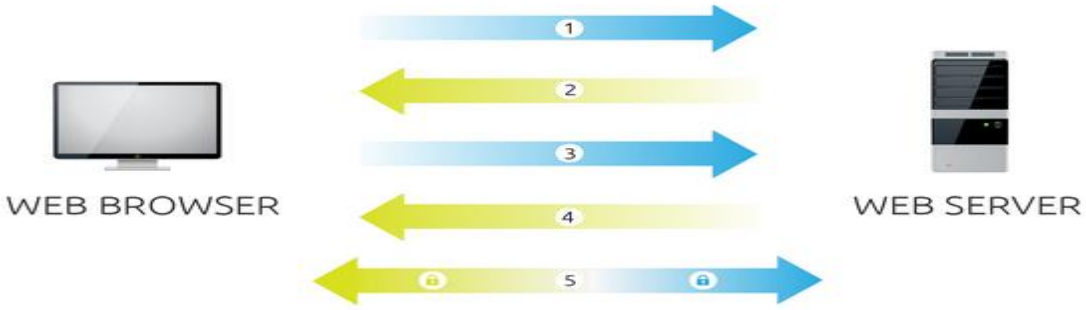
Гэрчилгээг авахын тулд , та өөрийн серверт гэрчилгээ таних хүсэлт /CSR/ үүсгэх ёстой. Энэ үйл ажилллагаа нь таны серверт хувийн болон нийтийн түлхүүрийг үүсгэдэг. CSR өгөгдлийн файл нь гэрчилгээ үүсгэгчийн нийтийн түлхүүрийг агуулж байдаг. Гэрчилгээ үүсгэгч нь CSR файлийг өөрийн түлхүүрийг хөндөлгүйгээр бусдын хувийн түлхүүрт тохирохоор өгөгдлийн бүтцийг үүсгэхийн тулд ашигладаг.

SSL гэрчилгээний хамгийн чухал хэсэг бол итгэмжлэгдсэн гэрчилгээ үүсгэгчийн тоон гарын үсэг юм. Хэн ч гэрчилгээ үүсгэж болох боловч веб хөтөчүүд нь тухайн байгууллагын итгэмжлэгдсэн гэрчилгээ үүсгэгчдийн жагсаалтаас ирсэн гэрчилгээнд л итгэдэг. Хөтөчүүд нь урьдчилан суулгагдсан итгэмжлэгдсэн гэрчилгээ үүсгэгчдийн жагсаалттай хамт ирдэг ба үүнийг итгэмжлэгдсэн гэрчилгээ үүсгэгчдийн дэлгүүр гэж нэрлэдэг. Итгэмжлэгдсэн гэрчилгээ үүсгэгчдийн дэлгүүрт багтах болон итгэмжлэгдсэн гэрчилгээ үүсгэгч болохын тулд компани нь аюулгүй байдлын аудид хийлгэсэн мөн хөтчөөс гаргасан стандартуудыг биелүүлсэн байх ёстой.

SSL гэрчилгээ нь гэрчилгээ үүсгэсэн байгууллага болон домайн/веб хуудсыг гуравдагч талын этгээдээр баталгуужуулагдсан байна.

1.5.3.2. SSL гэрчилгээ нь хэрхэн аюулгүй холболтыг үүсгэдэг вэ?

Веб хөтөч нь SSL – ээр хамгаалагдсан веб сайтад хандахаар оролдоход, хөтөч серверийн хооронд “SSL гар барилцах” үйл ажиллагаа явагдаж SSL холболт үүсдэг. “SSL гар барилцах” нь хэрэглэгчид үзэгдэхгүй бөгөөд хоромхон хугацаанд явагддаг. Хамгийн чухал нь, дараах гурван түлхүүр SSL холболтыг үүсгэхэд ашиглагддаг: нийтийн , хувийн болон сейшн /session/ түлхүүр. Нийтийн түлхүүрээр шифрлэгдсэн ямар зүйл зөвхөн хувийн түлхүүрээр эсрэгээрээ тайлагдана. Яагаад гэвэл нийтийн болон хувийн түлхүүрээр шифрлэгдэж, тайлахад үйл ажиллагааны их хэмжээний хүч шаарддаг, тэдгээр нь зөвхөн “SSL гар барилцах” ажиллагааны турш ашиглагдаж тэгш хэмт сейшн түлхүүрийг үүсгэдэг. Аюулгүй холболт үүссэний дараа, сейшн түлхүүр бүх дамжиж буй өгөгдлийг шифрлэгдэхэд ашиглагддаг.



Зураг 13. SSL ажиллагаа

1. Веб хөтөч хамгаалагдсан веб сервер болон веб сайтад холбогдох. Веб хөтөч сервер өөрийгөө тодорхойлох гэж хүсэлт гаргаж байна.
2. Сервер нь серверийн нийтийн түлхүүрийг багтаасан, SSL гэрчилгээний хуулбарыг илгээнэ.
3. Хөтөч гэрчилгээг итгэмжлэгдсэн гэрчилгээ үүсгэгчийн жагсаалтаас шалгаж холбогдоход зөвшөөрөгдсөн веб хуудас мөн эсэхийг шалгана. Хэрэв мөн бол серверийн нийтийн түлхүүрийг ашиглан сейшн түлхүүрийг буцаана.
4. Сервер хувийн түлхүүрээ ашиглан сейшн түлхүүрийг задалж хүлээн зөвшөөрөгдсөн сейшн түлхүүрийг буцаана.
5. Сервер болон хөтөч хооронд сейшн түлхүүртэй хамт бүх шифрлэгдсэн өгөгдөл дамжина.

1.6. 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:

1. 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.
2. 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 сканердэж эсвэл фото зургийг нь авч цахим хэлбэрт оруулсан хуулбар

- Зурмал гарын үсэг бүхий факс
- Ямар нэг баримтын агуулга дотор сканердэж 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 ихэнх 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.

1.6.1. 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.

Жишээ 1: 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.

Жишээ 2: 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.

1.6.2. Хэш 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.

1.7. 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 төвшин дэхь хэрэглээ / Security level assignment / :
5. Аюулгүй байдлын цэвэрлэгээний төвшинд 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.

1.8. SQL Injection

SQL injection бол програм болон вебийг өгөгдлийн сантай холбогдох үед гардаг хамгаалалтын сул талыг ашиглан програм болон веб сайтад халдах арга юм. SQL Тарилга нь системийн хамгаалалтын сул талыг ашиглан хор хөнөөл учируулахуйц SQL илэрхийлэлээр програм хангамжийн өгөгдлийн сангийн давхаргад халдах кодчиллын техник юм. Маш ойлгомжтойгоор тайлбарлахад SQL асуулгад тарилга. хийх буюу өөрийнхөө хүссэн тэмдэгтүүдийг query дотор оруулаад, дараа нь өөрийнхөө хүссэн үр дүнг гаргаж авахыг SQL тарилга гэдэг юм. Дэлхийн нийт веб болон програмын 60 хувь нь SQL injection халдлагаас сэргийлэгдээгүй байдаг гэсэн судалгааны дүн бий.

SQL тарилга өртөх орчин:

SQL тарилгад ихэвчлэн веб сайтууд, веб програм хангамжууд өртдөг боловч SQL өгөгдөл удиртлагад ямар ч төрлийн програмд халдах боломжтой байдаг юм. **Жишээлбэл:** Веб суурьтай систем, десктоп програм, гар утасны програм гэх мэт. Түүнчлэн онлайн эсвэл офлайн горимд ажилладаг нь ч тийм чухал биш тухайн шинж чанарт нь тааруулсан SQL тарилга хийх боломжтой байдаг.

SQL тарилга халдлагад өртөх алдаа:

SQL тарилгад өртдөг гол гол алдаанууд байдаг. Жишээлбэл туршлагагүй хөгжүүлэгчид аюулгүй байдлыг дутуу хангах хэрэглэгчийн оруулсан өгөгдлийг буруу, дутуу шүүх, хэрэглэгчид шаардлагагүй эрхийг өгөх, алдааны мэдээлэл хэт ихийг мэдээлэх зэрэг байдаг.

SQL тарилга халдлага:

SQL тарилгыг хар малгайт хакерууд ашиглаж халдага хийдэг. Хар малгайт хакер гэдэг нь ерөнхийдөө муу талын эвдэж сүйтгэж болох бүтэхгүй зүйл хийж байдаг хакерийг хэлнэ.

SQL тарилга халдлагын төрлүүд:

SQL тарилгаар халдлага хийхэд хэд хэдэн төрлийн аргууд байдаг.

Үндсэн 3н төрлийн арга :

1. **Хэрэглэгчийн оруулсан өгөгдөлд суурилсан тарилга**

   Энэ арга нь хэрэглэгчийн мэдээлэл оруулах талбарт өөрийн хүссэн тэмдэгтүүдийг залгаж бичээд өгөгдлийн сангийн давхаргад хор хөнөөл учируулахуйц SQL асуулгыг үүсгэж ажилуулдаг хамгийн энгийн арга юм.

2. **Жигнэмэгд суурилсан тарилга**

   Энэ арга нь жигнэмэг буюу хэрэглэгчийн броузерд хадгалагдах багахан хэмжээний өгөгдөл юм. Ихэнхдээ жигнэмэгийг хэрэглэгчийн талаарх мэдээллийг хадгалахад (хэрэглэгчийн дугаар, нэр гэх мэт) ашигладаг. Жигнэмэг дэх утгыг ашиглан тарилга хийж болдог.

3. **Серверийн хувьсагчиар дамжуулан тарих**

   Энэ арга нь серверд байрлах хувьсагч жишээлбэл SESSION зэрэгт тарилга хийж болно. Мөн HTTP header-ийн утгуудад тарилга хийх боломжтой.

Хамгаалалт хийх аргууд:

- **Цагаан жагсаалт**

  Цагаан жагсаалт арга нь хэрэглэгчийн ашиглах тэмдэгтийн утгыг хязгаарлаж өгдөг юм. Жишээлбэл нууц үг оруулах талбарт зөвхөн том жижиг үсэг болон тоо ашиглах ёстой гэж оруулж өгч болно. Ингэснээр өгөгдлийн сангийн давхаргад хор хөнөөл учруулахуйц SQL асуулга болох тусгай тэмдэгтүүдээс нэг ёсны зугтаж байна гэсэн үг юм.

- **Хар жагсаалт**

  Хар жагсаалт арга нь хэрэглэгчийн оруулсан тэмдэгтэнд хор хөнөөл учруулахуйц SQL илэрхийлэл үүсгэх тэмдэгтүүд байна уу гэдгийг шалгаад хэрэв тийм тэмдэг байвал хасч өгдөг юм. Жишээлбэл хэрэглэгчийн оруулсан тэмдэгтээс DROP, TABLE, UNION зэрэг тэмдэгт орсон байвал хасч хаяна гэсэн үг юм.

- **Шифрлэлт**

  Шифрлэлтийн аргуудыг ашиглах нь мэдээллийг бусдад алдах аюулаас хамгаалдаг юм. Жишээлбэл системд хэрэглэгчийн нууц үгийг заавал шифрлэж өгөгдлийн санд хадгалах ёстой байдаг. Энэ аргаар бүх өгөгдөлөө шифрлэж нааш хэрэглэгчид харагдах хэсэгт хөрвүүлэн ашиглаж болох юм. Энэ нь гэхдээ маш нууц өгөгдөлтэй мэдээллийн системүүдийн хувьд л тохиромжтой арга юм. Бусад тохиолдолд энэ арга төвөгтэй байдаг.

- **Эрх хязгаарлах**

  Энэ арга нь програм хангамжийг ашиглах хэрэглэгчийг ангилж тус бүрд нь шаардлагатай эрхийг нь өгөгдлийн сангийн давхаргад өгөх юм. Ингэснээр програм хангамжийн өгөгдлийн санд зөвхөн зарим нэгэн хэсэг руу хандах эрхтэй болно гэсэн үг. Жишээ нь хүснэгт устгах, баазийг унтраах эрх ихэнх хэрэглэгчид шаардлагагүй. Ийм замаар бид халдлагаас аль болох бага шарх авч гарах боломж ихсэх юм.

1.9. Веб програм хангамжийн судалгаа

Вебийн түүх 1980-аад оны сүүл үеэс эхлэлтэй. 1989 онд Европийн Цөмийн Физикийн Судалгааны Төвд (CERN) дэлхийгээр нэг тархсан судлаач эрдэмтдийг компьютерийн сүлжээний тусламжтайгаар өөр хооронд нь холбож, санаа оноогоо солилцож байх боломжийг олгох “WWW” төсөл хэрэгжиж эхэлсэн 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 веб рүү 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 аппликейшний 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. Энэ нь 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 ачаалаж 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

1.10. 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.

1.11. Ашигласан 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 оруулаа.

