Универзитет у Београду

Електротехнички факултет

Дипломски рад

Апликација за размену порука уз контролу приступа применом енкрипције засноване на атрибутима

Ментор:

Павле Вулетић

Студент:

Јован Ивковић 203/18

Београд, октобар 2023.

Захвалница

Родитељима, Ивани и Миодрагу, и сестрама, Емилији и Софији, хвала вам на разумевању и подршци током студија. На свим скуваним кафама, и спремљеним лимунадама и ужинама, буђењима за испите и сталног подсећања. Без вас цео процес би био много тежи.

Професору Павлу Вулетићу, на разумевању које ми је пружио приликом израде рада.

Садржај

1. Увод

Контрола приступа и енкрипција су кључни аспекти безбедности информација али доносе неке изазове у коришћењу у оквиру комплексних система као што су *Big Data* и IoT[1]. Ова комплексност може увести слабе тачке у системе безбедности и отежати управљање.

IoT доноси са собом изазове у смислу коришћења широког спектра разноврсних уређаја од паметних сатова до фрижидера који имају различите процесорске способности или меморију, што може ограничити могућности енкрипције. Процена је да ће број IoT уређаја бити преко 30,9 милијарди до 2025 [1]. Са толиким бројем уређаја повезаних на мрежу, дистрибуција, обнова и управљање кључевима представља велики изазов. Такође, поставља се питање и контроле приступа с обзиром на то да IoT уређаји често шаљу и примају податке па је важно осигурати да само овлашћени имају права приступа одређеним информацијама. Велика количина података коју генерише и користи IoT мрежа назива се језеро података[2] и подлеже концепту *Big Data*. Када је *Big Data* у питању поставља се питање перформанси система јер енкрипција и декрипција података захтевају значајну процесорску снагу јер је у овом случају у питању велики обим података што може довести до значајног кашњења.

Од велике је важности да се и енкрипција и контрола приступа обављају што је ефикасније могуће, због протока и обраде података великих размера, те је због тога проистекла потреба да се пронађу нова решења и алгоритми. У овом раду објаснићемо и демонстрирати основне функције и начине рада једног понуђеног алгоритма, енкрипције засноване на атрибутима, којим има потенцијал за широку примену.

[1] *Internet of Things*, интернет ствари

[2] енг. *Data lake*

2. Енкрипција заснована на атрибутима

Енкрипција заснована на атрибутима[3] (ABE) представља значајан напредак и модеран приступ у области криптографије јавног кључа. ABE је систем који се и даље усавршава и није још увек широко распрострањен.

2.1. Енкрипција и контрола приступа

Енкрипција је процес конвертовања читљивих података (познатих као *plaintext*) у нечитљиву форму (познату као *ciphertext*) коришћењем опредељеног алгоритма и кључа како би се спречило неауторизовано приступање и читање тих података. Представља кључни аспект информационе безбедности и има фундаменталну улогу у заштити података и информација у савременом свету.

Кључеви за енкрипцију служе као математички параметри који контролишу функцију енкрипције. Енкрипција се може класификовати као симетрична или асиметрична на основу типа кључева који се користе. Енкрипција је суштински инструмент за очување приватности и безбедности у данашњем дигиталном добу и неки сматрају да ће како технологија напредује и постаје све присутнија у свакодневном животу, те да ће са даљом дигитализацијом друштва њен значај наставити да расте.

Симетрична енкрипција, или енкрипција приватним кључем, користи исти кључ за шифровање и дешифровање података. Ако желите да некоме пошаљете тајну поруку користећи симетричну енкрипцију, и ви и прималац бисте морали да имате исти приватни кључ. Ако се овај кључ компромитује, нападач може и шифровати и дешифровати поруке. Са развојем интернета дошло је до проблема наглог пораста броја симетричних кључева који би био потребан за комуникацију између корисника. Наиме, за међусобну комуникацију n корисника било би нам потребно $\frac{n*(n-1)}{2}$ кључева, односно има квадратни раст. Због проблема који проистичу из потребе да се увећан број кључева сигурно чува и размењује, смишљен је концепт асиметричне енкрипције.

[3] енг. *Attribute-based Encryption*

Асиметрична енкрипција, или енкрипција са јавним кључем, користи пар кључева - јавни кључ (који се може слободно делити и јавно је доступан) за шифровање порука и приватни кључ (који треба да остане тајан) за дешифровање порука. За сваког корисника везан је један такав пар кључева. Примера ради, ако неко жели да пошаље тајну поруку, користио би јавни кључ примаоца за шифровање, али само би прималац могао да дешифрује ту поруку са својим приватним кључем. Веза између јавног и приватног кључа заснована је на математичким проблемима за које је лако верификовати решење (да ли приватни кључ одговара јавном), али га је веома тешко и захтевно наћи (извести приватни кључ из јавног). Асиметрична енкрипција осим тајности података може обезбедити верификацију идентитета пошиљаоца, тако што би он послати поруку енкриптовао својим приватним, а прималац је енкриптовао његовим јавним кључем. Овде треба напоменути да су симетрични алгоритми значајно бржи од асиметричних те се углавном користе за размену генерисаних симетричних кључева.

Тако је нашла примену:

- за обезбеђивању приватности у свакодневној комуникацији између људи за размену порука, имејлова и у заштити других личних података.
- у услугама онлајн трговине[4]користи се за заштиту осетљивих информација које се преносе приликом интернет куповине, попут бројева кредитних картица.
- у сервисима складиштења у облаку[5] обезбеђује кључни механизам заштите у виду приступа подацима у облаку где корисници чувају своје податке.
- за корпоративну безбедност где компаније користе енкрипцију како би заштитиле своје пословне тајне, интерну комуникацију и податке клијената.
- у банкарству служи за заштиту финансијских трансакција и података о рачунима корисника.
- дигиталном потписивању итд.

Контрола приступа је други кључни аспект безбедности информација. Док енкрипција спречава неовлашћен приступ подацима, контрола приступа је процес обезбеђивања података који омогућава организацијама да управљају ко је овлашћен да приступи

[4] енг. *e-commerce*

[5] енг. *cloud storage*

подацима и ресурсима. Сигурна контрола приступа користи политике које верификују идентитет корисника и осигурава да се одговарајући нивои приступа додељују корисницима. Њене компоненте су аутентификација, ауторизација, контрола и ревизија приступа. Постоје различити модели контроле приступа од којих ћемо навести ([1] и [2]):

- Дискрециона контрола приступа[6] (DAC) - власник информација има дискреционо контролише ко може да приступи информацијама.
- Контрола приступа заснована на атрибутима[7] (RBAC): права се додељују на основу улоге корисника унутар организације.
- Контрола приступа заснована на садржају[8] (CBAC): политика дефинише правила ко може видети које податке, а права се додељују на основу самог садржаја
- Контрола приступа заснована на атрибутима[9] (ABAC): најфлексибилнији модел контроле којим се могу емулирати сви остали, приступ се додељује на основу комбинације атрибута корисника и карактеристика окружења

2.2. Принцип рада ABE

ABE омогућава сложену контролу приступа подацима енкрипцијом на основу одређених атрибута корисника или карактеристика окружења/система, а не само на основу његовог јединственог идентитета како је то случај са традиционалним системима енкрипције са јавним кључем (пар јавни/приватни кључ је јединствени идентитет корисника у тим системима). ABE је систем којим се може обезбедити ABAC на нивоу података ефикасно и грануларно, што је последица тога да ABE омогућава парцијалну енкрипцију, за разлику од традиционалних система који раде на принципу све или ништа. Другим речима, ABE омогућује примену контроле приступа на нивоу података. Да би корисник био у стању да дешифрује податке потребно је да његов кључ, или поседује атрибуте који задовољавају политику приступа шифрованих података, или

[6] енг. *Discretionary Access Control*

[7] енг. *Role-based Access Control*

[8] енг. *Content-based Access Control*

[9] енг. *Attribute-based Access Control*

поседује политику приступа коју задовољавају атрибути шифрованих података, у зависности од варијанте система. Такође, ABE кључеви енкапсулирају више различитих атрибута, што смањује укупан број кључева у системима са сложеним приступним политикама.

Главни разлог за слабу распрострањеност ABE и њених имплементација је велика математичка комплексност система и алгоритама који су потребни за шифровање/дешифровање. Трошкови примене ABE у тренутку када је концепт предложен су били превисоки. Математичке операције које захтевају процеси енкрипције и декрипције били су превише захтевни за тадашње хардверске и софтверске капацитете, што је чинило ABE непрактичним за стварну употребу. Развој криптографских технологија, као што су криптографија елиптичних кривих[10] и енкрипција унутрашњег производа предиката[11], били су кључни за превазилажење изазова са ABE алгоритмом. Ова технолошка достигнућа омогућила су интеграцију ABE-а у модерне криптографске системе, где сада пружа гранулирану и ефикасну контролу приступа шифрованим подацима.

