Батлав. Мэдээллийн сүлжээ, аюулгүй байдлын салбарын эрхлэгч:

..... /доктор (Ph.D) Б.Мөнхбаяр/

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

Дипломын төсөл гүйцэтгэх төлөвлөгөө

Дипломын төслийн сэдэв:
Монгол: " Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь"
Англи: " Developing Prototype System of Proxy Re-Encryption Scheme"

Төслийн зорилго: Proxy Re-Encryption схемийн хэрэглээнүүдийг судалж, нэгэн хэрэглээг хэрэгжүүлэх туршилтын систем хөгжүүлэх

Гүйцэтгэх оюутны овог нэр: А.Мягмарцэрэн/B190970106/
Холбоо барих утас: 99754252

№	Ажлын бүлэг, хэсгийн нэр	эзлэх хувь	дуусах хугацаа
Бүлэг №1. Өгөгдөл хуваалцах үйлчилгээний тухай			
1	1.1 Өгөгдөл хуваалцах үйлчилгээний тухай 1.2 Өгөгдлийн аюулгүй байдал 1.3 Шифрлэх схемүүд 1.4 Файл шифрлэх аргууд	20%	
Бүлэг №2. Прокси дахин шифрлэлтэд суурилсан файл хуваалцах систем			
2	2.1 Прокси дахин шифрлэлт 2.2 Хөгжүүлэх технологи, хэл сонгох 2.3 Хөгжүүлэлтийн орчин бэлдэх	40%	
Бүлэг №3. Прокси дахин шифрлэлтэд суурилсан файл хуваалцах систем хөгжүүлэх			
3	3.1 Системийн шаардлага 3.2 Системийн загвар 3.3 Системийн хөгжүүлэх 3.4 Файл хуваалцах системийг турших	40%	
Бүлэг №4. Ерөнхий дүгнэлт			

Төлөвлөгөөг боловсруулсан оюутан: ..... /А.Мягмарцэрэн/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 30% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-1		IV/03-IV/07	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-1 хийсэн багш: ..... /доктор (Ph.D) В.Нямсүрэн/

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 50% -с багагүй байна.	Огноо	доктор (Ph.D), Ц.Энхтөр багшийн гарын үсэг
1	Үзлэг-2			IV/17-IV/21	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-2 хийсэн багш: ..... /доктор (Ph.D), Ц.Энхтөр/

ТӨГСӨЛТИЙН АЖЛЫН ҮЗЛЭГИЙН ХУУДАС

Оюутны код: B190970106
Оюутны нэр: А.Мягмарцэрэн
Сэдвийн монгол нэр: ” Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь”
Сэдвийн англи нэр: ” Developing Prototype System of Proxy Re-Encryption Scheme”
Удирдагч багш: доктор (Ph.D) В.Нямсүрэн
Зөвлөгч багш: доктор (Ph.D), Ц.Энхтөр, магистр Ц.Манлайбаатар

№	Үзлэгийн гүйцэтгэл	Авсан оноо (10 оноо)	Гүйцэтгэлийн 70% -с багагүй байна.	Огноо	магистр Ц.Манлайбаатар багшийн гарын үсэг
1	Үзлэг-3			V/08-V/12	

Багшийн товч зөвлөгөө, тайлбар:

.....
.....
.....
.....
.....
.....
.....

Үзлэг-3 хийсэн багш: ..... /магистр Ц.Манлайбаатар/

№	Үзлэгийн гүйцэтгэл	Гүйцэтгэлийн 90% -с багагүй байна.	Огноо	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн гарын үсэг
1	Үзлэг-4		V/15-V/19	

№	Удирдагч доктор (Ph.D) В.Нямсүрэн багшийн үнэлгээ (30 оноо)	Огноо	Удирдагч багшийн гарын үсэг
1		V/17	

Удирдагч багш: ..... /доктор (Ph.D) В.Нямсүрэн/

Жич: Удирдагч багш өөрийн үнэлгээгээ 30 хүртэл оноогоор өгөх ба үнэлгээ тавьсан хуудсыг оюутанд буцааж өгөлгүй төгсөлтийн нарийн бичгийн даргад хураалгана уу.