1.11.1. Андройд системийн судалгаа

Андройд бол мэдрэгчтэй дэлгэцтэй ухаалаг гар утас ба таблет зэрэг хөдөлгөөнт хэрэгслүүдэд зориулан бүтээгдсэн, Линүкст 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 (2.3–2.3.7)
- Honeycomb (3.0–3.2.6)
- Ice Cream Sandwich (4.0–4.0.4)
- Jelly Bean (4.1–4.3.1)
- KitKat (4.4–4.4.4, 4.4W–4.4W.2)
- Lollipop (5.0–5.1.1)
- Marshmallow (6.0)

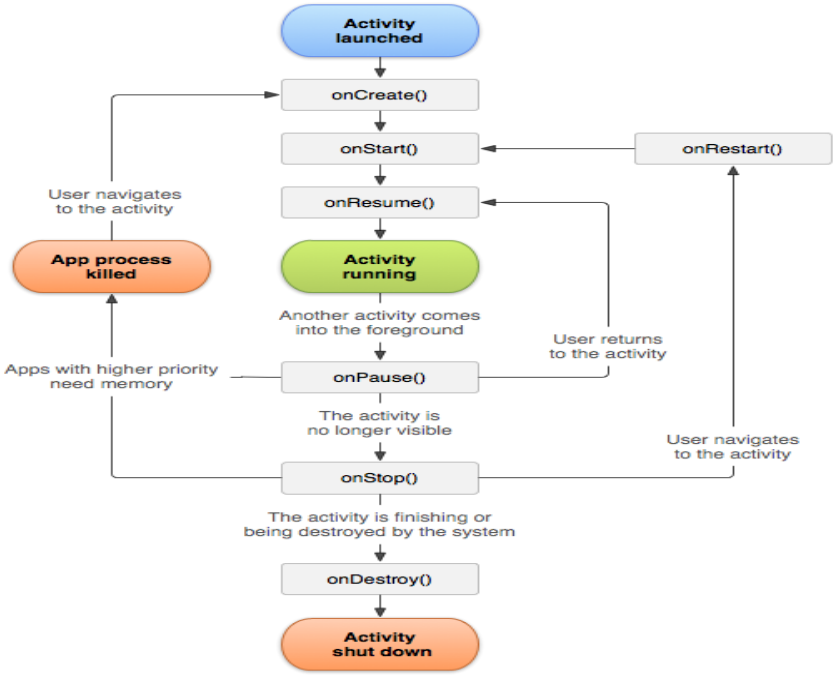
1.11.2. Андройд аппликейшний судалгаа

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



Зураг 14. Андройд хөгжүүлэлтийн амьдралын цикл

1.11.3. 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 хэлнүүдтэй төстэй юм.

1.11.4. JQuery

JQuery бол жава-скриптийн фрэймворк бөгөөд клиент талд код бичиж байгаа веб хөгжүүлэгчдэд хэрэг болох маш олон зүйлүүдийн жава-скрипт функцын санг бэлтгэсэн байдаг. Өөрөөр хэлбэл JQuery нь хэрэглээг хөнгөвчлөх зорилготой веб хөтөч хамааралгүй (Cross browser) клиент талын жава-скрипт сангийн цуглуулга юм. Эдгээр сан нь дараах зүйлүүдийг хамардаг. HTML элементийн сонгох.

- 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 Жава-скрипт 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 жава-скрипт функцуудийг 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 жава-скрипт функцээр дамжуулан хүссэн JQuery-ийн функцыг дуудаж өгнө.
- JQuery нь тодорхой бичиглэлийн дүрэмтэй.

jQuery –йин үндсэн 3 төрлийн хэрэглээ түгээмэл байдаг.

- HTML document–д
- CSS файлд загвар өгөх,
- JavaScript файлтай харьцах.

1.11.5. Bootstrap

Веб програм нь гар утас, таблет зэрэг дээр ажиллах учир тухайн төхөөрөмжийн хэмжээнээс үл хамааралд 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 веб дизайныг (responsive web design) дэмжин ажилладаг болсон. Bootstrap нь веб 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 веб аппликэйшнийн дизайныг хийхэд хялбар болгож өгнө. Грид систем гэдэг нь хуудасны бүтцийг 2 хэмжээст хүснэгтэд хуваан зохиомжлохыг хэлнэ.

1.11.6. 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 хөгжүүлэлтэд 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.

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.

2. ХОЁРДУГААР БҮЛЭГ

2.1. 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.

2.1.1. Хэрэглэгчийн функциональ шаардлага

Хэрэглэгч :

Хэрэглэгч нь гар утасны програм ашиглах бөгөөд дараах үйлдлүүдийг хийнэ.

- Хичээл харах
- Асуулт харах
- Асуулт асуух
- Жишээ харах
- Тохиргоо хийх

Админ :

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

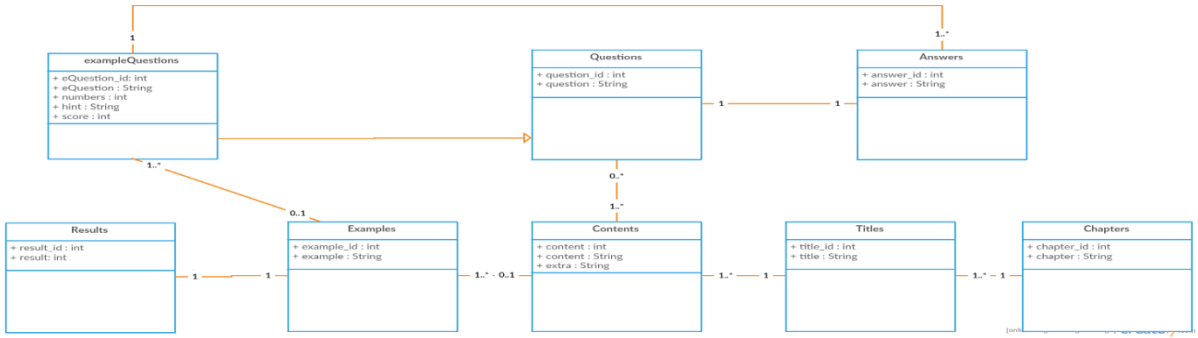
- Хичээл нэмэх
- Хичээл хасах
- Хичээл засах
- Жишээ нэмэх
- Жишээ хасах
- Жишээ засах
- Асуултад хариулах
- Асуултад хасах
- Системд өөрийн нэр нууц үгээр нэвтрэх

2.1.2. Хэрэглэгчийн функциональ бус шаардлага

- Үйл ажиллагааны
  - Хэрэглэгчид зориулсан програм нь ямар ч төрлийн андройд үйлдлийн системтэй төхөөрөмж нь дээр ажилладаг байна.
  - Администрийн 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

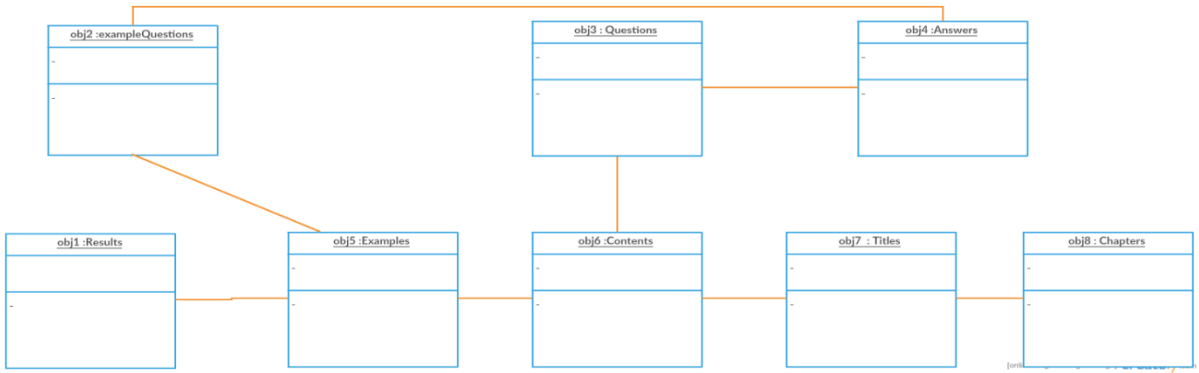
2.2. Системийн статик шинжилгээ

Гар утас болон веб системд шаардлагатай классууд болон түүний шинж чанар, үйлдлүүдийг тодорхойлон классын диаграмыг боловсруулллаа. Эдгээр классууд нь шинж авах (get) болон өгөх(set) үйлдлүүд хийдэг болно.



Зураг 15. Класс диаграм

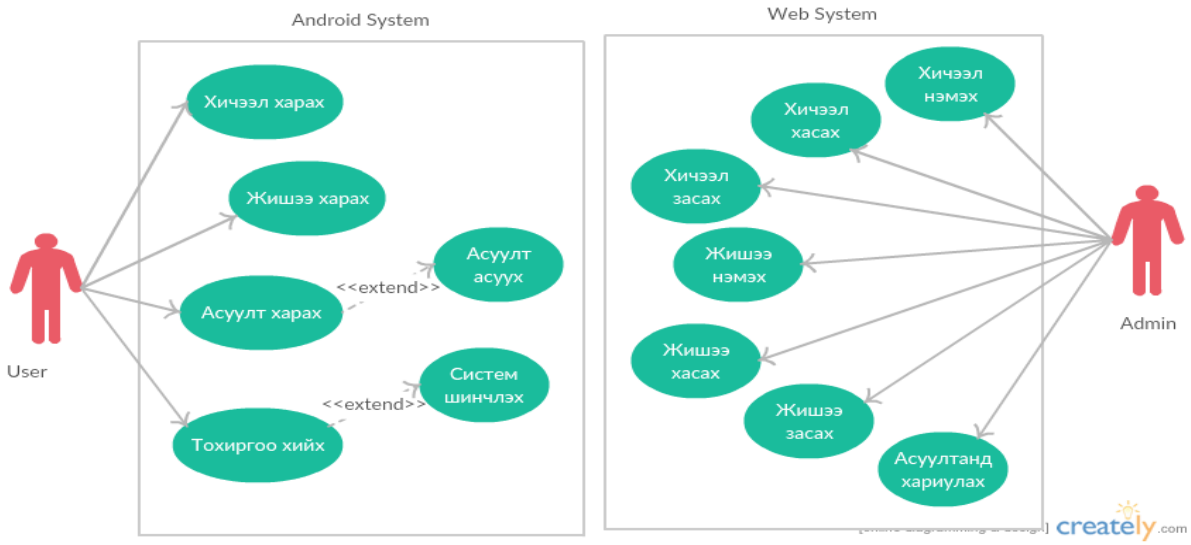
Боловсруулсан классын диаграм дээр тулгуурлан обьектууд болон тэдгээрийн хоорондын холбоосыг харуулсан обьектын диаграмыг боловсруулллаа.



Зураг 16. Обьект диаграм

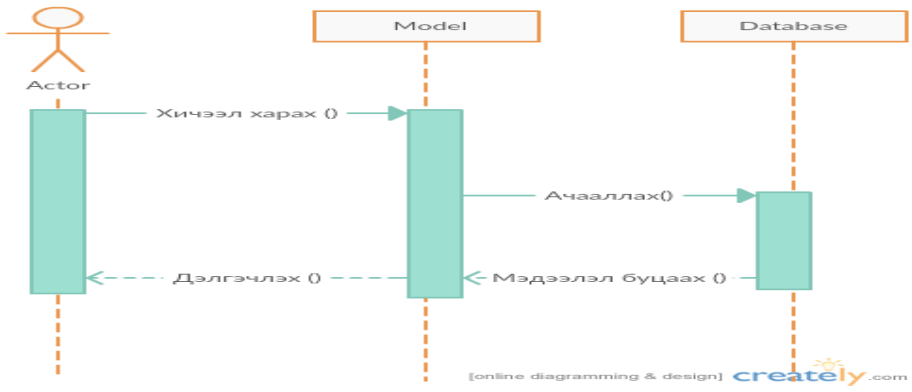
2.3. Системийн динамик шинжилгээ

Гар утас болон веб систем нь тус тусдаа хэрэглэгчтэй ба тэдгээрийн системд гүйцэтгэх үүрэг нь өөр өөр байна. Гар утасны системд хэрэглэгч нь хичээл харах, асуулт харах, асуулт асуух, асуулт хариулт тоглох, жишээ харах, програмыг шинэчилдэг байна. Веб системд хэрэглэгч нь хичээл нэмэх, хасах, засах ба хэрэглэгчээс ирсэн асуултад хариулдаг байна. Системийн үйлдлүүдийг ажлын явцын диаграмаар дүрсэлбэл доорх диаграмд үзүүлсэн хэлбэрээр дүрслэгдэнэ.