Увођење криптографије елиптичних кривих у ширу употребу, омогућило је ефикасније и безбедније шифровање података уз знатно мање рачунарских ресурса. Елиптичне криве пружају снажну криптографску заштиту користећи краће кључеве и веће брзине у односу на RSA, значајно убрзавајући процес шифровања и дешифровања. Уз већу ефикасност овог приступа, ABE је постао ближи стварној примени.

Енкрипција на основу елиптичних кривих, користи аритметику алгебарских структура елиптичних кривих над коначним пољима за постизање криптографских циљева. Основна идеја је да, док је лако множити тачке на криви, али тешко одредити једну на основу друге, тзв. "проблем дискретног логаритма". Најпознатија верзија је Вејлово[12] упаривање на елиптичним кривама Вајерштрасовог[13] облика.

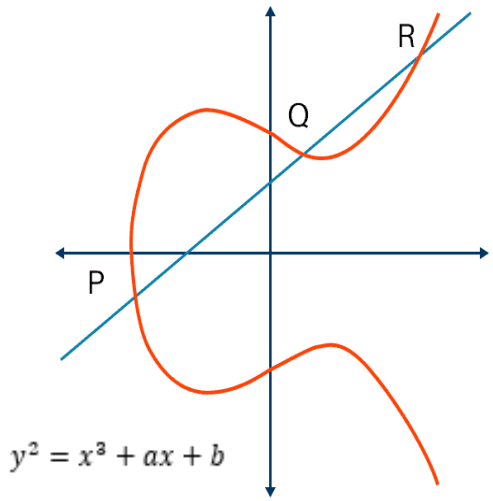
---

[10] енг. *Elliptic Curve Cryptography*

[11] енг. *Inner Product Predicates Encryption*

[12] André Weil (1906 - 1998), француски математичар

[13] Karl Theodor Wilhelm Weierstrass (1815 - 1897), немачки математичар



Слика 1 - Елиптична крива и њена формула

Даље, и релативно ново (функционално тек пар година), технолошко унапређење стигло је са енкрипцијом унутрашњег производа предиката (IPPE). Овај приступ омогућава изузетно флексибилну контролу приступа, где се дозволе заснивају на сложеним условима између атрибута и придружених политика, као и претрагу над енкриптованим подацима. Нека су два вектора, **v** (вектор атрибута асоцираним са шифрованим подацима) и **w** (вектор предиката асоциран са тајним кључем корисника). Тајни кључ корисника је конструисан тако да, како би корисник успешно дешифровао податке, унутрашњи производ ова два вектора мора бити једнак 0. Нпр. **v** = [1, -1, 1, 0, 0], корисник са кључем чији је вектор предиката **w1** = [0, 1, 1, -3, 4] био би у могућности да дешифрује податке, док корисник са кључем чији је вектор **w2** = [0, 1, 2, -3, -4] не би могао да приступи подацима ($\boldsymbol{v} * {w_1}^{\boldsymbol{T}} = \mathbf{0}$, док је $v * {w_2}^{T} = 1$).

Системи који користе IPPE могу бити веома флексибилни и могу се користити за имплементацију сложених приступних контрола. На пример, вектор **v** може представљати сет атрибута или права која су потребна да би се приступило одређеном ресурсу, док вектор **w** представља атрибуте или права које корисник поседује. Дешифровање је могуће само ако се услови између та два вектора подударају (тј. ако унутрашњи производ задовољава одређени критеријум). За примену IPPE неопходно је

направити систем који може да трансформише политике приступа и атрибуте у векторе предиката.

IPPE је моћан алат у области криптографије, јер омогућава софистицирану контролу приступа подацима на основу аритметичких услова, а не само класичне провере идентитета или припадности одређеној групи. Он представља један од основних градивних блокова за конструкцију напреднијих криптографских система, укључујући и ABE. IPPE је заправо специфичан облик ABE са одређеним особинама које га чине посебно погодним за одређене примене.

2.3. Предности и мане

ABE пружа подршку за потенцијално велики број атрибута. Повећање броја атрибута доводи само до линеарног повећања величине шифрованог текста, што је прихватљиво. Постоје варијанте ABE које значајно смањују величину шифрованог текста и уклањају чак и ову линеарну везу.

Политика приступа дефинисане су над овим атрибутима као логички изрази који могу имати комплексну структуру коришћењем AND, OR и NOT логичке капије и њиховим угњеждавањем. Треба напоменути да већина имплементација има ограничење да се сваки атрибут може појавити највише једном у логичком изразу политике приступа. Тај проблем се решава поделом атрибута на више нових тако да покривају одређене међусобно ексклузивне случајеве. Ово омогућава да се могу формирати комплексне политике приступа, које би могле да покрију разне ивичне случајеве.

Корисник може добити приступ ако и само ако његов кључ задовољава политику приступа. Измена права приступа своди се у том случају само на измену атрибута корисника.

Предности ABE енкрипције могу се сумирати као:

- **Флексибилност:** ABE омогућава креирање комплексних приступних политика. Приступ одређеним деловима података се може дати корисницима различитих категорија/класа.

- **Отпорност на заверу[14]:** Једна од важних карактеристика ABE је отпорност на колузионе нападе. То значи да чак и ако нападач држи више кључева и покуша да комбинује своје кључеве, неће моћи да дешифрује податке осим ако барем један од њих не задовољава потребну политику приступа.
- **Скалабилност:** ABE је дизајниран да буде скалабилан, што значи да може подржавати велики број атрибута и сложене политике приступа без значајног утицаја на перформансе. Такође, број кључева је смањен у односу на традиционалне приступе: Уместо да за сваки атрибут има по један кључ, ABE има један кључ који је везан за више атрибута.
- **Применљивост:** ABE је посебно користан у сценаријима где је потребна флексибилна контрола приступа на дистрибуираним системима, као што је програмирање у облаку или систем IoT уређаја. Више о применама ABE енкрипције видећемо у глави 3.

Иако је концепт ABE моћан и има значајног потенцијала, као и сваки систем, и ABE има своје недостатке.

Главна од њих је непостојање јасно дефинисаног механизма повлачења атрибута. Повлачење атрибута може значити одузимање тог атрибута од конкретног корисника, или уклањање атрибута из скупа свих могућих атрибута (односно одузимање атрибута свим корисницима који га поседују). Практични примери за одузимање атрибута конкретном кориснику и био када запослени у фирми добије унапређење и постане менаџер или пређе из одељења за маркетинг у одељење за стратегију. Пример за уклањање атрибута из скупа свих могућих би била реорганизација фирме укидањем постојећих одељења/одсека и формирањем нових.

Овде је од суштинске важности је направити разлику између атрибута дозвола и атрибута идентитета. Атрибути дозвола могу бити атрибути улога (одељење, позиција у фирми итд.) или атрибути окружења (локација, мрежа итд.). Атрибути идентитета се везују за идентитет корисника (биометријски подаци, имејл, јмбг итд.).

[14] енг. *collusion*

При укидању/одузимању атрибута генерални проблем код ABE је да атрибуте дозвола може имати више корисника, с тим у вези не постоји јединствени приступ како овај проблем решити и оно није тривијално. Најједноставније решење, али и оно које највише смањује перформансе, је да се кориснички кључеви генеришу поново при сваком захтеву за декрипцијом. На овај начин били бисмо сигурни да корисници баратају са правим атрибутима, али бисмо оптеретили централи сервер за генерацију кључева. Једно од предложених решења је и да се дода атрибут са тренутним датумом који би се мењао сваким новим даном, онда се претпоставља да сви корисници којима нису укинута права приступа ажурирају вредност атрибута једном дневно вредностима које добију од мобилног сервера кључева[15] (MKS), који служи као централни ауторитет/сервер. Овај алгоритам користи лење учитавање[16] па је могуће да прође и до 24 сата пре него што корисник добије праве вредности атрибута, односно буде уклоњен из система. Доказано је да постоји негативна корелација између пада перформанси централног ауторитета (мада је могуће у неким верзијама система са хијерархијским приступом да издавање кључева буде делегирано на регионалном нивоу, смањујући оптерећење централног сервера) и потенцијалног повећања времена које корисник може провести са погрешним атрибутима.

Иако проблем постоји и у ревизији атрибута дозвола, ревизија атрибута идентитета (нпр. промена имејла) доводи до потребе да се сав шифровани садржај који је био намењен конкретном кориснику мора дешифровати старом вредношћу и онда затим дешифровати новом вредношћу идентитета, с обзиром да и након те промене тај корисник треба имати приступ као ресурсима раније намењеним њему.

Један од кључних проблема везаним за атрибуте је и само планирање њиховог броја и назива. Како се компанија временом шири долазиће до проширења броја атрибута или промена њихових скупова вредности. Како код већина тренутних имплементација ABE дужина шифрованих података зависи од максималног броја атрибута јасно је да је потребно направити мудар одабир и стратегију називања атрибута. Иако се иде ка томе

[15] енг. *Mobile Key Server*

[16] енг. *lazy loading*

да енкрипција не зависи од максималног броја атрибута, технологија није и даље довољно узнапредовала.

Треба напоменути и то да је ABE неефикасан алгоритам у виду перформанси, јер време извршавања операције декрипције предуго као узрок тога што корисник (углавном) мора стално генерисати нове кључеве, с обзиром да је декрипција најчешћа операција у систему.