ТӨГСӨЛТИЙН АЖЛЫН ЯВЦ

№	Хийж гүйцэтгэсэн ажил	Биелсэн хугацаа	Удирдагчийн гарын үсэг
1	Бүлэг №1. Proxy Re-Encryption схемийн онолын хэсэг	2023-4-28	
2	Бүлэг №2. Серверт шифрлэгдсэн файл хуваалцах судалгаа	2023-4-21	
3	Бүлэг №3. Proxy re-encryption систем хөгжүүлэх	2023-5-18	
4	Бүлэг №4. Ерөнхий дүгнэлт	2023-5-25	

Ажлын товч дүгнэлт

.....
.....
.....
.....
.....
.....
.....

Удирдагч: ..... /доктор (Ph.D) В.Нямсүрэн/

ЗӨВШӨӨРӨЛ

Оюутан А.Мягмарцэрэн–н бичсэн төгсөлтийн ажлыг УШК-д хамгаалуулахаар тодорхойлов.

Салбарын эрхлэгч: ..... /доктор (Ph.D) Б.Мөнхбаяр/

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

ШҮҮМЖИЙН ХУУДАС

Мэдээллийн сүлжээ, аюулгүй байдлын салбар–н салбарын төгсөх курсийн оюутан А.Мягмарцэрэн-н "Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь" сэдэвт төгсөлтийн ажлын шүүмж.

1. Төслөөр дэвшүүлсэн асуудал, үүнтэй холбоотой онолын материал уншиж судалсан байдал. Энэ талаар хүмүүсийн хийсэн судалгаа, түүний үр дүнг уншиж тусгасан эсэх.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

2. Төслийн ерөнхий агуулга. Шийдсэн зүйлүүд, хүрсэн үр дүн. Өөрийн санааг гарган, харьцуулалт хийн, дүгнэж байгаа чадвар.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

3. Эмх цэгцтэй, стандарт хангасан өөрөөр хэлбэл диплом бичих шаардлагуудыг биелүүлсэн эсэх. Төсөлд анзаарагдсан алдаанууд, зөв бичгийн болон өгүүлбэр зүйн гэх мэт /Хуудас дугаарлагдаагүй, зураг хүснэгтийн дугаар болон тайлбар байхгүй, шрифт хольсон, хувилсан зүйл ихээр оруулсан/.

   .....
   .....
   .....
   .....
   .....

4. Төслөөр орхигдуулсан болон дутуу болсон зүйлүүд. Цаашид анхаарах хэрэгтэй зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

5. Төслийн талаар онцолж тэмдэглэх зүйлүүд.

   .....
   .....
   .....
   .....
   .....
   .....
   .....

6. Ерөнхий оноо. (30 оноо)

   .....

Шүүмж бичсэн: ..... /магистр Г.Баяр/

Ажлын газар: .....

Хаяг (Утас) .....

Шинжлэх Ухаан, Технологийн Их Сургууль
Мэдээлэл, Холбооны Технологийн Сургууль

Хураангуй

Proxy Re-Encryption схемийн туршилтын системийг хөгжүүлэх нь

А.Мягмарцэрэн
b190970106@must.edu.com

Түлхүүр үгс: мэдээллийн аюулгүй байдал, прокси дахин шифрлэлт

Товчилсон үгс

PRE **P**roxy **R**e-**E**ncryption
BBS **B**laze **B**leumer **S**trauss

БҮЛЭГ 1

Өгөгдөл хуваалцах үйлчилгээний тухай

1.1 Өгөгдөл хуваалцах үйлчилгээ

Мэдээллийн технологийн хувьд өгөгдөл хуваалцах гэдэг нь өгөгдлийг олон хэрэглэгчид эсвэл програмуудад ашиглах боломжтой болгох практикийг хэлдэг. Мэдээлэл солилцох олон шалтгаанаас дурдвал алсаас ажиллах боломжийг нээнэ, ажилын үр дүнг нэмэгдүүлэх, эсвэл гуравдагч талтай хамтран ажиллах зэрэг олон боломжийг олгодог.

1.1.1 Өгөгдөл хуваалцах технологиуд

Өгөгдөл хуваалцах олон технологи байдаг. Зарим технологиудаас дурдвал.