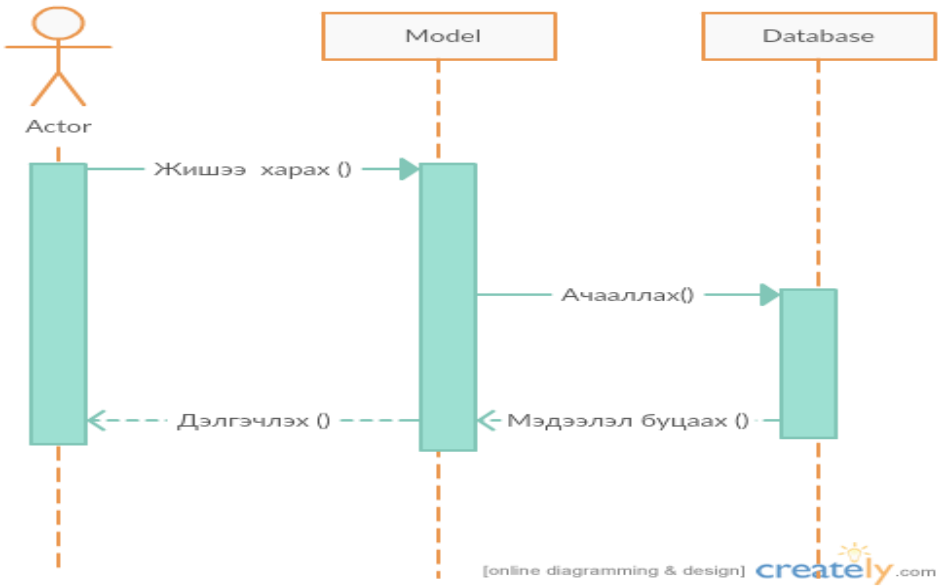
Зураг 17. Ажлын явцын диаграм

Use case диаграм дээр гар утасны хэрэглэгчийн үндсэн үйлдлүүдийн нэг болох хичээл харах үйлдийн дарааллын диаграмыг боловсруулаа.



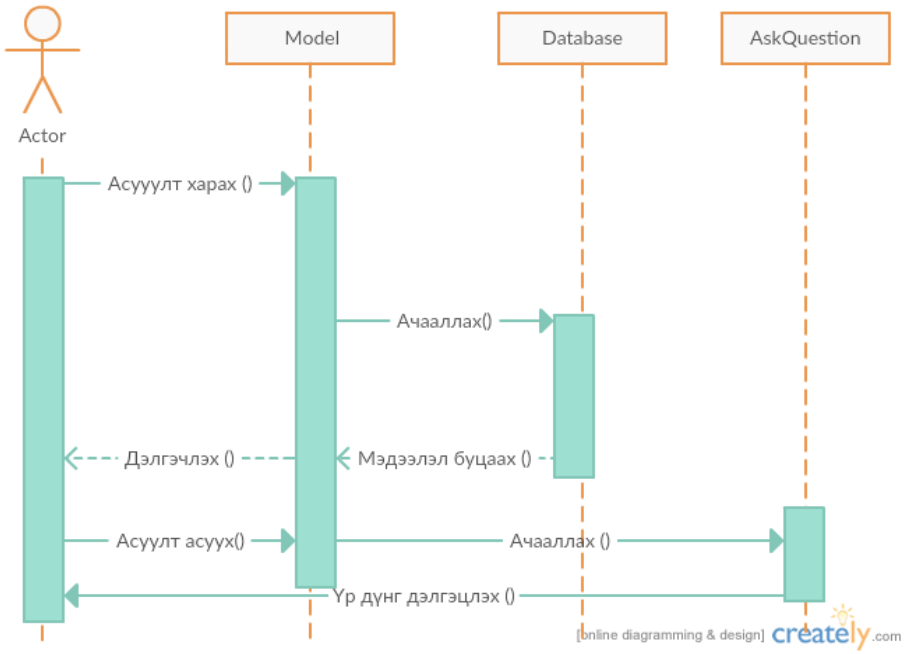
Зураг 18. Дарааллын диаграм 1

Use case диаграм дээр гар утасны хэрэглэгчийн үндсэн үйлдлүүдийн нэг болох жишээ харах үйлдийн дарааллын диаграмыг боловсруулаа.



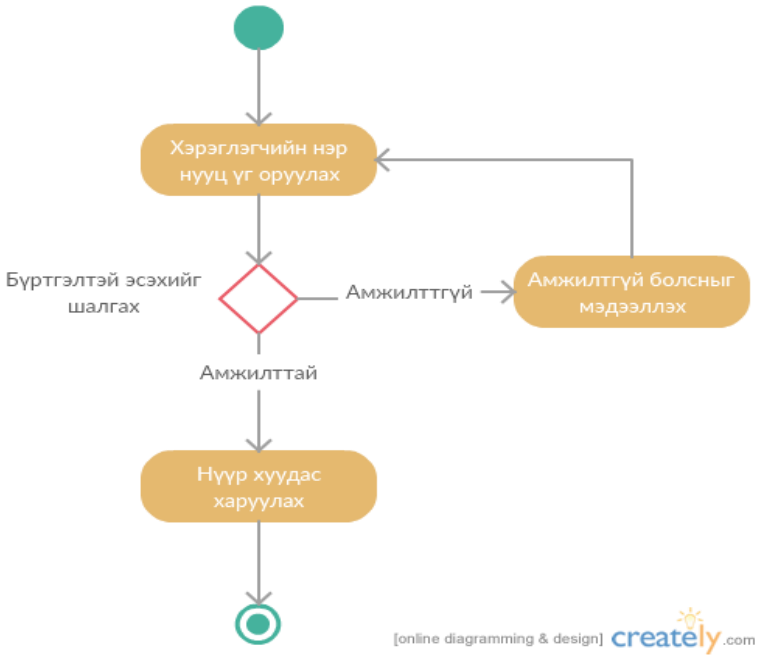
Зураг 19. Дарааллын диаграм 2

Use case диаграм дээр гар утасны хэрэглэгчийн үндсэн үйлдэлүүдийн нэг болох асуулт харах болон асуулт асуух үйлдийн дарааллын диаграмыг боловсруулаа.



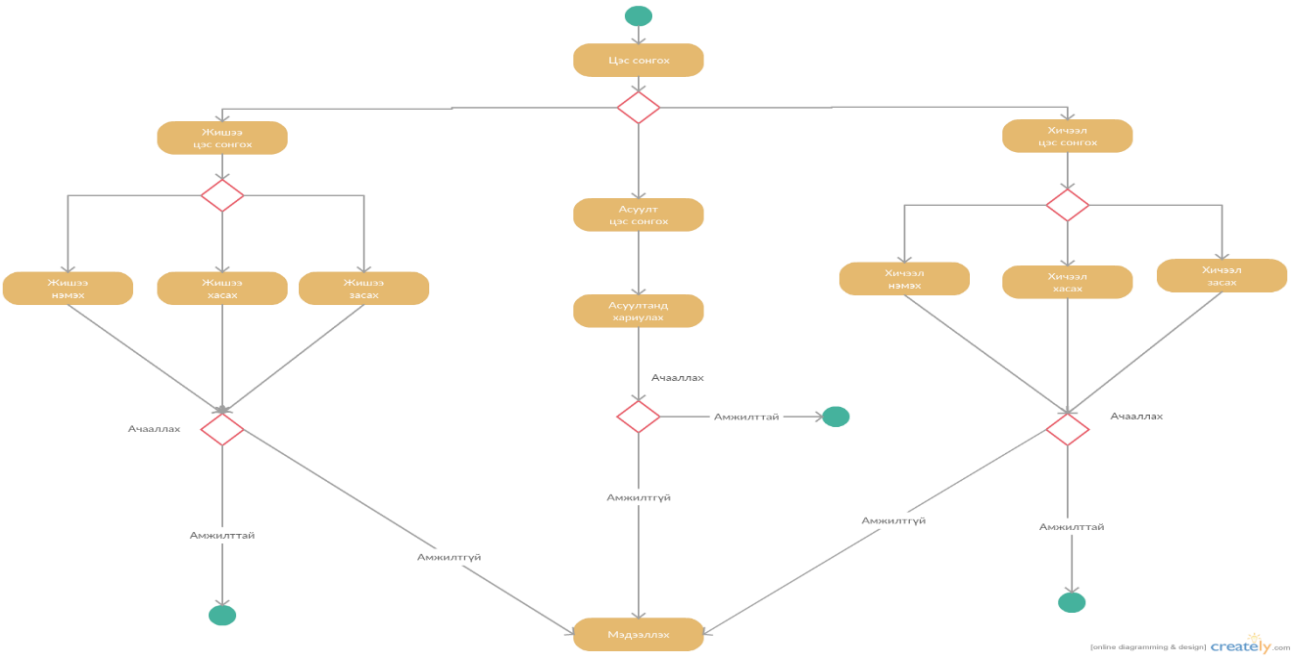
Зураг 20. Дарааллын диаграм 3

Админ хэрэглэгч буюу багш веб системд нэвтрэх үйл идэвхжилтийн диаграмыг боловсрууллаа.



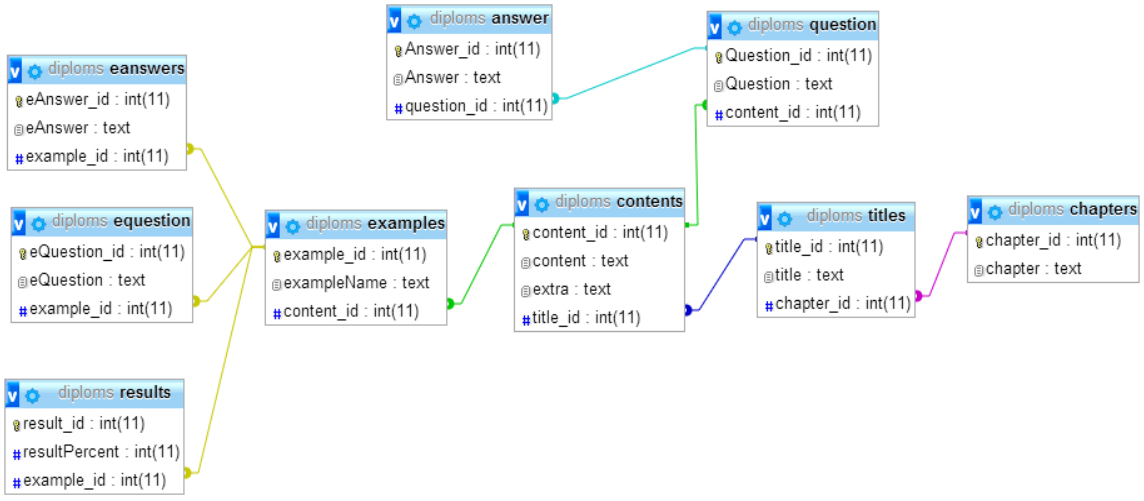
Зураг 21. Үйл идэвхжилтийн диаграм 1

Админ хэрэглэгч буюу багш веб системд нэвтрэн орсны дараах үйлдлүүдийн үйл идэвхжилтийн диаграмыг дүрсэлсэн байдал.



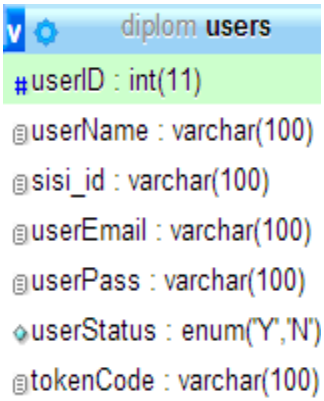
Зураг 22. Үйл идэвхжилтийн диаграм 2

Гар утасны программд ашиглагдах хүснэгтүүд дээр тулгуурлан холбоост өгөгдлийн сангийн зохиомж боловсруулаа.



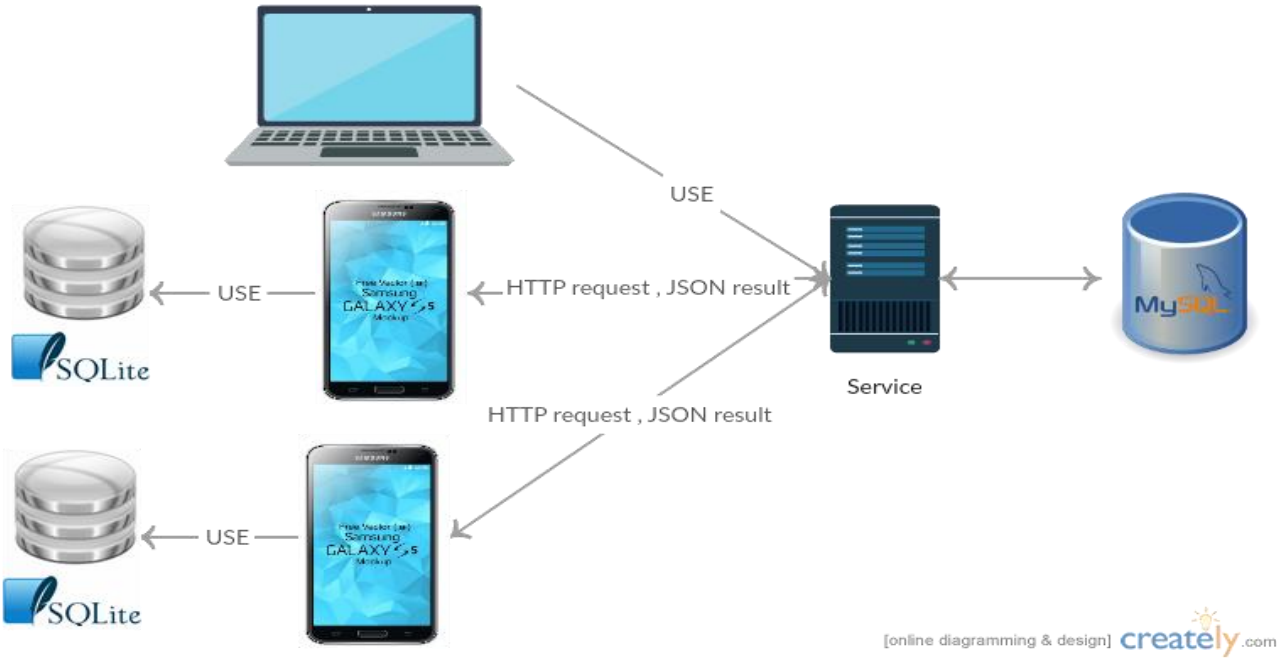
Зураг 23. Холбоост өгөгдлийн сангийн зохиомж

Веб системд ашиглагдах өгөгдлийн сангийн зохиомжыг гар утасны программд зориулсан өгөгдлийн сангийн зохиомж дээр тулгуурласан бөгөөд хэрэглэгч бүртгэх зорилгоор users гэсэн хүснэгт нэмсэн болно.