Једна од мањкавости ABE система је што (чак и код његових делегираних верзија) ипак постоји једна тачка отказа[17], а то је централни сервер односно MKS.

Мане ABE могу се сумирати као:

- **Велика комплексност:** ABE системи захтевају напредну математику и алгоритме, што их чини тежим за имплементацију и одржавање.
- **Перформансе:** Због своје комплексности, као и честих операција генерисања кључа, ABE је углавном доста спорији од традиционалних метода шифровања.
- **Управљање атрибутима:** Повлачење, одузимање и додавање атрибута је не тривијалан проблем и не постоји стандардизовано решење
- **Управљање кључевима:** Због потенцијалне невалидности кључева услед промена вредности или скупа атрибута, мора се обратити пажња на координацију, депоновање и одузимање кључева, узимајући у обзир како се променила политика приступа у односу на конкретног корисника.

[17] енг. *single point of failure*

2.4. Варијанте ABE шема

Иако постоји много варијанти ABE шема (само CP-ABE се може поделити на девет подварианти [4]) овде наводимо основне три. Такође, нове врсте и имплементације ABE се константно развијају, те можемо рећи да је ово веома живо поље криптографије.

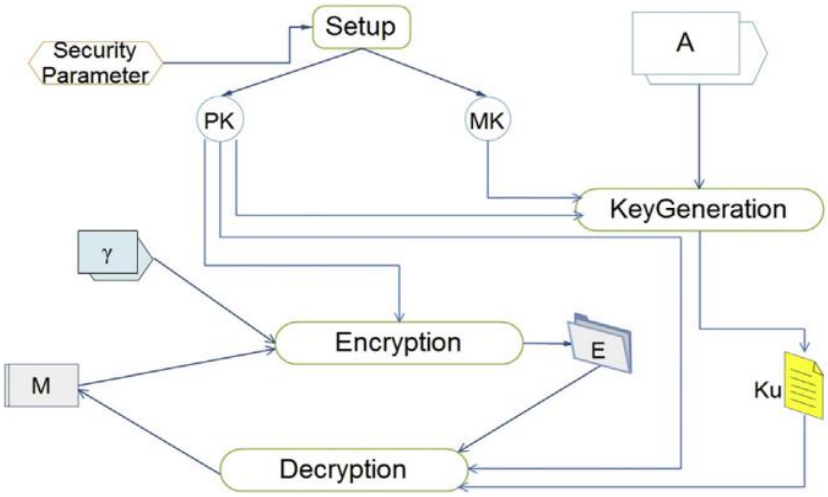
Од значаја би било напоменути и да у оригиналној поставци, ABE није била отпорна на пост-квантне нападе, с обзиром да су оне користиле криптографију елиптичних кривих, која се ослања на проблем дискретних логаритама који није безбедан у пост-квантном смислу, као градивни елемент. Међутим, активно се развијају нове врсте криптографије и система енкрипције, па је тако IPPE са дистрибуцијом кључева и сакривеном политиком приступа (DIPPE) [5], врста ABE која има анти-квантне особине. Такође, комбинацијом ABE са одређеним врстама других алгоритама добијају се анти-квантне перформансе енкрипције, што ћемо видети у наставку.

2.4.1. ABE са политиком кључа (KP-ABE)

У KP-ABE шеми[18] атрибути се користе за шифровање података, док кориснички кључ садржи политику приступа, у виду стабла приступа, која дефинише податке којима корисник може приступити. У KP-ABE, политика приступа је интегрисана у тајни кључ корисника, док су атрибути интегрисани у шифровани текст. Приступ је дозвољен ако атрибути шифрованог текста одговарају политици приступа која је уграђена у тајни кључ корисника. У KP-ABE сваки корисник добија тајни кључ у који је уграђена контрола приступа, енкодирањем у структуру са посебним пољима за вредност кључа и политику приступа или конкатенацијом на кључ, у виду логичког израза или стабла приступа. На исти начин се повезују и атрибути коришћени за шифровање са шифрованим подацима. Ово значи да су и политика приступа и атрибути коришћени за шифровање видљиви, и контрола приступа се врши пре самих операција декрипције, што значајно смањује време потребно да се утврди да ли је декрипција могућа, без извршавања математички скупих операција. Постоје врсте имплементација KP-ABE које сакривају приступну политику. На пример, кључ може бити повезан са политиком "Одељење=Маркетинг AND Позиција=Менаџер". Када неко жели да шифрује податке,

[18] енг. *Key-Policy Attribute-Based Encryption*

они дефинишу сет атрибута за те податке. На пример, подаци могу бити означени атрибутима "Одељење = Маркетинг" и "Пројекат = Омега" у ком случају корисник не би успео да дешифрује податке. Корисницима се генеришу тајни кључеви на основу политика приступа које су им додељене.



Слика 2 - KP ABE шема [9]

Систем KP-ABE се састоји од четири алгоритма, мада употреба јавног кључа у генерисању корисничког тајног кључа и декрипцији варира у зависности од конкретне имплементације:

Setup(lambda) = pk, mk - алгоритам за генерисање јавног и мастер тајног кључа, где је ламбда сигурносни параметар (нпр. величина скупа могућих атрибута)

E(pk, gamma, data) = gamma||cipher – алгоритам енкрипције, где је gamma је скуп атрибута којима се подаци шифрују

GenerateKey(mk, A, pk) = A||Ku - алгоритам генерисања корисничког тајног кључа, где је A политика приступа

D(pk, gamma ||cipher, A||Ku) = data – алгоритам декрипције

Корисник може дешифровати шифровани текст само ако сет атрибута шифрованог текста задовољава политику приступа повезану с његовим тајним кључем. Узимајући у обзир горе наведени пример, корисник с кључем повезаним са политиком "Одељење=Маркетинг AND Позиција=Менаџер" не може дешифровати податке

означене атрибутом "Одељење=Маркетинг", али може уз политику "Одељење=Маркетинг OR Позиција=Менаџер".

Главна карактеристика KP-ABE је у томе што тајни кључ корисника одређује политику дешифровања података. То омогућава флексибилност у контроли приступа где власници података могу слободно дистрибуирати шифроване податке, без директне контроле политике приступа, али само они са одговарајућим тајним кључевима (и одговарајућим приступним политикама) могу дешифровати те податке. Међутим, у виду политика које могу бити дефинисане, KP-ABE је на неки начин ограничен јер углавном постоји ограничење да се сваки атрибут може појавити највише једном у политици приступа. Иако делује да је могуће дефинисати више приступних политика које би омогућиле дешифровање, с обзиром да политику приступа одређује издавач кључева, а то је MKS, то није случај.

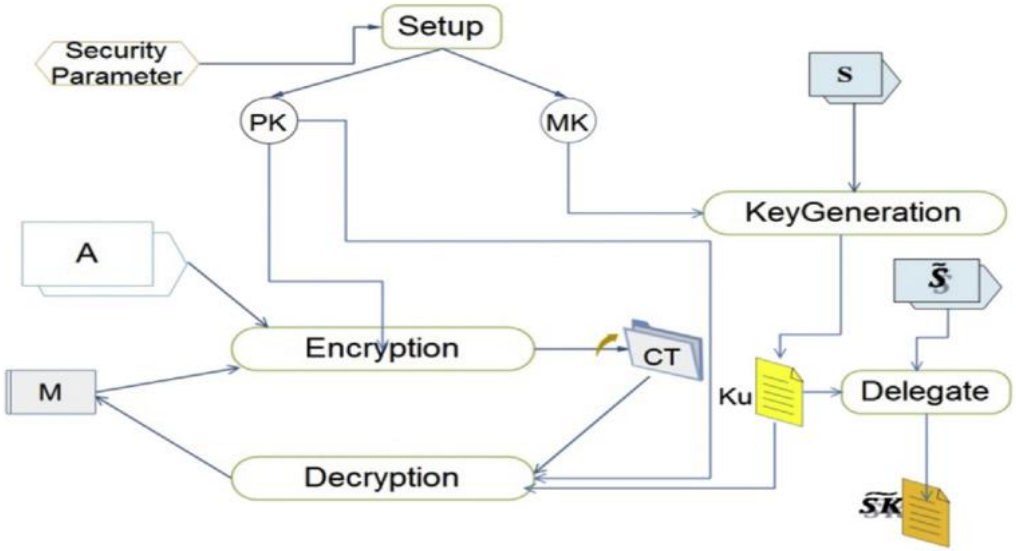
2.4.2. ABE са политиком шифрованог текста (CP-ABE)

У CP-ABE[19] подаци се шифрују са политиком приступа базираном на атрибутима корисника, при чему ови атрибути служе за креирање корисничких кључева. У случају имплементације ABE коришћењем криптографије елиптичних кривих, подаци се репрезентују као тачка на елиптичној криви, шифрују на одговарајући начин и онда се на њих конкатенира политика приступа у виду логичког израза или стабла . У имплементацији ABE засноване на IPPE, стабло приступа се преводи у вектор приступа, подаци се шифрују неким алгоритмом који зависи од имплементације и вектор приступа се конкатенира на шифроване податке.