- **Өгөгдлийн агуулах (Data warehousing)** нь нэг буюу хэд хэдэн ялгаатай эх сурвалжийг нэгтгэсэн төвлөрсөн агуулах юм. Архитектур нь шатлалаас бүрддэг. Дээд давхарга нь тайлагнах, дүн шинжилгээ хийх, үр дүнг харуулдаг front-end клиент юм. Дунд шат нь өгөгдөлд хандах, дүн шинжилгээ хийхэд ашигладаг аналитик механизмаас бүрдэнэ. Доод шат нь өгөгдлийг ачаалах, хадгалах өгөгдлийн сангийн сервер юм. Дээд болон дунд түвшний программууд нь доод давхаргад хадгалагдсан нийтлэг өгөгдлийн багцыг хуваалцах боломжтой.
  - Олборлох, хувиргах, ачаалах суурилсан (ETL based data warehouse)
  - Олборлох, ачаалах, хувиргах суурилсан (ELT based data warehouse)
- **Хэрэглээний программчлалын интерфэйс (API)** нь программ хангамжийн бүрэлдэхүүн хэсгүүд тодорхой протоколуудыг ашиглан хоорондоо харилцах боломжийг олгодог механизм юм. Интерфейс нь хоёр программын хоорондох үйлчилгээний тохиролцоо гэж үзэж болно. Энэхүү тохиролцоо нь хэрхэн харилцах хүсэлт болон хариултыг тодорхойлдог. Хандалтыг нарийн тодорхойлж болдог ба хэрэглэгчид яг ямар өгөгдөл хүсч болохыг зааж өгдөг.
  - SOAP APIs
  - RPC APIs
  - Websocket APIs
  - REST APIs
- **Холбооны сургалт (Federated learning)** нь тархсан өгөгдлийг багц дээр хиймэл оюун ухааныг сургах боломжийг олгодог. Бүх өгөгдлийг нэг дор цуглуулж нэгтгэхийн оронд тус тусдаа төхөөрөмж дээр хадгалж зөвхөн загварын шинэчлэлтүүдийг төв сервер рүү илгээдэг.
- **Блокчейн технологи** нь сүлжээн дотор ил тод мэдээлэл солилцох боломжийг олгодог өгөгдлийн сангийн дэвшилтэт механизм юм. Өгөгдлийг гинжин хэлхээнд холбосон блокуудад хадгалдаг. Сүлжээнээс зөвшилцөлгүйгээр гинжийг устгах эсвэл өөрчлөх боломжгүй.
- **Өгөгдөл солилцох платформууд**

  Нээлттэй өгөгдлийн платформууд нь өөр өөр өгөгдлийн багцыг нийтийн хэрэгцээнд ашиглах боломжийг ологдог. Ихэвчлэн өгөгдлийн менежмент, өгөгдлийн аюулгүй байдал, өгөгдөл нэгтгэх, өгөгдөл хуваалцах, хамтран ажиллах зэрэг олон төрлийн функцуудыг санал болгодог.

1.1.2 Файл хуваалцах

Олон хэрэглэгч эсвэл төхөөрөмж нэг файл эсвэл багц файлд хандах боломжийг олгох практикийг хэлнэ. Файл хуваалцахыг уламжлалт болон орчин үеийн янз бүрийн арга технологи ашиглан хийж болно.

- Физик зөөвөрлөгч: Файлуудыг CD, DVD эсвэл USB гэх мэт физик медиа ашиглан хуваалцаж болно. Энэ арга нь интернетийн хандалт хязгаарлагдмал эсвэл боломжгүй үед файл хуваалцахад тустай.

- Сүлжээгээр файл хуваалцах: Файлуудыг Server Message Block (SMB) эсвэл Network File System (NFS) зэрэг технологийг ашиглан дотоод сүлжээгээр хуваалцаж болно. Энэ арга нь байгууллага дотор эсвэл гэрийн сүлжээн дэх төхөөрөмжүүдийн хооронд файл хуваалцахад хэрэгтэй.

Орчин үеийн

- Клоуд сан: Dropbox, Google Drive эсвэл OneDrive зэрэг үүлэн хадгалах үйлчилгээ нь хэрэглэгчдэд үүлэн доторх файлуудыг хадгалах, бусадтай хуваалцах боломжийг олгодог. Энэ арга нь өөр өөр төхөөрөмж, байршилд файл хуваалцахад тустай бөгөөд интернэт холболттой хаанаас ч хандах боломжтой.