Зураг 24. Хэрэглэгчийг бүртгэх хүснэгт

Системд гар утасны клиент болон веб клиент-ууд байх ба Веб сервис харьцаж ажилна. Веб сервис нь MySQL өгөгдлийн сангийн системээс өгөгдлөө авна. Мөн гар утасны систем нь офлайн горимд файлд суурилсан өгөгдлийн сан болох SQLite-аас өгөгдлөө аван ажиллана. Веб сервис нь олон хэрэглэгч системд зэрэг хандах боломж олгоно.



Зураг 25. Архитектурын зохиомж

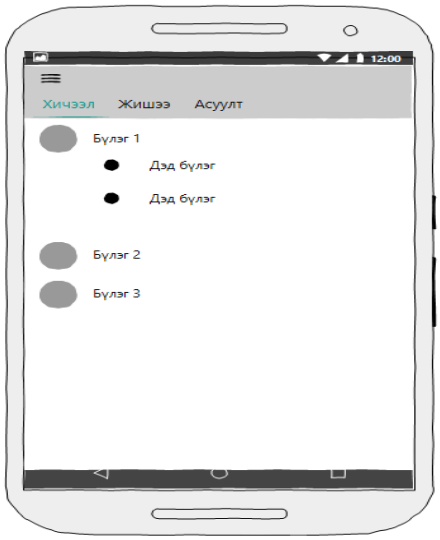
2.4. Хэрэглэгчтэй харьцах хэсгийн зохиомж

Prototype буюу туршилтын загваруудаа “Wireframing” програмыг ашиглан зурж үзлээ. Ингэхдээ вебийн загварыг http://mockups.com сайтыг ашиглан грийд системд орууллаа.

Хэрэглэгч хичээл харах, жишээ харах, асуулт харах, тохиргоо хийх гэсэн үндсэн цэстэй байна гэсэн хэрэглэгчийн шаардлагын дагуу гар утасны програмын үндсэн цэсийн хэрэглэгчтэй харьцах хэсгийн зохиомж боловсруулаа.

Зураг 26. Програмын цэс

Хэрэглэгч хичээл харахдаа үндсэн бүлэгээр нь харах ба хүссэн бүлгээ дэлгэрүүлж харах боломжтой мөн гэсэн хэрэглэгчийн шаардлагад тулгуурлан хичээл цэсний хэрэглэгчтэй харьцах хэсгийн зохиомж боловсрууллаа.

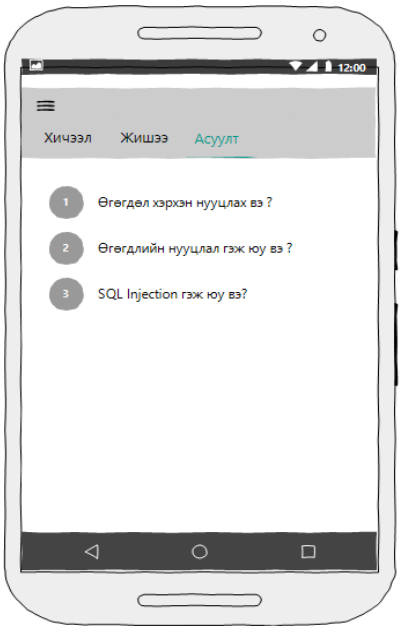


Зураг 27. Хичээл цэс

Хэрэглэгч жишээ харахдаа үндсэн бүлгүүдийн хүрээнд жишээ ажиллах боложтой байх гэсэн хэрэглэгчийн шаардлагад тулгуурлан жишээ цэсний хэрэглэгчтэй харьцах хэсгийн зохиомж боловсрууллаа.

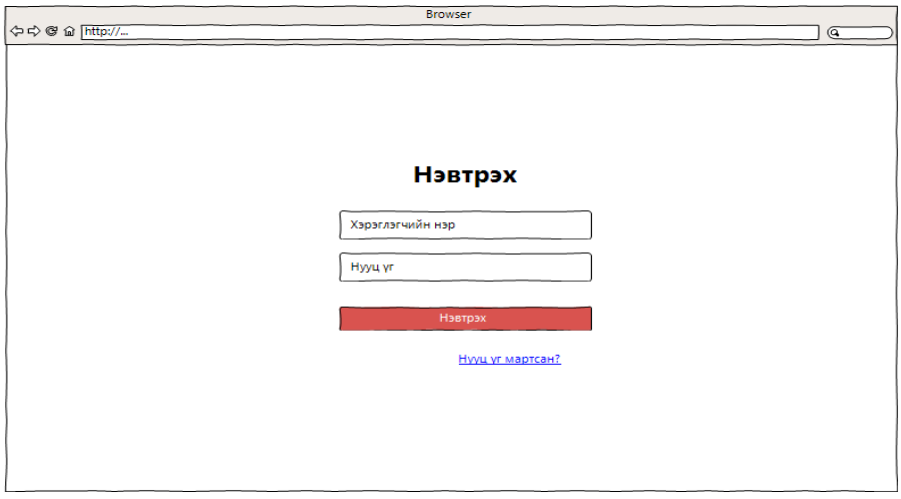
Зураг 28. Жишээ цэс

Хэрэглэгч асуулт харахдаа өмнө нь асуугдаж байсан асуулт бүрийг харах боломжтой байх гэсэн хэрэглэгчийн шаардлагад тулгуурлан асуулт цэсний хэрэглэгчтэй харьцах хэсгийн зохиомж боловсруулллаа.



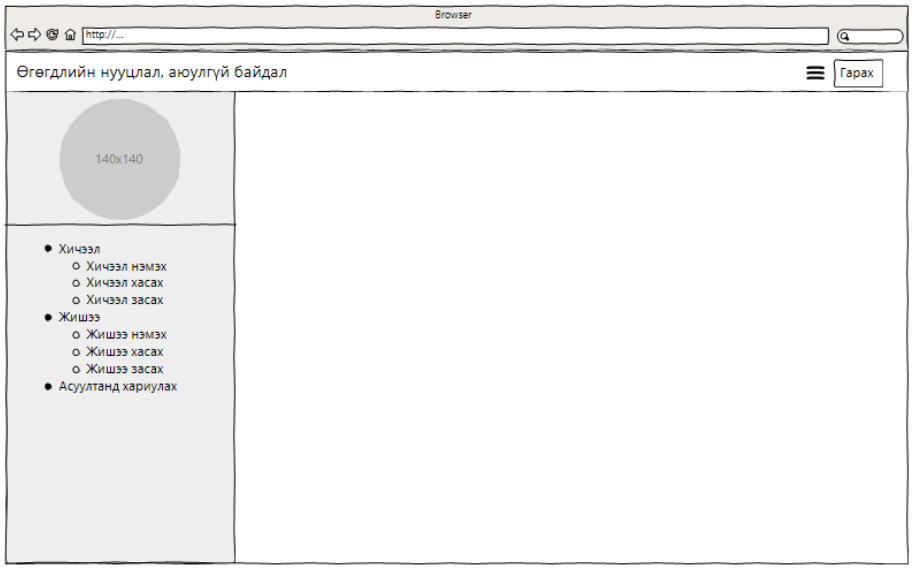
Зураг 29. Асуулт цэс

Админ хэрэглэгч буюу багш нь системд өөрийн нэр болон нууц үгээр нэвтэрдэг байх гэсэн хэрэглэгчийн шаардлагад үндэслэн веб системд нэвтрэх хэсгийн хэрэглэгчтэй харьцах хэсгийн зохиомж боловсруулллаа.



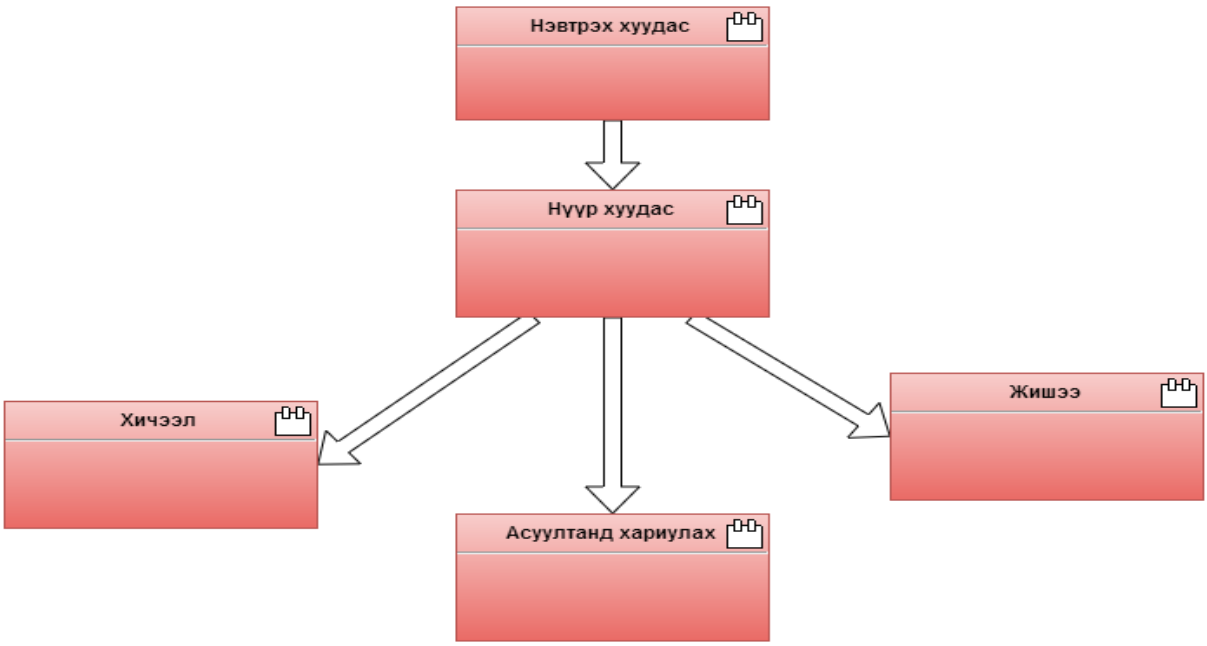
Зураг 30. Нэвтрэх хэсэг

Админ хэрэглэгч буюу багш нь системээс хичээл нэмэх, хасах, засах жишээ нэмэх, хасах,засах асуултанд хариулах гэсэн хэрэглэгчийн шаардлагад тулгуурлан хэсгийн хэрэглэгчтэй харьцах хэсгийн зохиомж боловсрууллаа.



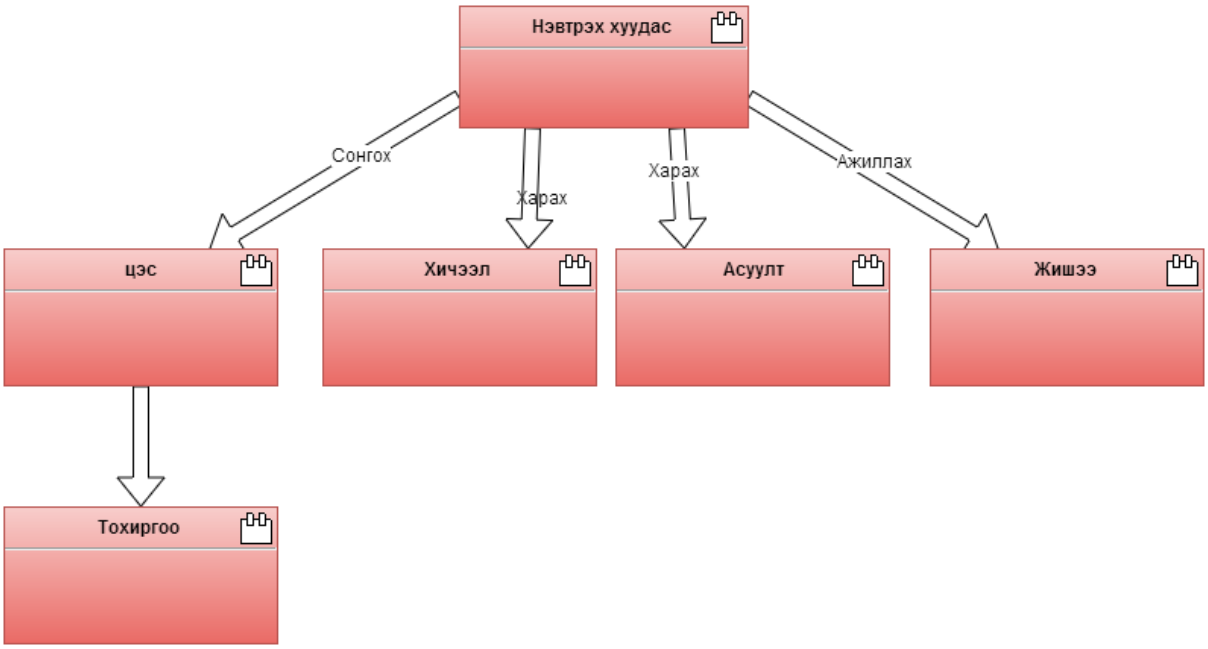
Зураг 31. Нүүр хуудас

Админ хэрэглэгч буюу багш нь веб системд нэвтэрсний дараах шилжилтийн загвар.