Пре него што се подаци шифрују, дефинише се политика приступа која описује ко може дешифровати податке и од ње се формира стабло приступа. На пример, политика приступа може бити дефинисана као "(Одељење = Финансије AND Позиција = Менаџер)

[19] енг. *Ciphertext-Policy Attribute-Based Encryption*

OR (Одељење = ИТ AND Стаж > 5 година)". Подаци се шифрују користећи дефинисану политику приступа. Резултирајући шифровани текст садржи ову политику.



Слика 3 - CP- ABE шема [9]

Корисницима се додељују тајни са придруженим атрибутима. На пример, неком кориснику може бити додељен кључ који садржи атрибуте "Одељење = Финансије" и "Позиција = Менаџер". Корисник може дешифровати шифровани текст само ако његови атрибути задовољавају политику приступа уграђену у шифровани текст.

Систем CP-ABE се састоји од четири алгоритма:

Setup(lambda) = pk, mk - алгоритам за генерисање јавног и мастер тајног кључа, где је ламбда сигурносни параметар (нпр. величина скупа могућих атрибута)

E(pk, A, data) = A||cipher – алгоритам енкрипције, где је A политика приступа

GenerateKey(mk, s) = s||Ku - алгоритам генерисања корисничког тајног кључа, где је s скуп атрибута који су асоцирани са корисником.

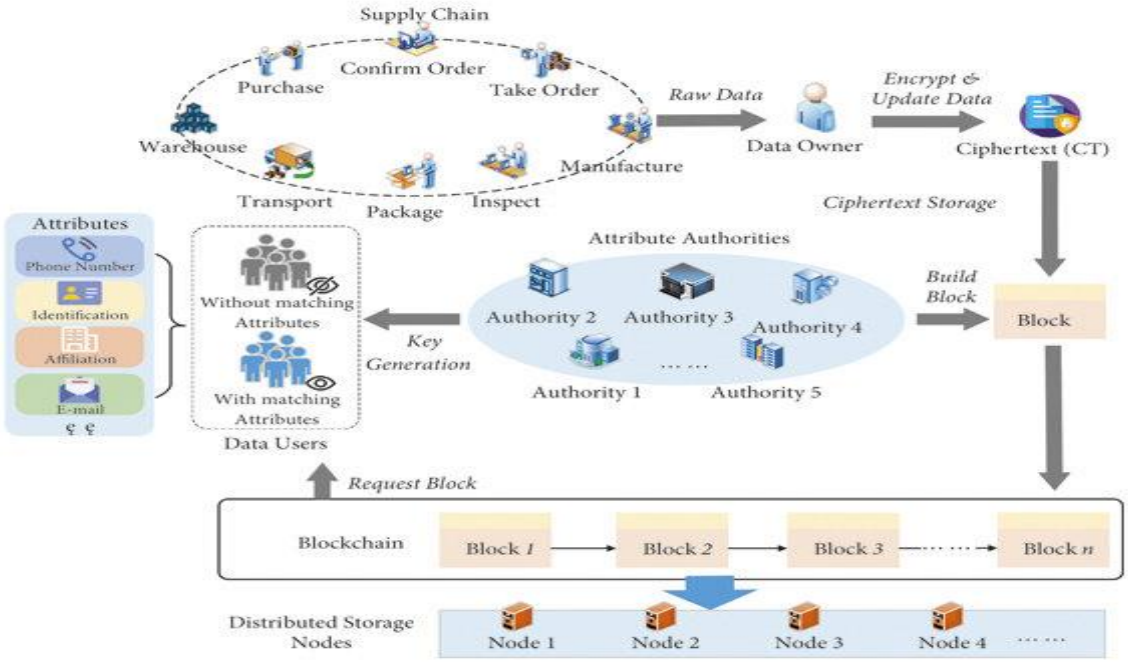
D(pk, A||cipher, s||Ku) = data – алгоритам декрипције

У горе наведеном примеру, корисник са атрибутима "Одељење = Финансије" и "Позиција = Менаџер" може дешифровати податке, јер његови атрибути задовољавају

дефинисану политику. Главна предност CP-ABE је у томе што омогућава фину грануларност и флексибилност у контроли приступа: власник података може дефинисати прецизне политике о томе ко може приступити подацима, а ове политике су директно интегрисане у шифровани текст. Другим речима, у CP-ABE, власник података одређује њихову политику приступа.

2.4.3. ABE са више ауторитета (MA-ABE)

MA-ABE[20] је варијација на стандардну енкрипцију засновану на атрибутима. У основи, док стандардни ABE систем има један централни ауторитет (CA) који управља атрибутима и издаје кључеве, MA-ABE системи имају више независних ауторитета који могу издавати кључеве за различите атрибуте. Један CA резултује тиме да систем има једну централну тачку отказа, тј. ризика (његовом компромитацијом било би компромитовано поверење у цео систем). У MA-ABE системима, више ауторитета управља различитим атрибутима, што дистрибуира одговорности и смањује ризик од компромитације.



Слика 4 - Архитектура MA-ABE система [10]

[20] енг. *Multi-Authority Attribute-Based Encryption*

У великим организацијама или распрострањеним системима, имплементација једног централног ABE система може бити непрактична. MA-ABE омогућава различитим деловима организације или система да функционишу као одвојене целине са сопственим ауторитетима. Пошто различити ауторитети управљају различитим атрибутима, теже је саставити комплетан профил корисника на основу његових атрибута.

У MA-ABE системима, политика приступа може се створити тако да захтева атрибуте из различитих ауторитета. На пример, корисник може требати атрибут "Одељење=Финансије" од једног ауторитета и "Позиција=Менаџер" од другог ауторитета да би дешифровао одређену поруку. У класичној поставци MA-ABE потребно је да корисник поседује атрибуте који задовољавају политике сваког од ауторитета појединачно. Постоје варијанте у којима је довољно задовољавати политику само једног ауторитета како би се дешифровали подаци које је тај ауторитет шифровао, без обзира да ли их је шифровао други ауторитет.

Повећање броја ауторитета као последицу има потребу за синхронизацијом између њих и обезбеђивање конзистентности у атрибутима и политикама приступа може бити сложено. Самим тим, потребно је одредити правилне стратегије додавања и одређивања атрибута. Такође, математичка и рачунска сложеност система са вишеструким ауторитетима може бити већа у поређењу са стандардним ABE системима.

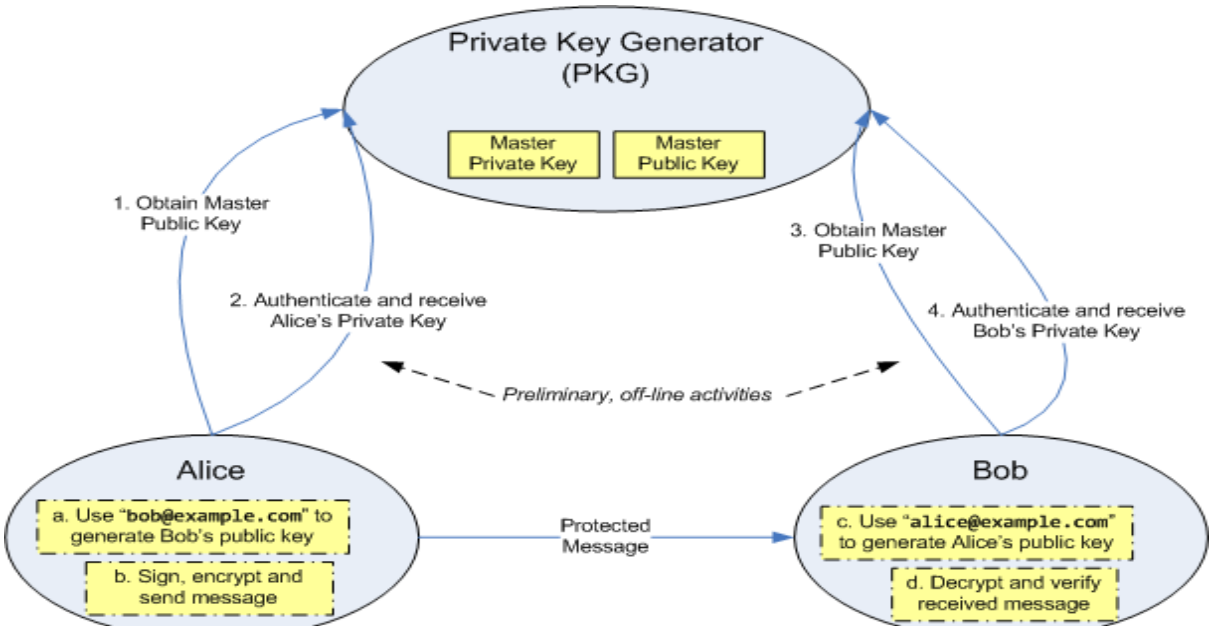
MA-ABE системи представљају, упркос свему, важан корак напред у развоју децентрализованих система контроле приступа који могу обезбедити већу приватност и безбедност за кориснике.