- Файл дамжуулах үйлчилгээ: WeTransfer, Hightail эсвэл Filemail зэрэг файл дамжуулах үйлчилгээ нь хэрэглэгчдэд том хэмжээний файлуудыг бусдад хурдан бөгөөд хялбар илгээх боломжийг олгодог. Энэ арга нь байгууллагаас гадуурх хүмүүстэй файл хуваалцах эсвэл имэйл хавсралтын хязгаарт хүрсэн үед хэрэгтэй.

- Per-to-peer файл хуваалцах: Peer-to-peer (P2P) файл хуваалцах нь хэрэглэгчдэд төвлөрсөн сервер ашиглахгүйгээр шууд бие биетэйгээ файл хуваалцах боломжийг олгодог. P2P файл хуваалцах нь ихэвчлэн кино, программ хангамж гэх мэт том файлуудыг хуваалцахад ашиглагддаг боловч бусад төрлийн файлуудыг хуваалцахад ашиглаж болно.

1.2 Өгөгдлийн аюулгүй байдал

Өгөгдлийн аюулгүй байдал гэдэг нь дижитал мэдээллийг зөвшөөрөлгүй хандах, өөрчлөх, хулгайлахаас хамгаалах үйл ажиллагаа юм. Физик төхөөрөмжийн хамгаалалтаас эхлээд хандалтын удирдлага, программ хангамжийн логик аюулгүй байдал мэдээллийн аюулгүй байдлын бүх талыг хамарсан ойлголт юм.

Нууц эмзэг мэдээлэл санхүүгийн чадамж бичиг баримт зэргийг буруу зорилгоор ашиглах боломжтой. Байгуулгын хувьд хэрэглэгчдийн мэдээлэлийг алдаж буруу гарт орохоос сэргийлж хамгаалах ёстой. Мөн тухайн байгуулга нь хакдуулах мэдээлээлээ алдах нь нэр хүнд нь халтай ба хэрэглэгчдийн итгэлийг алдах аюултай.

1.2.1 Өгөгдлийн аюулгүй байдлын төрлүүд

- **Шифрэлэлт** нь түлхүүр нууц үггүйгээр өгөгдлийг унших боломжгүй болгодог ба криптографын алгоритмуудыг ашиглан энгийн текстийг шифрлэх үйл явц юм. Энэ нь халдагчид өгөгдөлд нэвтэрсэн байсан ч зохих итгэмжлэлгүйгээр үүнийг уншиж чадахгүй гэдгийг баталгаажуулахад тусалдаг.

- **Хандалтын удирдлага** нь нууц өгөгдөлд хэн хандах эрхтэй болохыг тэдний үүрэг, зөвшөөрлийн түвшинд үндэслэн хязгаарладаг. Үүнд нууц үг, биометрийн баталгаажуулалт, хамгаалалтын токен зэрэг арга хэмжээ багтана.

- **Нөөцлөх, сэргээх** үйл явц нь аюулгүй байдлын зөрчил эсвэл өгөгдөл алдагдсан тохиолдолд сэргээх боломжтой байхын тулд мэдээллийн хуулбарыг үүсгэх, хадгалах явдал юм.

- **Физик аюулгүй байдал** нь өгөгдөл хадгалах төхөөрөмж болон физик хандалтыг хамгаалахын тулд түгжээтэй хаалга, хамгаалалтын камер зэрэг физик хамгаалалтын арга хэмжээг ашигладаг.

- **Өгөгдөл устгах** Өгөгдлийг устгах нь хамгийн аюулгүй хэдий дахин ашиглах боломжгүй. Ихэвчлэн дахин ашиглахгүй өгөгдлийн дарж бичих зэргээр устгадаг.

- **Өгөгдлийн далдлах** нь нууц мэдээллийг анхны өгөгдлийн бүтцийг хадгалан зөвшөөрөлгүй хэрэглэгчдэд ашиглах боломжгүй болгож буй хуурамч мэдээллээр солих явдал юм.

1.2.2 Өгөгдлөл хуваалцах эрсдэлүүд

- **Нууцлалыг задруулах**

  Хувийн нууцыг алдагдуулахгүйгээр өгөгдлийг хуваалцахын тулд шифрлэлт, засварлах зэрэг нууцлалыг хамгаалах технологи нь өгөгдлийг аюулгүй хуваалцах боломжийг олгодог.