Зураг 32. Шилжилтийн загвар

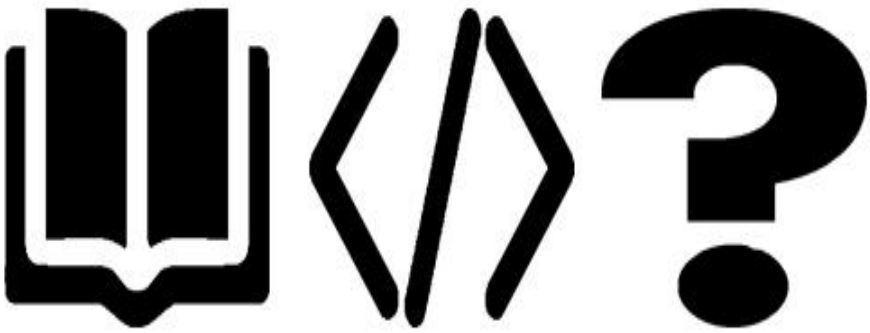
Хэрэглэгч гар утасны програмд нэвтэрсний дараах шилжилтийн загвар.



Зураг 33. Шилжилтийн загвар

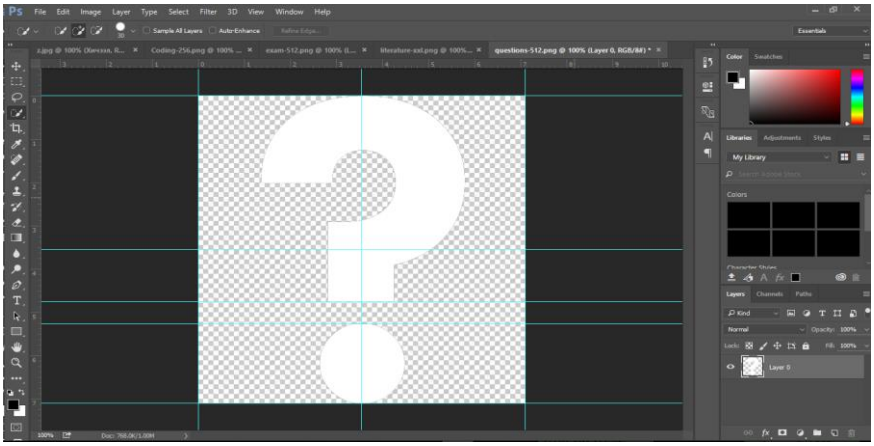
2.5. Шигтгээ зураг зурах

Энэ хэсэгт системдээ ашиглах шигтгээ зургуудаа “Adobe Photoshop CC” вектор болон растер зургийн програмыг ашиглан зурлаа. Шигтгээ зургаа вектор зургийн програмаар зурсан болохоор янз бүрийн хэмжээтэй дэлгэц дээр чанараа алдахгүй сайн зураг болж чадлаа.



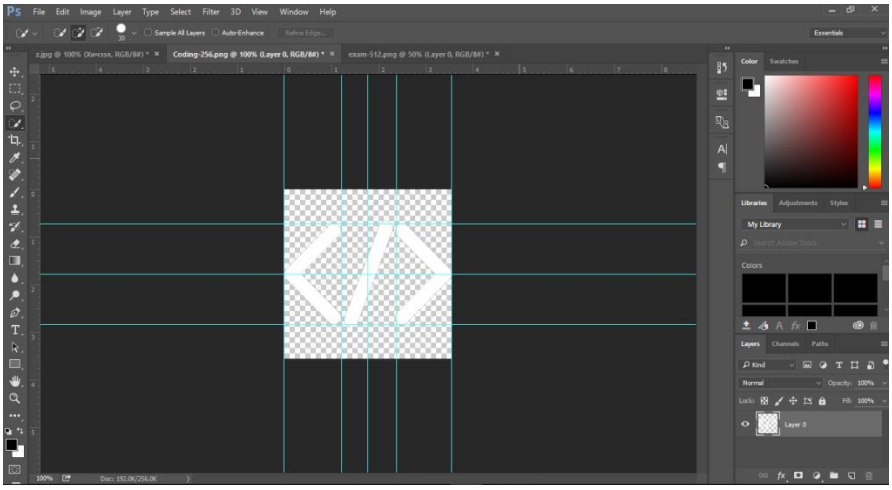
Зураг 34. Шигтгээ зураг

Асуулт цэсний шигтгээ зургийг зурсан байдал.



Зураг 35. Шигтгээ зураг зурсан байдал 1

Жишээ цэсний шигтгээ зургийг зурсан байдал.



Зураг 36. Шигтгээ зураг зурсан байдал 2

Бүлгийн дүгнэлт

Энэ бүлэгт өөрийн системийн бүтэц үйл ажиллагааг нарийвчлан гаргаж гар утасны болон веб програм хөгжүүлэхэд зайлшгүй шаардлагатай классын диаграмм, обьектийн диаграм, ажлын явцын диаграм, дарааллын диаграм, үйл идэвхжилтийн диаграм, холбоост өгөгдлийн сангийн зохиомж, системийн шилжилтийн загвар, архитектурын зохиомж, хэрэглэгчтэй харьцах хэсгийн зохиомж зэргийг зурж боловсруулаа.

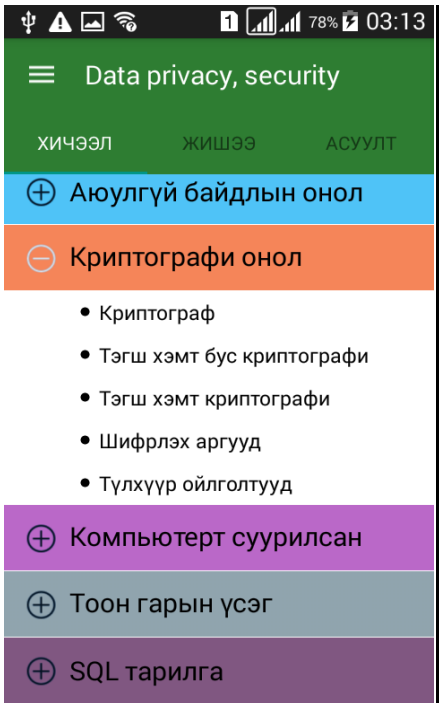
3. ГУРАВДУГААР БҮЛЭГ

3.1. Хэрэгжүүлэлт

Энэхүү бүлэг нь системийг хийж гүйцэтгэх хамгийн чухал үе бөгөөд шинжилгээ болон зохиомж дээр хийсэн баримт бичгүүд дээр тулгуурлан хэрэгжүүлэлтээ хэрхэн хийсэн болон судалгааны үр дүнд олж авсан мэдлэгээ яаж ашигласан талаар бичсэн болно. Кодчилох үед гарсан хүндрэлүүдээс өөрийнхөө хэрэгтэй гэж бодсон зарим асуудлуудын талаар энэ бүлэгт оруулсан юм.

Тулгамдсан асуудал(онцлох) : /Хичээл цэс/

Хичээлийг бүлэг бүлгээр нь бүлэг дээр дарахад дэд бүлэг хардаг байхаар зохиомжлох хэрэглэгчийн шаардлагыг шийдсэн байдал. Энэхүү асуудлыг шийдэхдээ Expandable-г дахин тодорхойлж өөр хэрэгтэй байдлаар зохиомжилж ашигласан болно.

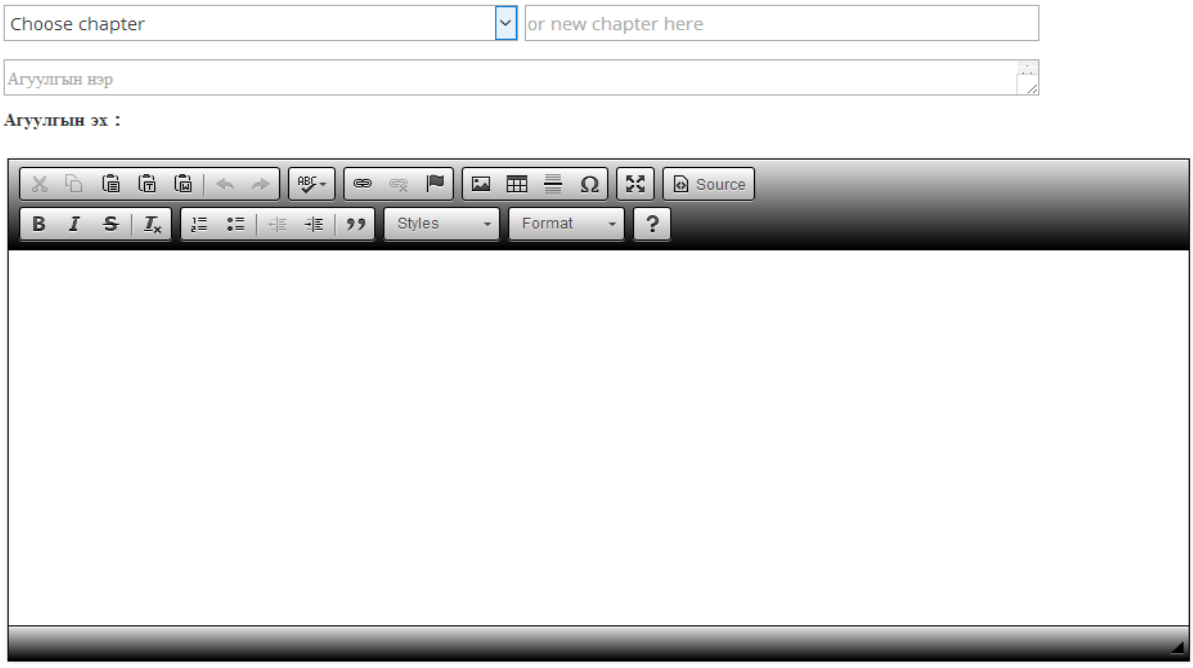



```
public class ExpandableListAdapter extends BaseExpandableListAdapter {

    private Context _context;
    private List<String> _listDataHeader; // header titles
    private HashMap<String, List<String>> _listDataChild;

    public ExpandableListAdapter(Context context, List<String> listDataHeader,
                                 HashMap<String, List<String>> listChildData) {
        this._context = context;
        this._listDataHeader = listDataHeader;
        this._listDataChild = listChildData;
    }

    @Override
    public Object getChild(int groupPosition, int childPosititon)
    {
        return this._listDataChild.get(this._listDataHeader.get(groupPosition))
                .get(childPosititon);
    }

    @Override
    public long getChildId(int groupPosition, int childPosition) { return childPosition; }

    @Override
    public View getChildView(int groupPosition, final int childPosition,
                             boolean isLastChild, View convertView, ViewGroup parent)
    {

        final String childText = (String) getChild(groupPosition, childPosition);

        if (convertView == null) {
```

Зураг 37. Хичээл цэс шийдэл

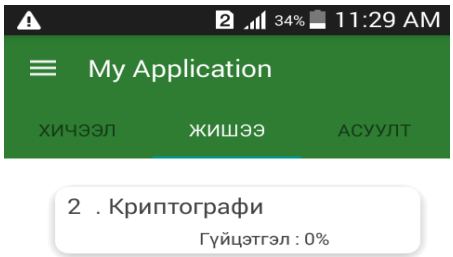
Хичээл цэсний мэдээллийг хэрэглэгчдэд ойлгомжтой, товч тодорхой харуулах гэсэн хэрэглэгчийн шаардлагыг шийдсэн байдал. Энэхүү асуудлыг дараах байдлаар зохиомжилж харуулах байдлаар шийдсэн болно. Админ хэрэглэгч буюу багш нь

мэдээлэл оруулахыг хэсгийг CKEDITOR ашиглан шийдэж өгсөн. Энэхүү CKEDITOR нь мэдээллийг хэрэглэгчдэд ойлгомжтой байдлаар зохиомжлох боломжтой юм.