2.5. Сродне врсте енкрипције

АВЕ као врста енкрипције јавним кључем има директних и индиректних веза са више врста енкрипција јавним (у начину дефинисаности и примени) и приватним кључем (у имплементацији и употреби). У наставку ћемо навести сродне врсте енкрипција јавним кључем:

2.5.1. Енкрипција заснована на идентитету

Енкрипција заснована на идентитету[21] (IBE) представља асиметричну енкрипцију засновану на некој врсти ID-а (биометријски подаци, јмбг итд.). IBE је врста шифровања са јавним кључем у којој је јавни кључ корисника нека јединствена информација о идентитету корисника (нпр. адреса е-поште корисника). То значи да пошиљалац који има приступ јавним параметрима система може да шифрује поруку користећи нпр. текстуалну вредност имена или адресе е-поште примаоца као кључа. Пријемник добија свој кључ за дешифровање од централног ауторитета, коме треба веровати јер генерише тајне кључеве за сваког корисника. Код IBE јавни кључ може бити нека лако препознатљива информација, као што је e-mail адреса. И IBE пати од централизације ауторитета јер је потребан CA како би верификовао и издавао идентификације.



Слика 5 - Кораци у IBE енкрипцији [11]

[21] енг. *Identity-based encryption*

Иако ABE и IBE делују слично, главна разлика је у томе што ABE дозвољава енкрипцију која се ослања на комбинацију атрибута, док IBE користи јединствени идентификатор (као што је e-mail) као кључ. У том смислу ABE представља генерализацију IBE, чак је и развијање доказа о ваљаности IBE енкрипције претходило концепцији и истом таквом доказу за ABE, односно ABE је био интуитивни наставак развоја концепта IBE.

2.5.2. Хомоморфна енкрипција

Хомоморфна енкрипција[22] је посебна врста криптографске технике која омогућава извођење рачунских операција (аритметичких и логичких) директно на шифрованим подацима, без потребе за њиховим дешифровањем. Након што се операција изведе, резултат може бити дешифрован да би се добио тачан одговор. Ово пружа могућност обраде поверљивих информација у шифрованом облику, што гарантује заштиту података чак и током обраде.

Хомоморфна енкрипција је идеална у случајевима где организације желе да обрађују поверљиве податке без дешифровања, на пример, анализа података у облаку без излагања сирових података.

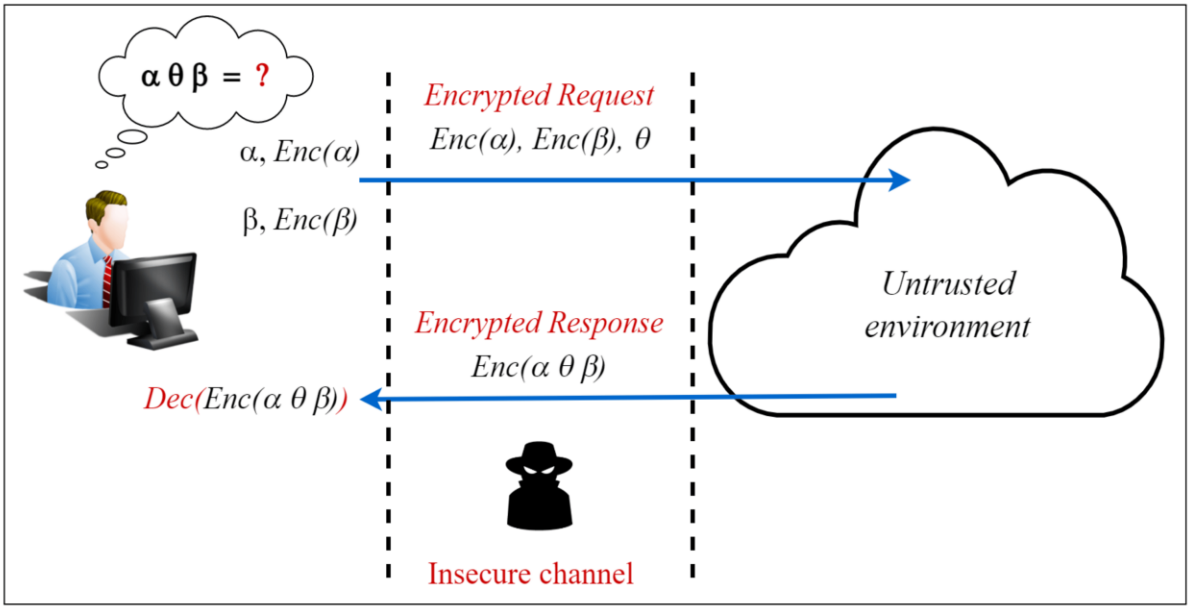
На пример, ако постоје два шифрована броја која треба сабрати, хомоморфна енкрипција омогућава да се та операција изведе без дешифровања тих бројева. Када се резултат дешифрује, добиће се тачан збир тих бројева.

Овде ћемо изложити само најсложенију врсту, и ону са најширом применом, HE:

- **Потпуно хомоморфна енкрипција[23]** (FHE) омогућава неограничено извођење оба типа операција (аритметичких и логичких) над шифрованим подацима. Ово је најфлексибилнија, али и најизазовнија врста хомоморфне енкрипције за имплементацију.

[22] енг. *Homomorphic encryption*

[23] енг. *Fully Homomorphic encryption*



Слика 6 – Приказ интеракција у хомоморфној енкрипцији [12]

ABE је добар избор за комуникацију један-према-више и фино зрнасту контролу приступа подацима шифровања у окружењу у облаку. FHE омогућава серверима у облаку да изврше валидне операције са шифрованим подацима без дешифровања. Потпуно хомоморфно шифровање засновано на атрибутима (ABFHE) из решетки[24], не само да комбинује предности и ABE и FHE, већ тако конструисана може да се одупре и квантним нападима. [4]

Хомоморфна енкрипција, иако доста обећава у смислу потенцијалних апликација, и даље је предмет интензивних истраживања, посебно када је реч о питањима ефикасности и практичности имплементације у стварним апликацијама.

[24] енг. *lattices*

2.5.3. Функционална енкрипција

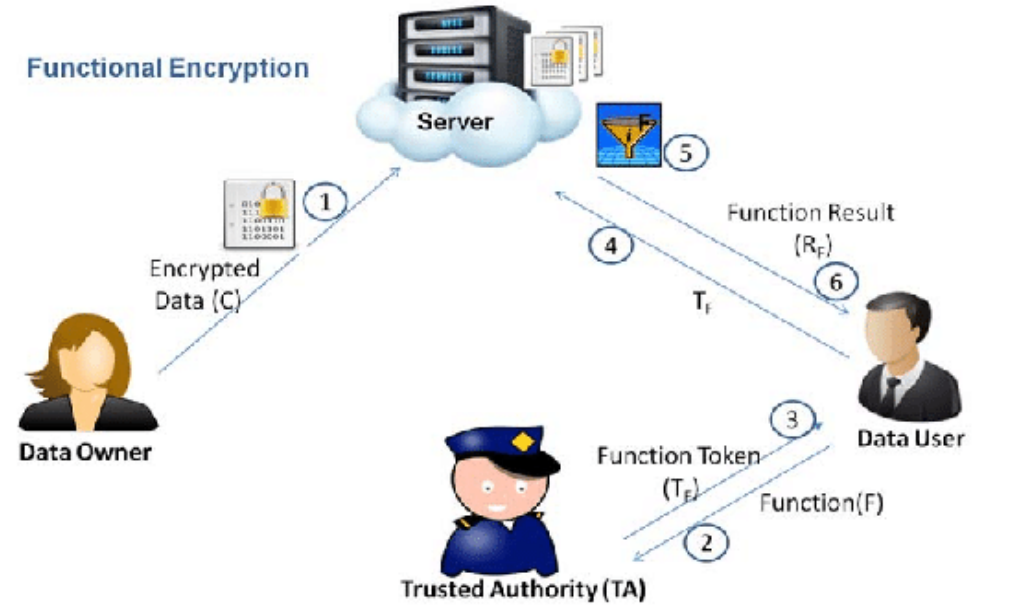
Функционална енкрипција[25] (FE) је генерализација енкрипције са јавним кључем у којој поседовање тајног кључа омогућава да се научи функција онога енкриптованих података.

FE, заправо, генерализује или може да емулира (теоријски) све алгоритме енкрипције са јавним кључем, укључујући енкрипцију засновану на идентитету (IBE) и енкрипцију засновану на атрибутима (ABE).

$$(pp, mk) \leftarrow \text{setup}(1^\lambda)$$
$$sk \leftarrow \text{keygen}(mk, k)$$
$$c \leftarrow \text{enc}(pp, x)$$
$$y \leftarrow \text{dec}(sk, c)$$

,где је $y = F(k, x)$ са вероватноћом 1.

Где су pp и mk редом, јавни и главни (мастер) тајни кључеви. k је одређени параметар (скуп атрибута) којим се генерише тајни кључ корисника sk, док су x и c, plaintext и ciphertext респективно.