- **Өгөгдлийн буруу тайлбар**

  Өгөгдөл бэлтгэгч болон хэрэглэгчдийн хоорондын харилцаа холбоо дутмагаас буруу тайлбар гарч болзошгүй. Шинжээчид тайлан, үр дүнг тайлбарлахдаа буруу таамаглал дэвшүүлж болно. Жишээлбэл, тухайн сард үйлчлүүлэгчдийн захиалга багассан нь маркетингийн төсөв багатай холбоотой байж болох ч бодит шалтгаан нь бүтээгдэхүүний бэлэн байдлын саатал байж болох юм.

- **Өгөгдлийн чанар муудах**

  Давхардсан эсвэл дутмаг чанар муутай өгөгдөл авах эрсдэлтэй.

Аюулгүй өгөгдөл хуваалцах

Байгууллагийн хэмжээ, төрөл, салбараас хамааран аюулгүй мэдээлэл солилцох олон арга зам байдаг. Дагаж мөрдөх эрсдэлгүйгээр өгөгдөл хуваалцах аюулгүй байдлыг хангахын тулд байгууллага бүр хийх ёстой зургаан алхмыг энд оруулав.

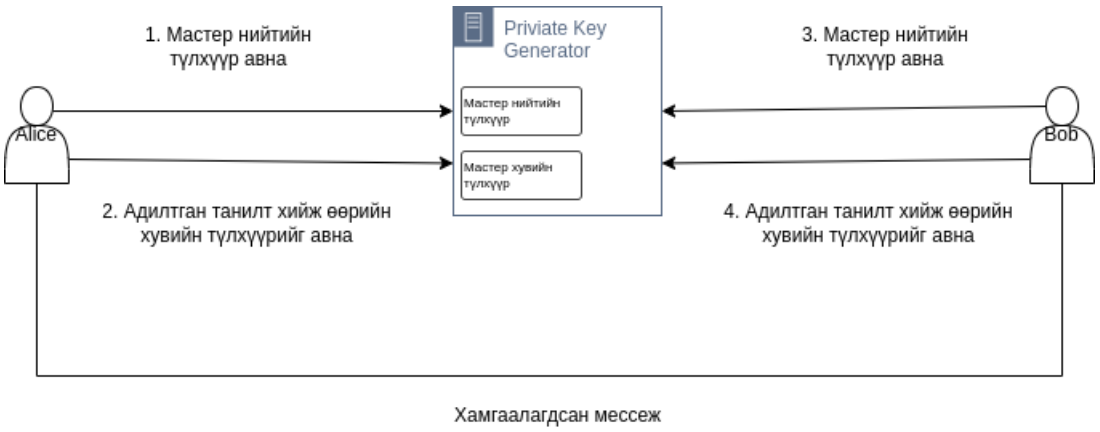
1. Өгөгдлийн ангилал, мэдээллийн удирдлагын бодлогыг бий болгох
2. Өгөгдөл хуваалцах аюулгүй байдлын зохих хяналтыг хэрэгжүүлэх
3. Таны нууц мэдээлэл хаана байгаа болон түүнд хэн хандах боломжтойг хянах
4. Аюулгүй бизнесийн харилцааны сувгуудыг ашигла
5. Аюулгүй мэдээлэл хуваалцах талаар ажилчдаа сурга
6. Бодлого, үйл явц, хэрэглүүрээ тогтмол хянаж үзээрэй

1.3 Шифрлэх схемүүд

Танилтад суурилсан шифрлэлт (IBE)

Тэмдэгт мөр зэрэг мэдэгдэж буй утгаас нийтийн түлхүүр үүсгэх боломжийг олгодог. Итгэмжлэгдсэн гуравдагч тал түлхүүрүүдийг үүсгэж өгдөг(PKG). Хувийн түлхүүр үүсгэгч (PKG) итгэмжлэгдсэн гуравдагч тал холбогдох хувийн түлхүүрүүдийг үүсгэдэг. PKG эхлээд мастер нийтийн түлхүүрийг нийлтэй тавьж, мастер хувийн түлхүүрийг хадгална. Аль ч тал мастер нийтийн түлхүүр, таних утгыг ашиглан тохирох нийтийн түлхүүрийг гаргаж авах боломжтой. Харгалзах хувийн түлхүүрийг авахын тулд мастер түлхүүрээр гаргаж авсан таних түлхүүрийг ашиглана.