Зураг 38. CKEDITOR

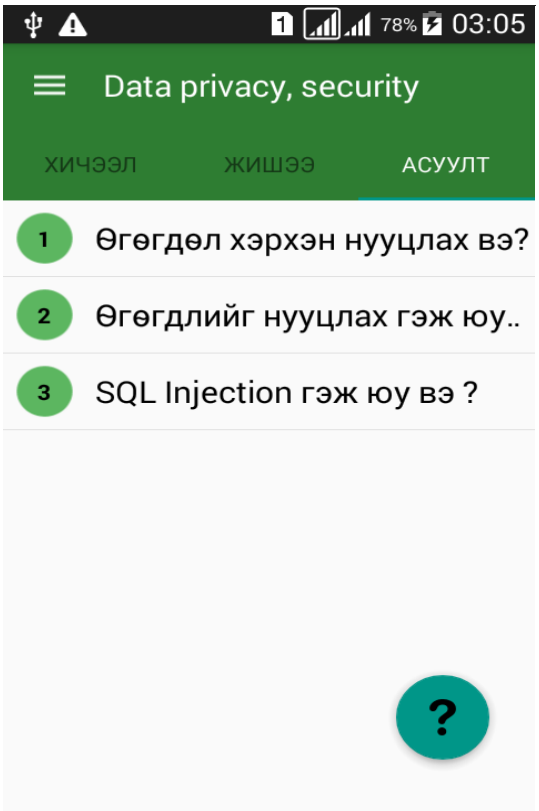
Жишээ цэсэнд хичээл цэсэнд байрлах хичээлүүдийн агуулгад үндэслэн боловсруулсан асуулт хариулт байна. Энэхүү асуудлыг RecycleView-г өөрт хэрэгтэй байдлаар зохиомжилж харуулах байдлаар шийдсэн болно.




```
public class CustomAdapter extends RecyclerView.Adapter<CustomAdapter.MyViewHolder> {

    private ArrayList<DataModel> dataSet;

    public static class MyViewHolder extends RecyclerView.ViewHolder {

        TextView textViewName,textViewpoint,textViewper;
        ImageView start;

        public MyViewHolder(View itemView) {
            super(itemView);
            this.textViewName = (TextView) itemView.findViewById(R.id.name);
            this.textViewpoint = (TextView) itemView.findViewById(R.id.point);
            this.textViewper = (TextView) itemView.findViewById(R.id.per);
            this.start  = (ImageView)itemView.findViewById(R.id.start);
        }
    }

    public CustomAdapter(ArrayList<DataModel> data) { this.dataSet = data; }

    @Override
    public MyViewHolder onCreateViewHolder(ViewGroup parent,
                                           int viewType) {
        View view = LayoutInflater.from(parent.getContext())
                .inflate(R.layout.cards_layout, parent, false);

        view.setOnClickListener(ExampleFrag.myOnClickListener);

        MyViewHolder myViewHolder = new MyViewHolder(view);

        return myViewHolder;
```

Зураг 39. Жишээ цэсний шийдэл

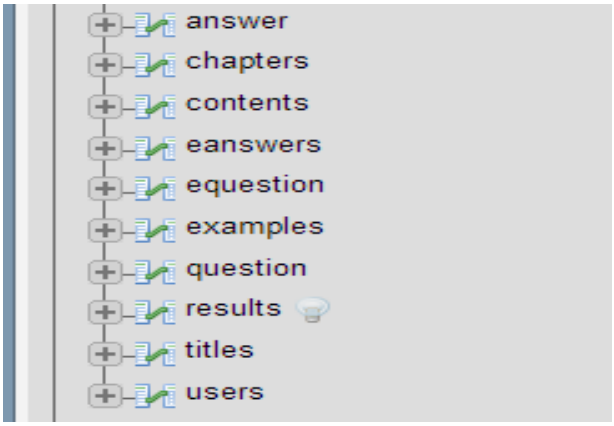
Асуулт цэсэнд өгөгдлийн нууцлал, аюулгүй байдлын сэдвийн хүрээнд өөрт тулгамдаж буй асуудлыг админ хэрэглэгч буюу багшаас асууж шийдвэрлэх боломж олгодог байх ба бусдад тулгамдсан асуудлууд мөн шийдлүүдийг харах боломжтой байна. Энэхүү асуудлыг дараах байдлаар зохиомжилж харуулах байдлаар шийдсэн болно. Асуулт асуух хэсгийн кодчлол.



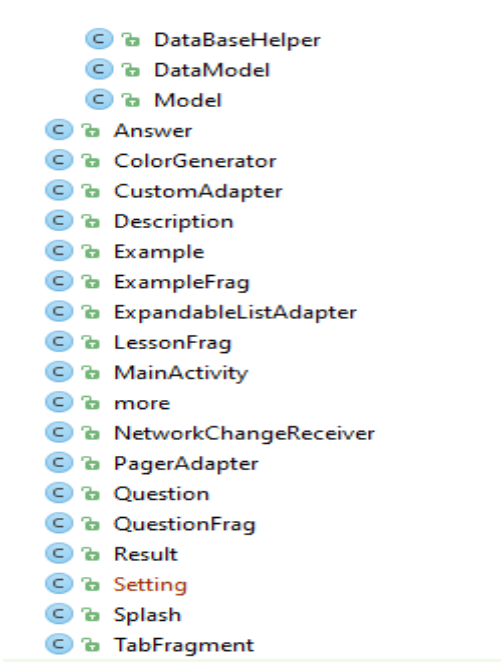

```
class SendPostReqAsyncTask extends AsyncTask<String, Void, String> {
    @Override
    protected String doInBackground(String... params) {
        String question = params[0];
        List<NameValuePair> nameValuePairs = new ArrayList<>();
        nameValuePairs.add(new BasicNameValuePair("question", question));

        try {
            HttpClient httpClient = new DefaultHttpClient();
            HttpPost httpPost = new HttpPost(
                    "http://10.0.52.147/webservice/Questions.php");
            httpPost.setEntity(new UrlEncodedFormEntity(nameValuePairs));

            HttpResponse response = httpClient.execute(httpPost);

            HttpEntity entity = response.getEntity();

            //is = entity.getContent();


        } catch (ClientProtocolException e) {

        } catch (IOException e) {

        }
        return "success";
    }

    @Override
    protected void onPostExecute(String result) {
        super.onPostExecute(result);
```

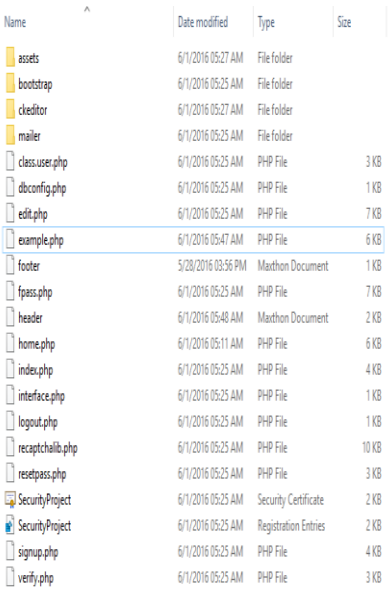
Зураг 40. Асуулт цэсний шийдэл

Гар утасны болон веб системд ашигласан өгөгдлийн сангийн хүснэгтүүдээ харьцаат өгөгдлийн сангийн диаграмын дагуу PhpMyAdmin багажийг ашиглан үүсгэв. Жишээ болгон зарим хүснэгтийн бүтцийг харуулав.



Гар утасны програмын хөгжүүлэхэд үүссэн жава файл болон веб систем хөгжүүлэхэд үүссэн файлуудын бүтцийг харуулав.





ДҮГНЭЛТ

Гар утасны програм: Өгөгдлийн нууцлал аюулүй байдлын тусламж сэдэвт баклаварын судалгааны ажлыг 14-н долоо хоногийн хугацаанд МУИС ХШУИС МКУТ-ийн доктор, профессор Н.Оюун-Эрдэнэ багш дээр сонгон төлөвлөгөөний дагуу хийх ажлуудыг гүйцэтгэн системийн анхны хувилбарыг амжилттай гаргалаа.

Төслийг хэрэгжүүлэхдээ аль болох хэрэглээ болон цаашид сайжруулан хөгжүүлж болох талаас нь харан гүйцэтгэсэн болно. Уг систем нь гар утасны хэрэглэгчдэд өгөгдлийн нууцлал, аюулгүй байдлын талаар мэдлэг олгох, ямар чухал болохыг ойлгуулах зорилготой ба хэрэглэгчдэд хэрэглэхэд хялбар, ойлгомжтой байлгахаар системийг хийж гүйцэтгэлээ.

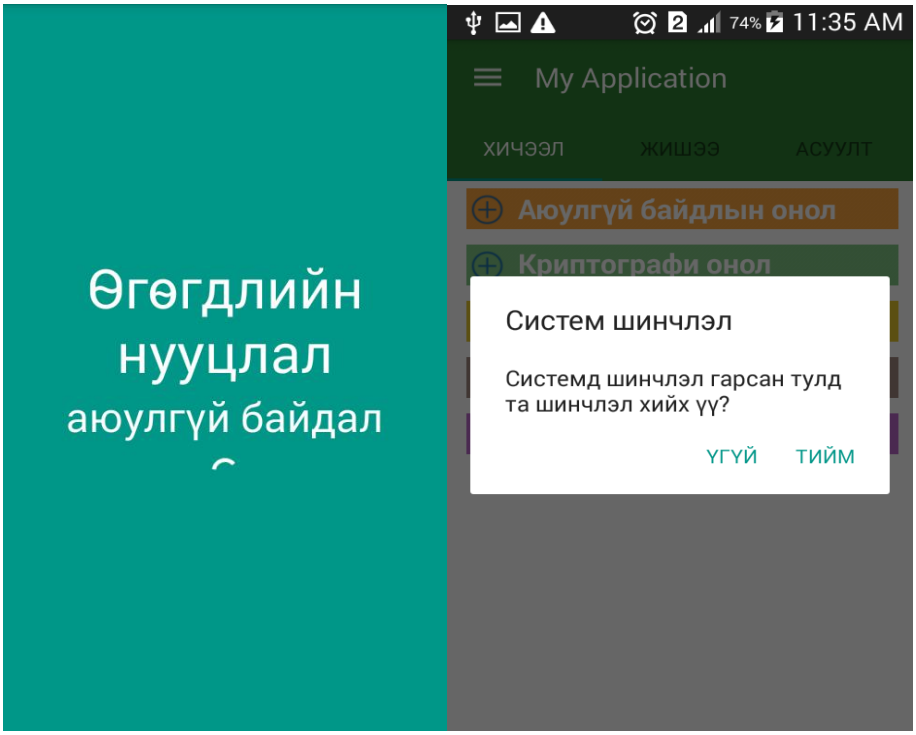
Энэхүү системийг хийж гүйцэтгэснээр өмнө нь ашиглаж үзэж байгаагүй сүүлийн үеийн шинэлэг техник технологи, арга барилуудыг судалж ашиглалаа. Мөн олон дэд дэд системүүдийг интегрейшн хийж нэгдсэн систем үүсгэж арвин туршлага хуримтлуулж авч чадлаа. Мөн системд хичээл цэсэнд өөрийн судалсан онолын судалгаанд үндэслэн таван бүлэг хорин хоёр дэд бүлгийг агуулгатай нь нэмлээ. Жишээ цэсэнд жишээ болгон криптограф болон sql тарилгын жишээ нэмлээ. Асуулт цэсэнд жишээ болгон гурван асуулт оруулж хариултыг нэмлээ.

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://jquery.com/
6. http://getbootstrap.com/
7. https://www.sqlite.org/
8. https://www.androidhive.info/
9. https://www.javacodegeeks.com/
10. https://www.w3schools.com/

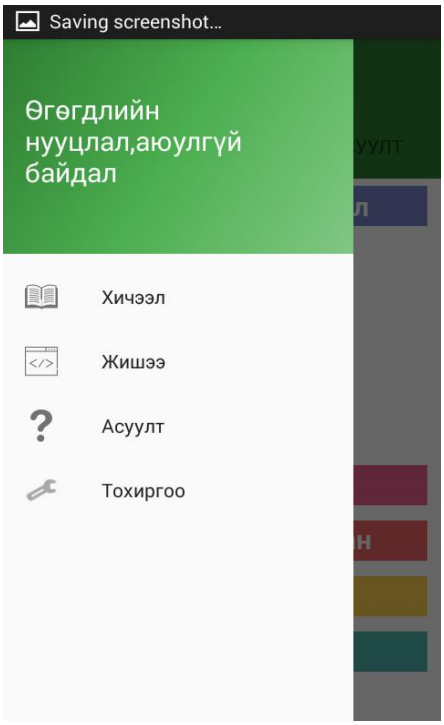
ХАВСРАЛТ А

Гар утасны програмын ажилгаа:



Програмыг ажиллуухад болгонд интернет холболтыг шалгана. Хэрэв интернетэд холбогдсон бол шинэчлэл гарсан үед автоматаар дараах цонх гарч ирнэ. Энэ талбар нь програмд шинэчлэл хийх эсэхийг асуусан асуулга ба зөвшөөрсөн тохиолдолд програмд шинэчлэл хийгдэнэ.