Слика 7 – Могући сценарио примене функционалне енкрипције [11]

[25] енг. *Functional Encryption*

Може се рећи да за одређени кључ $fkey$ добијамо $dec(enc(x), fkey) = f(x)$. Самим тим функционална енкрипција превазилази ограничења дешифровања на све или ништа код класичних система. За $f(x) = x$ добија се класична енкрипција јавног кључа за k=1 и ништа уосталом. Лако се види и да разлишитим варијантама k и $f(x)$ можемо представити и генерализовати (барем у теорији) све системе енкрипције јавним кључем. Такође, можемо приметити да као и хомоморфна енкрипција, FE враћа функцију енкриптованих података, с тим што је главна разлика то да HE враћа шифровану вредност функције. Самим тим, да би се резултат HE могао искористити, свакако је потребно имати приватни кључ корисника чији су подаци. Код FE то није случај, јер она враћа дешифровану вредност функције над енкриптованим подацима.

У практичне сврхе, функција f не може бити произвољна. Уместо тога, постојеће FE шеме су скројене за специфичне класе функција. До сада, ефикасне FE шеме постоје само за линеарне (унутрашње производе) и квадратне полиноме. Иако FE шеме засноване на више-линеарним мапама и замагљивању неразлучивости[26] које подржавају општије функције већ постоје у теорији, тренутно су далеко од практичне.

[26] енг. *indistinguishability obfuscation*

2.6. Кратак историјат

- 1984. године Ади Шамир (Adi Shamir) је предложио први пут IBE, али без конкретног решења или доказа. Након што је представио концепт, није дошло до напретка на овом пољу дуги низ година

- 1985. године Нил Коблиц (Neal Koblitz) и Виктор С. Милер (Victor S. Miller) су независно предложили употребу елиптичних крива у криптографији. Ови алгоритми улазе у широку употребу између 2004. и 2005.

- 2001. године шеме засноване на Бонеј-Френклин спаривањима (Boneh–Franklin pairings) и шема енкрипције Кокса (Cocks) засноване на квадратним резидуалима су решиле проблем енкрипције засноване на идентитетима (IBE)

- 2004. Амит Сахаи (Amit Sahai) и Брент Вотерс (Brent Waters) су објавили решење које су накнадно побољшали Випул Гојал (Vipul Goyal), Омкант Пандеј (Omkant Pandey), Амит Сахаи и Брент Вотерс 2006. године. (референца на fuzzy identity base encryption)

- 2007. године Мелиса Чејс (Melissa Chase) и други истраживачи су предложили енкрипцију засновану на атрибутима са више овлашћења који заједно генеришу приватне кључеве корисника. [7]

- 2013. године Сергеј Горбунов (Sergey Gorbunov), Винод Ваикунтанатан (Vinod Vaikuntanathan) и Хоетек Ви (Hoeteck Wee) су објавили „Енкрипцију засновану на атрибутима за кола“ која представља прву шему енкрипције засновану на атрибутима за готово све приступне политике. Шема такође постиже пост-квантну безбедност, што значи да је та криптографска шема отпорна на потенцијалне нападе помоћу квантних рачунара. Другим речима, чак и када квантни рачунари постану практично доступни и моћни, ова шема ће и даље бити сигурна.

- 2007. године Амита Сахаиа и Брента Вотерса предлажу функционалну енкрипцију (FE)

- 2007. године Џонатан Кац (Jonathan Katz), Амит Сахаи и Брент Вотерс уводе појам енкрипције са предикатом која подржава дисјункције, полиномијалне једначине и унутрашње производе.

- 2010. године Дан Бонеј, Амит Сахаи и Брент Вотерс формализују FE. Међутим, до скоро, већина инстанци функционалне енкрипције подржавала је само ограничене класе функција, као што су Булове формуле. [8]

- 2012. године неколико истраживача је развило шеме функционалне енкрипције које подржавају произвољне функције.

- Европска Унија је финансирала пројекат FENTEC који је трајао у периоду од 2018. до 2021. Кроз пројекат су развијене нове имплементације функционалне енкрипција (FE) као ефикасна алтернатива "све или ништа" приступу традиционалне енкрипције.

3. Примена АБЕ енкрипције

Како је АБЕ енкрипција вид асиметричне енкрипције у којој приступ шифрованим подацима зависи од атрибута корисника, а не од конкретног идентитета (мада и идентитет може бити атрибут), ово омогућава АВЕ енкрипцији већу грануларност и вишеструку примену када је реч о контроли приступа. АВЕ енкрипција представља моћан алат за комплексна и динамичка окружења где традиционални методи контроле приступа можда нису довољно грануларни или адаптивни.

У наставку је дато неколико најзначајнијих области где се АБЕ енкрипција може применити:

3.1. Сервиси у облаку

У окружењима рачунарства у облаку, подаци могу бити шифровани коришћењем АВЕ тако да само овлашћени корисници, који задовољавају одређене атрибуте, могу приступити тим подацима. У комбинацији са одређеним алгоритмима дају вишеструку корист и штите сигурност података и приступа њима.

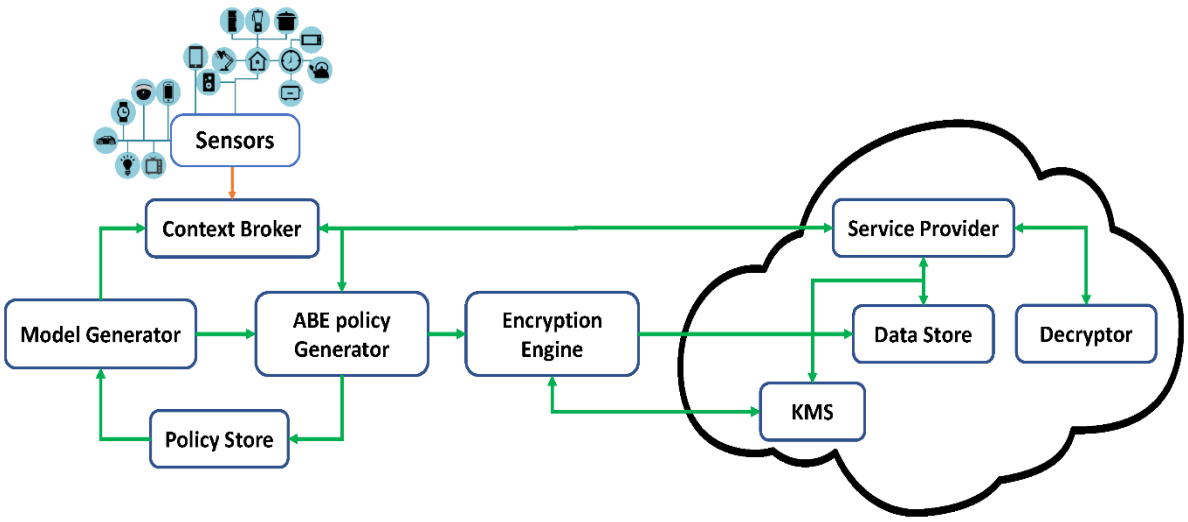
Нпр. у производима типа софтвер-као-сервис, много различитих корисника чува податке у облаку. Да би се уверили да при приступу облаку корисник може приступити само својим подацима, можемо користити АВЕ енкрипцију.

У претходном поглављу већ смо навели да у комбинацији са FHE, може се добити енкрипција која идеално испуњава потребе рачунарства у облаку. Па тако без пуног дешифровања података можемо проверавати и контролу приступа и вршити аритметичке истовремено над енкриптованим подацима.

Још једна синергична веза са другом енкрипцијом би била веза са претраживој енкрипцији. У овом слушају АВЕ може помоћи при претрази докумената на основу кључних речи, којима може да шифрује индекс документа, како би ефикасно проверио њихово присуство у документу. Наиме, уколико би смо оригинални индекс документа шифровали користећи кључне речи за претрагу, дешифровањем по политици кључних речи које се претражују, могли бисмо да добијемо прави индекс документа који тражимо уколико једна од кључних речи којима је шифровано испуњава нашу политику приступа (КР-АВЕ).

3.2. Паметни градови и IoT

У интегрисаним системима где многи сензори и уређаји комуницирају међу собом, ABE може ограничити ко може приступити и контролисати те уређаје. У паметним градовима, уређаји и сензори стално сакупљају податке о грађанима, као што су локација, потрошачке навике, здравствено стање итд. ABE може помоћи у заштити тих података тако да их може приступити или декриптовати само они који имају одговарајуће атрибуте.