1. Бэлтгэл үе: PKG нь өөрийн мастер түлхүүрүүдийг үүсгэнэ.
2. Алис нийтийн мастер түлхүүрийг авна. Өөрийн хувийн түлхүүрыг авна.
3. Боб-ийн имэйл гэх мэт өвөрмөц мэдээллээр Боб-ын нийтийн түлхүүрийг авч шифрлэлт хийн явуулна.
4. Боб PKG-ээс өөрийн хувийн түлхүүрийг авч шифрийг тайлж авна.



Зураг 1.1: Танилтад суурилсан шифрлэлт

Шинж чанарт суурилсан шифрлэлэт (ABE)

IBE-тэй ерөнхийдөө төстэй. Шинж чанаруудаар бүлэглэж зөвхөн нэг хэрлэгчийн түлхүүр ашиглахгүй олон хүн тайлах боломжтой. Үндсэн хоёр төрөлтэй. Түлхүүр-Дүрэмийн шинж чанарт суурилсан шифрлэлт(KP-ABE) болон Шифртекст-Дүрэмийн шинж чанарт суурилсан шифрлэлт (CP-ABE).

Гомоморф шифрлэлт (HE)

Энэ нь шифрлэгдсэн өгөгдлийг тайлахгүйгээр тооцоолол хийх боломжийг олгодог шифрлэлтийн төрөл юм.

- Хэсэгчилсэн гомоморф шифрлэлт нь зөвхөн нэг төрлийн хаалганаас бүрдэх хэлхээний үнэлгээг дэмждэг схемүүдийг хамардаг, жишээ нь нэмэх эсвэл үржүүлэх.
- Зарим төрлийн гомоморф шифрлэлтийн схемүүд нь хоёр төрлийн хаалгыг үнэлж чаддаг, гэхдээ зөвхөн хэлхээний дэд бүлэгт зориулагдсан.

- Түвшинтэй бүрэн гомоморф шифрлэлт нь хязгаарлагдмал (урьдчилан тодорхойлсон) гүнтэй олон төрлийн хаалганаас бүрдэх дурын хэлхээний үнэлгээг дэмждэг.
- Бүрэн гомоморф шифрлэлт (FHE) нь хязгааргүй гүнтэй олон төрлийн хаалганаас бүрдсэн дурын хэлхээг үнэлэх боломжийг олгодог бөгөөд гомоморф шифрлэлтийн хамгийн хүчтэй ойлголт юм.

Прокси дахин шифрлэлт (PRE)
Дахин шифрлэж өөр хүн тайлах боломжтой бологдог.

1.4 Файл шифрлэх хадгалах

Шифрэлэлт нь тэгш хэмт ба тэгч бус шифрэлт хэш үндсэн гурван төрөл байдаг.

1.5 Бүлгийн Дүгнэлт

Өгөгдөл хуваалцах болон өгөгдөлийн аюулгүй байдлын судалсан. Орчин үеийн шифрэлэлтийн схемүүдийн судлаж прокси дахин шифрлэх схемтэй харицуулж давуу тал болон сул тал харицуулсан.

БҮЛЭГ 2

Прокси дахин шифрлэлтэд суурилсан файл хуваалцах систем

2.1 Прокси дахин шифрлэлт

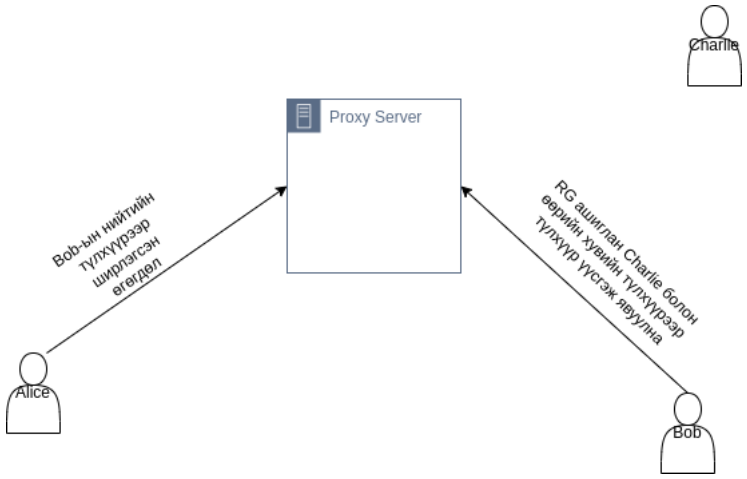
Прокси дахин шифрлэлт нь нийтийн түлхүүрээр шифрлсэн өгөгдөлийг дахин ширфлэж өөр хувийн түлхүүрээр тайлах боломжийг олгодог.