Мөн шинэчлэл хийхийг зөвшөөрөөгүй тохиолдолд хуучин програм үргэлжлүүлэн ажиллана.



Програмын үндсэн цэсүүд

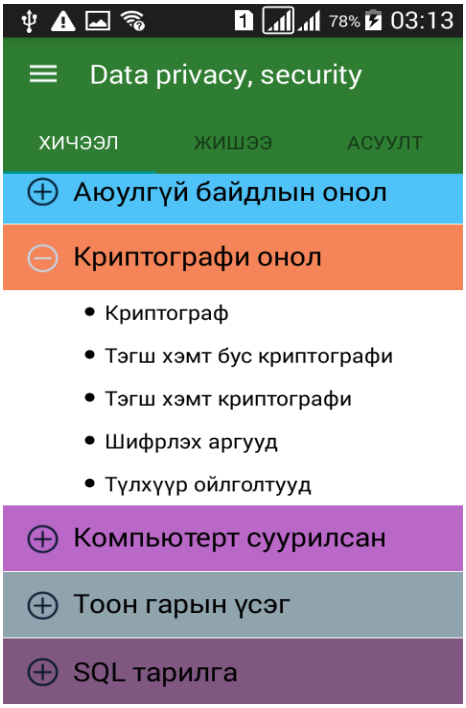
1. Хичээл

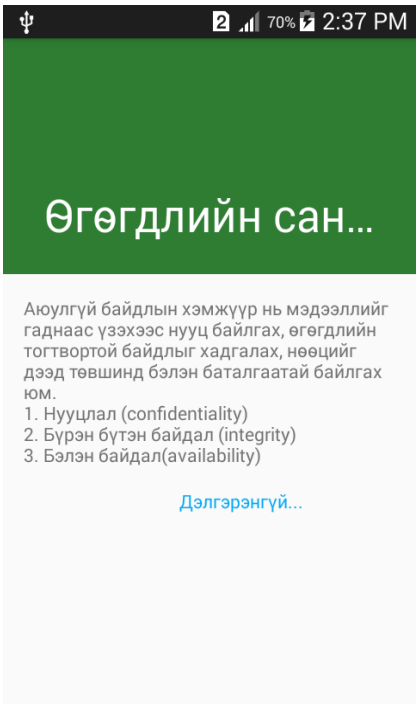
   Энэхүү цэсэн өгөгдлийн нууцлал, аюулгүй байдлын үндсэн ойлголт түүний бичиг баримт байна.
2. Жишээ

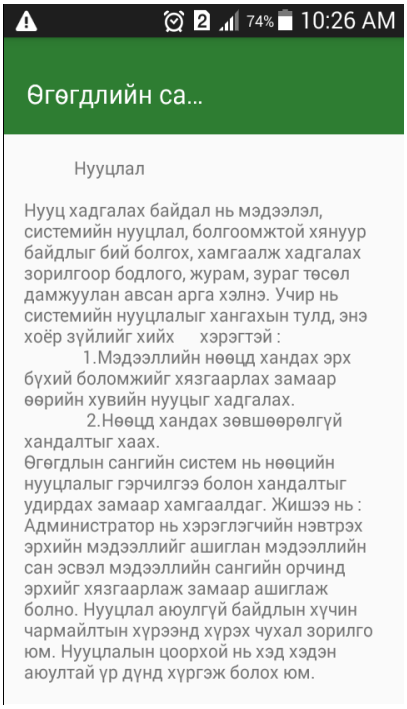
   Хичээл цэсэнд багтсан хичээлүүд дээр үндэслэн боловсруулсан асуулт хариулт байна.
3. Асуулт

   Өгөгдлийн нууцлал, аюулгүй байдлын талаар өөрт тулгарч буй асуултаа багшаасаа асуух, мөн бусдад тулгарсан асуудлыг хэрхэн шийдвэрлэснийг харах боломжтой
4. Тохиргоо

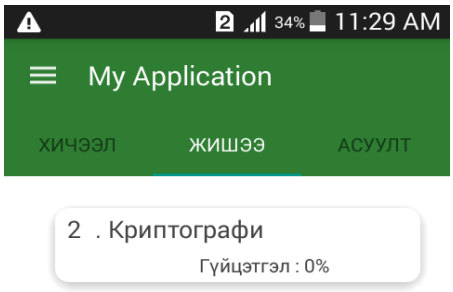
   Системд шичлэл гарсан эсэхийг өөрөө шалгах, шинчлэл хийх боломжтой.

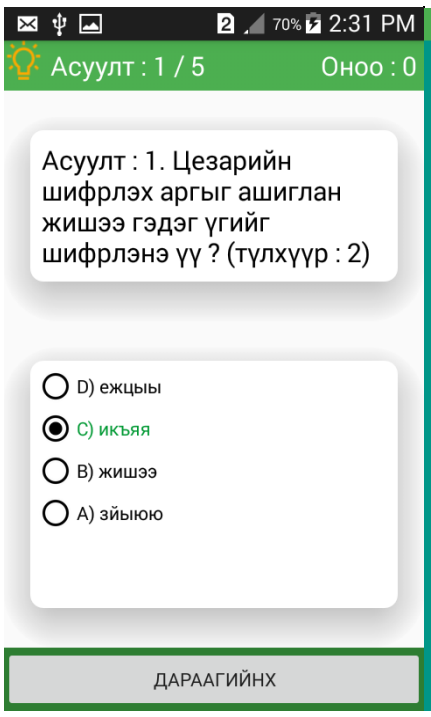


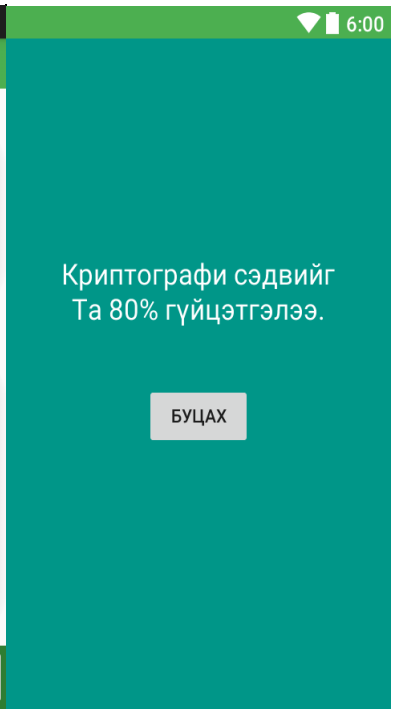




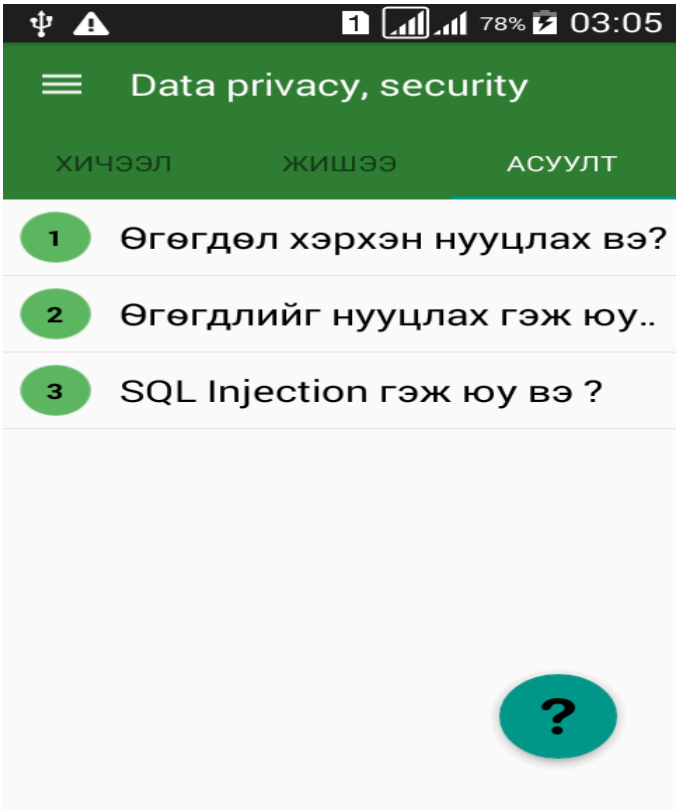
Хичээл цэснээс өөрт хэрэгтэй хичээлийн товчхон мэдээлэл авах мөн хүсвэл дэлгэрэнгүй мэдээлэл авах боломжтой байна.





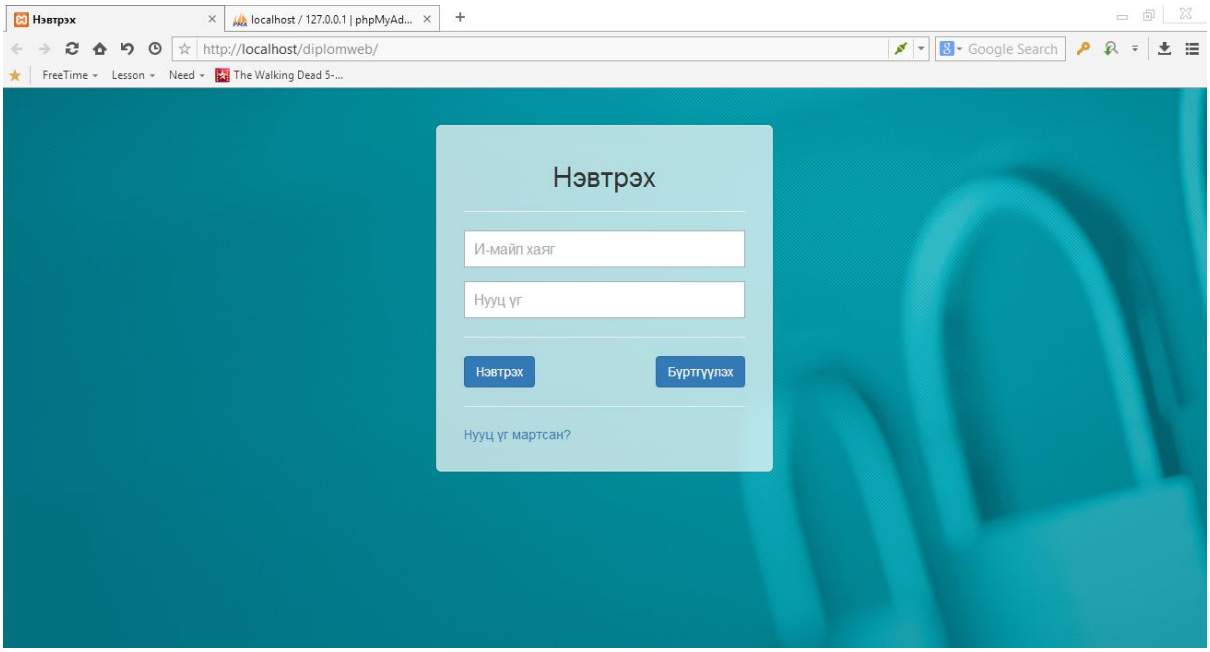


Жишээ цэснээс судалсан хичээлээ сонгон тухайн хичээлийнхээ тухай асуулт хариулт бөглөн дүгнүүлвэл боломжтой.

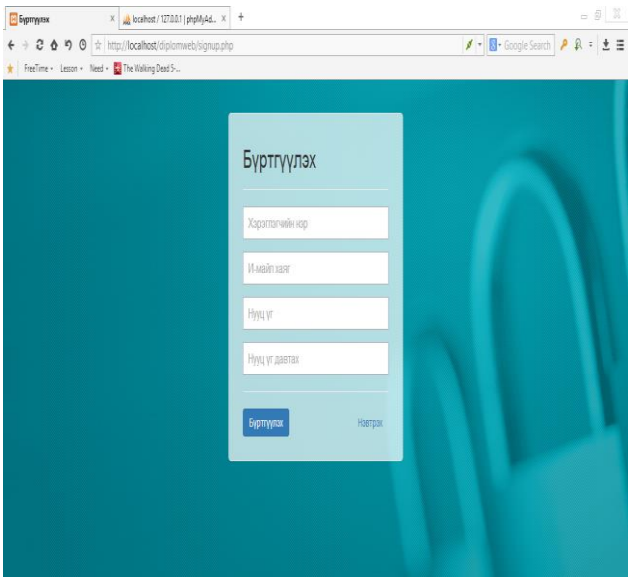


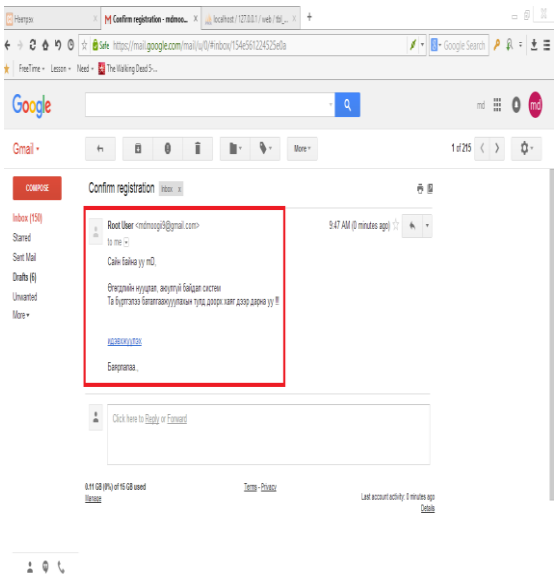
Асуулт цэсэнд өгөгдлийн нууцлал, аюулгүй байдалтай холбоотой өөрт тулгамдсан асуудлуудаа админ хэрэглэгчэээс асуух. Мөн бусад тулгамдсан асуудлуудын шийдлийг харах боломжтой.