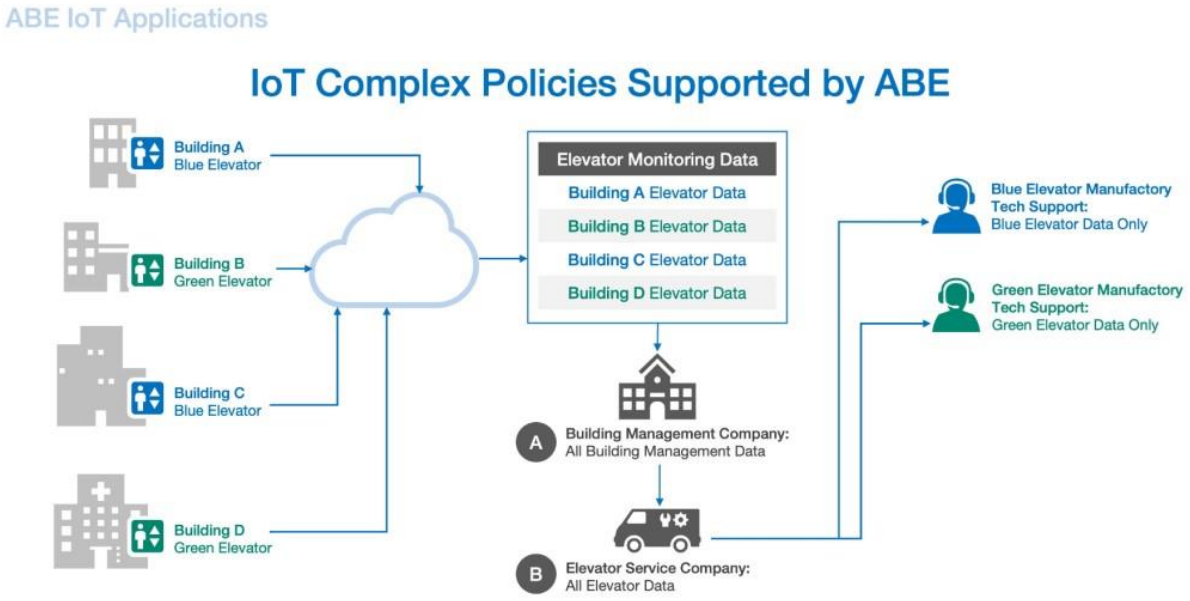


Слика 8 – Потенцијална архитектура ABE у паметним градовима [13]

У IoT окружењима, може постојати потреба да се одређеним подацима приступа на основу улоге или атрибута уређаја. Нпр., подаци о саобраћају можда су доступни само саобраћајним инжењерима или одређеним грађевинским компанијама.

Традиционални системи управљања приступима могу бити тежак за употребу на великој скали у паметним градовима. С обзиром на то да ABE користи атрибуте за одређивање права приступа, она може бити ефикаснија у таквим окружењима. IoT уређаји често функционишу у динамичким окружењима, где се уређаји стално додају, уклањају или ажурирају. ABE омогућава гипку и динамичку алокацију права приступа базирану на атрибутима уређаја.

ABE може помоћи у смањењу обима обавезних операција декрипције, с обзиром да ABE истом акцијом и декриптује садржај и врши контролу приступа, што је посебно корисно за IoT уређаје који можда раде са ограниченим ресурсима.



Слика 9 – Једна од могућих примена ABE у IoT-u [3]

Нпр., посматрајмо паметни град у коме користимо IoT уређаје за мониторинг и прикупљање података о раду лифтова у зградама. На нивоу сваке зграде би се агрегирали подаци везани за лифтове у тој згради. Сваки лифт има свој број модела, зграду којој припада, као и све остале придружене податке прикупљене од разних уређаја који су у њему инсталирани. Док би политика приступа подацима везаним за зграду била таква да јој може приступити само фирма која се бави њеним одржавањем, једна таква фирма би могла да види све податке везане за конкретну зграду. Лифтови би додатно своје податке могли шифровати атрибутом фирме која се бави њиховим одржавањем, као и бројем свог модела. Фирма за одржавање лифтова би на нивоу зграде могла да приступи само подацима о лифтовима, а у случају да морају да лифт сервисирају код стручних сервиса, могли би слободно да проследе све податке о лифтовима којима је потребно сервисирање, јер знају да ће сервиси дешифровати податке са бројевима модела лифтова које сервисирају, те су сигурни да ће добити информације само о оним лифтовима који су за сервисирање и за који су специјализовани.

У свету паметних градова и ИоТ, где безбедност и приватност постају све важнији, ABE представља моћан алат који може адресирати многе изазове и потребе.

3.3. Дигитални новчаник

Дигитални новчаник је концепт држања свих личних докумената, укључујући и платне податке (нпр. кредитне картице или број рачуна уколико треба да примити уплату), сертификате, пропуснице, здравствену књижицу итд., у дигиталном формату. Примена овог концепта олакшала би и убрзала процес верификације при коришћењу саме услуге. Наводимо као примере:

- Показивање пасоша и авионске карте на аеродрому.
- Очитавање карте за превоз и уплата средстава на њу.
- Скенирање КОВИД сертификата и слике са личне карте на фудбалској утакмици.
- Очитавање полисе здравственог осигурања итд.

Како дигитални новчаник садржи велики број различитих информација које су углавном сензитивне, основни захтев како би овај концепт имао практичну примену је да сваки ауторитет који захтева одређене информације, добије искључиво оне информације које су му потребне односно које захтева.

Применом ABE могуће је направити систем са децентрализованом дистрибуцијом кључева и више ауторитета [13] у којем би корисник на својој апликацији дигиталног новчаника давао одређене пермисије разним ауторитетима (нпр. за аеродром би дозволио приступ за авионске карте и пасош) и од њих добијао њихове јавне кључеве. На основу датих пермисија формирао би вектор политике приступа којим би, уз јавне кључеве ауторитета, енкриптовао свој новчаник. Тада би корисник могао да за одређени ауторитет изда кључ са одређеним правом приступа и пошаље га ауторитету. При верификацији ауторитету би било довољно да очита корисников енкриптовани новчаник (нпр. преко QR кода) и добије само потребне информације дешифровањем новчаника већ достављеним кључем.

У неким од ових примера, брзина је од суштинског значаја, с обзиром да нпр. хиљаде људи чека да уђе на утакмицу у исто време. ABE у овом случају испољава високе перформансе јер су контроле приступа уграђене у саме податке у дигиталном новчанику, тако да раде чак и кад је систем ван мреже. Нема потребе за приступом другом систему, као што је сигурносни сервер у облаку. [2]

3.4. Електронска пошта

Корпорације могу користити ABE да шифрују е-пошту и документе тако да само примаоци са одређеним атрибутима могу да их дешифрују.

ABE омогућава да се порука шифрује тако да је доступна само примаоцима који задовољавају одређени скуп атрибута. На пример, порука може бити шифрована тако да је читљива само члановима одређеног одељења у компанији или особама са одређеним нивоом одговорности. Може се чак ићи и на већу грануларност у самим порукама тако што би само одређени примаоци могли неки сегмент поруке да виде.

Приликом слања поруке, систем може аутоматски да енкриптује поруку на основу атрибута или метаподатака поруке (нпр. на основу теме или садржаја), и на основу тих атрибута може је обележити као хитно. Нпр. шифровање метаподатка неким атрибутима порекла, и означавање поруке као хитне уколико долази из болнице (ово се може утврдити тако што би покушали да дешифрујемо са политиком "Порекло=Болница", уколико би дешифровање било успешно поруку бисмо означили са хитно – КР-ABE).

Додатни документи у електронској пошти често садрже осетљиве информације. ABE може бити коришћен да се документи шифрују тако да их може отворити и читати само примаоци са одређеним атрибутима.

С обзиром на дугорочну архивацију е-поште, ABE може осигурати да старе поруке остану шифроване и заштићене, док је приступ ограничен на основу актуелних атрибута корисника. Такође, могуће је додати временски атрибут при шифровању, чиме би се обезбедило да порука или документ постане недоступан након одређеног времена.

За групне мејл листе или дистрибуционе листе, ABE може бити коришћен да се осигура да порука дође до правих особа у оквиру групе, засновано на њиховим атрибутима или улогама.

ABE може бити интегрисан са другим системима унутар организације (нпр. системом за управљање идентитетима) да би се динамички доделили или изменили атрибути корисника.

3.5. Остале примене

3.5.1. Медицински записи

У здравственом сектору, ABE може бити коришћена да шифрује пацијентове податке тако да само овлашћено особље (нпр. лекари одређене специјализације, медицинске сестре итд.) може да их види. На тај начин бисмо могли осигурати безбедност врло сензитивних података, као што су медицински, од неовлашћеног приступа.

3.5.2. Системи за управљање дигиталним правима

ABE може бити коришћен у DRM системима да ограничи приступ дигиталном садржају на основу атрибута корисника. Корисник дешифрује заштићени дигитални садржај употребом лиценце, из које се изводе одређени атрибути. Уколико је лиценца истекла или постала неважећа из неког другог разлога, приступ садржају биће онемогућен.

3.5.3. Војна и обавештајна комуникација

Ограничавање приступа тајним подацима на основу ранга, улоге или мисије корисника. На овај начин се прецизније одредити дозволе које свако службено лице има.

3.5.4. Електронско гласање

Омогућавање гласачима да шифрују своје гласове тако да само овлашћени ентитети могу да их обрађују. Нпр. само би РИК или контролери изборног места за које су задужени могли да очитају електронски гласачки листић, и то само ако се налазе на локацији која је придружена бирачком месту.