Үндсэн хоёр төрөлтэй.

- Нэг чиглэлт (Unidirectional PRE)
- Хоёр чиглэлт (Bidirectional PRE)

Нэг чиглэлт PRE (KE, RG, E, R, D) хэсгүүдээс тогтоно.

1. Алис, Боб болон Чарли хувийн болон нийтийн түлхүүрийг үүсгэнэ. (KE)
2. Алис Боб-д зориулж өгөгдлөө шифрлэж серверт байршуулна.
3. Боб Алис-ын өгөгдлийг Чарли-тай хуваацлахын тулд RE(pkB,skB,pkC,skC) шифрлэж серверт байршуулна. Чарлигийн хувийн заавал шаардахгүй үүсгэж болно.
4. Боб RE-г ашиглаж үүсэгсэн түлхүүрийг серверт явуулж Алисын файлыг дахин шифрлэж Чарли тайлах боломжтой болно.



Зураг 2.1: Proxy Re-encryption scheme

Давуу талууд:

- Нууцлалыг сайжруулна: PRE нь оролцогч талуудын хувийн мэдээллийг задруулахгүйгээр өгөгдлийг хуваалцахыг зөвшөөрснөөр нууцлалыг сайжруулахад тусална. Энэ нь талууд нууцаар эсвэл хувийн нууц мэдээллийг задруулахгүйгээр мэдээллээ хуваалцахыг хүссэн тохиолдолд хэрэг болно.
- Нарийн төвөгтэй байдлыг багасгасан: PRE нь итгэмжлэгдсэн гуравдагч этгээдэд шифрлэлт болон шифрийг тайлах үйл явцыг удирдах боломжийг олгосноор шифрлэлт болон түлхүүрийн удирдлагын нарийн төвөгтэй байдлыг багасгахад тусална. Энэ нь ялангуяа олон талын оролцоотой, гол менежмент нь төвөгтэй, удирдахад хэцүү болж болзошгүй тохиолдолд хэрэг болно.

Сул талууд:

- Проксид итгэх: PRE нь дахин шифрлэлтийг гүйцэтгхэд гуравдагч талын прокси дээр тулгуурладаг ба схемийн аюулгүй байдал нь прокси талаас хамаарна.
- Хязгаарлагдмал өргөтгөх чадвар: PRE нь өргөтгөх чадварын хувьд хязгаарлагдмал байж болно. Учир нь хэрэглэчдийн тоо нэмэгдэхийн хэрээр олон талыг дэмжихэд шаардлагатай дахин шифрлэлтийн түлхүүрүүдийн тоо хурдацтай өсөх болно. Энэ нь гол менежментийг төвөгтэй болгож, удирдахад хэцүү болгодог.
- Potential for replay attacks: PRE нь халдагч хариуг зогсоож хандах эрхийг өөрт ашигтай солих боломжтой.
- Хүчингүй болгоход хүндрэлтэй байдал: PRE дахь өгөгдөлд хандах эрхийг цуцлах нь ялангуяа олон тал оролцсон тохиолдолд хэцүү байж болно. Хэрэв аль нэг талын дахин шифрлэлтийн түлхүүр алдагдсан бол бусад талуудын мэдээлэлд хандах эрхэд нөлөөлөхгүйгээр өгөгдөлд хандах эрхийг цуцлах нь хэцүү байж болно.
- Хязгаарлагдмал хэрэглээ: PRE нь харьцангуй шинэ бөгөөд шинээр гарч ирж буй технологи хэвээр байгаа бөгөөд илүү уламжлалт шифрлэлтийн схемүүдтэй харьцуулахад хэрэглээ нь хязгаарлагдмал байдаг. Энэ нь технологийг хэрэгжүүлэх, удирдах туршлагатай мэргэжилтнүүд бага байдаг.

2.2 Хөгжүүлэх технологи, хэл сонгох

2.3 Хөгжүүлэлтийн орчин бэлдэх