Веб програмын ажилгаа:

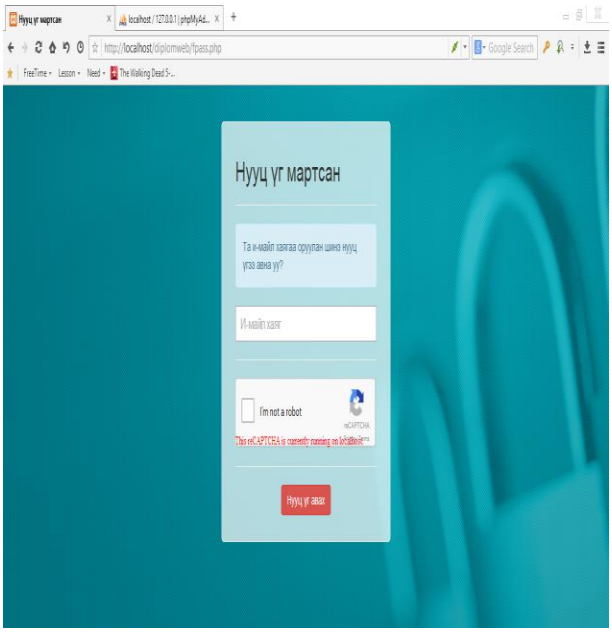


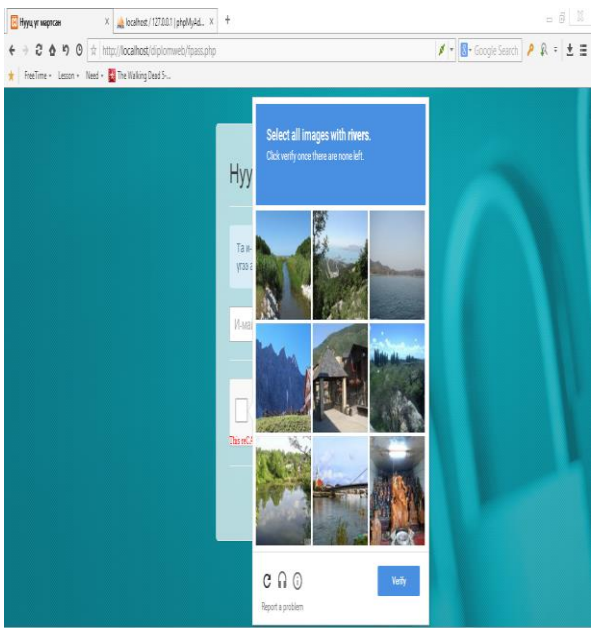
Системд хүсэлт тавьхад дараах харагдац харагдах ба админ хэрэглэгч буюу багш нь тухайн системд өөрийн бүртгэлийг үүсгэнэ. Үүсгэсэн бүртгэлээрээ



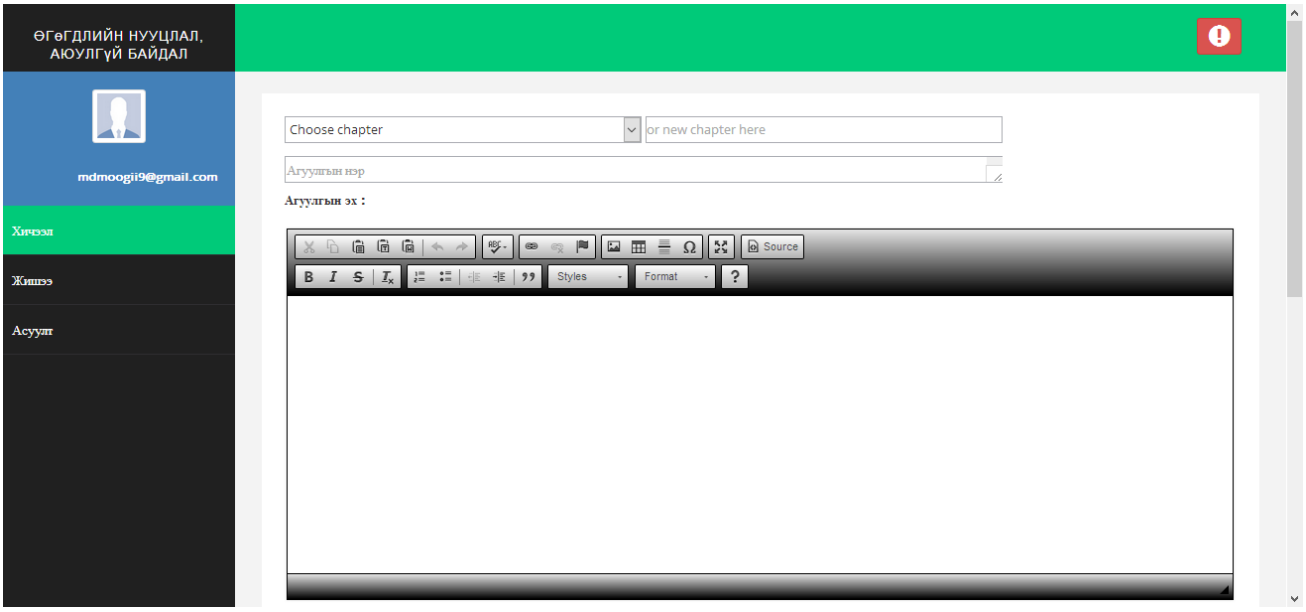


Хэрэглэгч системд бүртгэл үүсгэн и-мейл хаягаараа баталгаажуулсан тохиолдолд системд нэвтрэх эрхтэй болно.

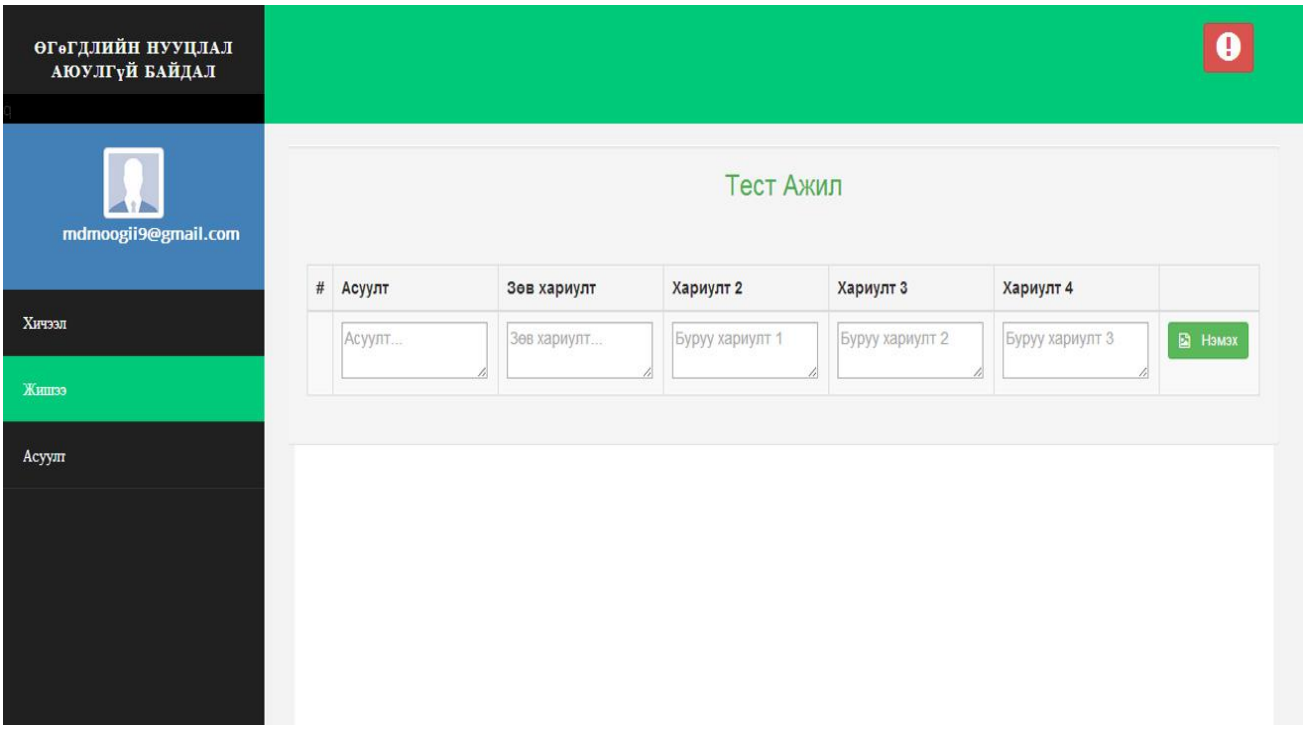




Хэрэглэгч нууц үгээ мартсан тохиолдолд и-мейл хаягаа ашиглан шинэ нууц үг авна. Ингэхдээ спам-с сэргийлэх зорилгоор катча бөглөнө.



Хэрэглэгч нэр нууц үгээ ашиглан системд нэвтэрсний дараа дээрх харагдац харагдах ба хэрэглэгчид ирсэн шинэ асуултууд мөн харагдана. Хичээл гэсэн цэс сонгогдсон байх бөгөөд хичээл нэмэх цонх мөн хичээл нэмэх цонхны доор бүх хичээлүүд харагдаfна.



Хэрэглэгч жишээ цэсийг сонгосноор одоо байгаа жишээнүүд харагдах ба шинээр жишээ нэмэх, жишээ засах, жишээ устгах боломжтой байна.

Хэрэглэгч асуулт цэсийг сонгосноор өгөгдлийн нууцлал, аюулгүй байдлын хүрээнд өөрт тулгамдаж буй асуудлыг асуух. Мөн бусдад тулгарсан асуудлыг хэрхэн шийдвэрлэсэн талаар мэдээлэл авах боломжтой.

ХАВСРАЛТ Б

Веб системийн аюулгүй байдал : SQL Injection

```
<script type="text/javascript">
  function checkPassword() {
    if($('#Password').val().length != 0) {
      var pattern = /(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{5,}/;
      if (!pattern.test($('#Password').val())) {
        $('#password').addClass('form-group has-error').removeClass('form-group has-success');
      }
      else {
        $('#password').addClass('form-group has-success').removeClass('form-group');
      }
    }
  }
</script>
```

Хэрэглэгчийн оруулсан нууц үгийг a-z, A-Z хүртэлх 5-аас дээш тэмдэгтээс бүрдсэн эсэхийг шалгах Javascript код. Хэрэв хэрэглэгчийн ашиглах нууц үг ийм бүтэцтэй биш бол нууц үг зөвхөн a-z, A-Z хүртэл 5-аас дээш тэмдэгтээс бүтнэ гэсэн сануулга харуулдаг байх юм.

```
$email = trim($_POST['txtemail']);
$upass = trim($_POST['txtupass']);

$word = array("'","/","include","connect","requre","or","select","union","from","drop","table","java","script");
foreach ($word as $color) {
  $upass = ereg($color,"",$upass);
}
```

Хэрэглэгчийн оруулсан нууц үгд хор хөнөөл учруулахуйц SQL асуулга үүсгэх боломжтой тэмдэгт болон үгүүд байна уу гэдгийг шалгаад байвал хасдаг код.

```php
try
{
    $password = md5($upass);
    $stmt = $this->conn->prepare("INSERT INTO tbl_users(userName,sisi_id,userEmail,userPass,tokenCode)
                                  VALUES(:user_name,:sisi, :user_mail, :user_pass, :active_code)");
    $stmt->bindparam(":user_name",$uname);
    $stmt->bindparam(":sisi",$sisi);
    $stmt->bindparam(":user_mail",$email);
    $stmt->bindparam(":user_pass",$password);
    $stmt->bindparam(":active_code",$code);
    $stmt->execute();
    return $stmt;
```

Хэрэглэгчийн оруулсан тэмдэгт мөрийг md5 функц ашиглан шифрлэж байна

userEmail	userPass
mdmoogii9@gmail.com	a44987440c0b9efdbd270eb6e4afe279

Өгөгдлийн сан дээр хэрэглэгчийн нууц үгийг шифрлэж хадгалсан байдал.