3.5.5. Бродкаст стриминг

Код стриминг сервиса као што су телевизија или подаци на DVD -у, могу се енкриптовати са ABE тако да само претплаћени корисници могу да их дешифрују и гледају.

3.5.6. Образовне платформе

Омогућавање наставницима и студентима да шифрују и деле материјале тако да само чланови одређене класе или курса могу да их приступе. Могуће је чак и саме материјале

(презентације, снимке предавања итд.) шифровати, тако да им се може приступити искључиво преко платформе када је студент улогован, јер су му тада очитани атрибути. У супротном материјали би били нечитљиви.

3.5.7. Безбедност индустријских система

У сектору индустријске контроле и система, ABE може бити коришћена да шифрује команде и податке тако да само овлашћени оператори и инжењери могу да приступе критичним системским контролама и подацима.

3.5.8. Ревизија логова

Свим програмерима у фирми је потребан приступ логу, међутим нису све информације у њему од значаја за сваког програмера, а неки програмери не би ни требало да виде неке информације (нпр. разлика у потребним информацијама за DevOps и оним за фронтенд програмере). У том случају, могуће је применити ABE како би се обезбедила грануларна контрола приступа информацијама у логовима на основу атрибута корисника , као што су тим или задужења.

4. Имплементација апликације за размену порука применом ABE

У овом поглављу биће описана спецификација проблема који се решава израдом апликације за размену порука, као и сви коришћени алати.

4.1.Спецификација решења

Практични део овог рада обухвата имплементацију апликације која треба да омогући сигурну размену порука са грануларном динамичком контролом приступа, као и приказ профила са статичком контролом приступа сензитивним информацијама, применом енкрипције засноване на атрибутима.

Посматрамо компанију у којој запослени често размењују поруке. Компанија нема развијену вертикалну организациону хијерархију и канале комуникације, те запослени на свим позицијама често размењују поруке са другим запосленима различитог ранга и из различитих одсека. Ове поруке су често обимне, а политика приступа различитим информацијама је комплексна. Информације којима располаже један запослени скоро увек су од значаја за већи број његових колега. Потребно је спречити редундантност порука у виду потребе корисника да шаље велики број порука које имају добар део истог садржаја међу собом, тако што би одређен садржај слао само запосленима који њему имају приступ. Последице редундантности порука је да се процес комуникације у компанији отежава и самим запосленима затрпава сандуче за поруке. Такође, потребно је да систем за размену порука омогућава запосленом преглед над свим колегама као и информације о њима, уколико је потребно да их контактира на други начин, али не сме доћи до неовлашћеног прегледа осетљивих података о колегама. У ту сврху, систем за размену порука мора бити имплементиран тако да омогућава да се у саму поруку угради грануларна контрола приступа њеним појединим деловима, као и контрола приступа осетљивим информацијама запослених. На овај начин иако је запослени прималац целе поруке, он ће моћи да приступи само оним њеним деловима за који има дозволу пошиљаоца, а биће послата само једна порука.

Систем се састоји из две међусобно независне компоненте:

1. клијентског графичког корисничког интерфејса (улога Клијент)
2. и серверског централног ауторитета (улога Сервер)

Клијента користе запослени у компанији и он им омогућава приступ и рад са системом за размену порука преко својих рачунара. Сервер је апликативни сервер самог система и потенцијално се налази ван система саме компаније (систем за размену порука је производ неке друге компаније који разматрана компанија користи, нпр. Slack), па Клијент и Сервер комуницирају преко интернета (HTTP-а). Сервер чува мастер кључеве за енкрипцију у бази, и генерише их по потреби.

Да би приступио коришћењу система, запослени мора да се аутентификује преко Клијента уносом својих креденцијала. Уколико је Клијент послао добре креденцијале, Сервер ће направити сесију за запосленог у којој ће сачувати његове атрибуте од значаја и у одговору му послати јавни кључ којим Клијент може енкриптовати нове поруке.

Након успешне аутентификације запослени може да:

- види све поруке које је примио или послао сортиране по времену од најскорије до најдавније.
- пошаље нову поруку
- прегледа профиле других запослених

Да би видео своје поруке запослени преко Клијента шаље захтев Серверу. Сервер извлачи из базе све поруке које су релевантне за запосленог на основу сесије корисника придружене захтеву, а затим генерише кориснички тајни кључ користећи атрибуте запосленог сачуване у сесији и мастер тајни кључ. Затим, декриптује садржај свих порука запосленог користећи кориснички тајни кључ и враћа их Клијенту у одговору. Клијент их затим приказује кориснику преко графичког корисничког интерфејса.

Да би послао нову поруку запослени преко Клијента уноси наслов поруке, имејл адресе примаоца поруке и садржај поруке. Садржај поруке се може или учитати из текстуалног фајла на Клијента или унети преко графичког корисничког интерфејса директно. Запослени на Клијенту одређује политике приступа одређеним секцијама садржаја поруке. Клијент пре слања поруке Серверу енкриптује садржај и наслов поруке, тако

што засебно енкриптује сваку секцију поруке користећи јавни кључ који му је послао Сервер приликом пријаве на систем и политике приступа коју је за ту секцију дефинисао запослени. Тако енкриптовану поруку Клијент шаље Серверу који је сачува у бази података.

За претрагу профила Клијент шаље захтев Серверу како би добио листу свих мејлова запослених у компанији. Запослени на графичком интерфејсу Клијента може да види листу мејлова и изабере мејл колеге чије профилне информације жели да види. Клијент затим шаље захтев Серверу са придруженом сесијом запосленог који је преко њега пријављен и мејлом запосленог чији профил се претражује. Сервер дохвата профил запосленог на основу прослеђеног мејла и генерише кориснички кључ на основу мастер тајног кључа и полисе, коју конструише на основу атрибута пријављеног запосленог придруженим сесији. Сервер декриптује осетљиве профилне информације корисника и шаље у одговору Клијенту пун профил траженог запосленог, уколико је декрипција била успешна, или само незаштићене информације из профила, уколико није. Клијент затим приказује запосленом профил од интереса преко графичког интерфејса.

Обе компоненте имплементиране су у Go програмском језику. Клијент је имплементиран у Fyne радном оквиру, док је Сервер имплементиран коришћењем Gin радног оквира. За базу података користи се PostgreSQL, а за комуникацију са њом као ORM се користи Bun. За енкрипцију је коришћена библиотека fentec-project/gofe и то из ње конкретно пакет abe и ABE шеме FAME и GPSW, као представници CP-ABE и KP-ABE респективно. Као атрибути за енкрипцију користе се имејл, позиција и одсек запосленог/корисника. Ограничење на обе шеме је да се сваки атрибут може у политици приступа појавити највише једном. Не постоје NOT капије у овим имплементацијама.

Због ограничења Fyne-а у виду подршке само за опадајуће листе са једноструким избором, уведена је и опција учитавања тела поруке из текстуалног фајла, како би се могле применити и сложеније политике приступа.

Приликом покретања сервера, повлаче се мастер кључеви за обе шеме из базе, уколико постоје, или се генеришу и чувају у бази, уколико не постоје. Сервер након пријаве корисника у одговору враћа FAME јавни кључ који се користи при енкрипцији порука.

Осетљиве податке корисника (плата и адреса становања) енкриптује сервер GPSW шемом приликом регистрације, користећи GPSW јавни кључ и атрибуте "email:ek",

"role:manager" и "department:dk". Значење оваквог вида шифровања је да ће корисник имати приступ сензитивним подацима ако:

1. припадају њему
2. је менаџер и гледа податке запосленог из истог одсека

За разлику од FAME шеме, GPSW не прихвата текстуалне атрибуте, те је потребно обезбедити недвосмислену и јединствену трансформацију из текстуалних у целобројне атрибуте. Приликом повлачења профила корисника политика дешифровања је "email:ek OR (role:rk AND department:dk)", где су ek, rk и dk ознаке за имејл, позицију и одсек корисника респективно. Кориснички кључ за декриптовање осетљивих информација се генерише на основу GPSW мастер тајног кључа који је учитан на серверу и конструисане политике приступа.

Енкриптовање порука реализује се применом FAME шеме на клијентској апликацији, и у овом случају нема фиксиране политике приступа, односно дефинише је корисник у интерфејсу клијентске апликације или у текстуалном фајлу. Енкрипција се врши посебно за сваки сегмент/параграф поруке користећи FAME јавни кључ, који је корисник добио од сервера након пријаве и који чува у меморији, и дефинисану политику приступа за одговарајући сегмент. Додатно енкриптује се и наслов поруке са политиком приступа дефинисаном тако да могу да га декриптују пошиљалац и сви примаоци поруке. Клијент затим шаље главу поруке (енкриптовани наслов, листу прималаца) на сервер, који је чува у бази и враћа њен ID у одговору. Енкриптовани сегменти порука се затим шаљу на сервер, један по један, са придруженим ID-јем поруке и бројем своје позиције у поруци како би порука могла накнадно да се реконструише. Сегменти без дефинисане политике приступа се енкриптују политиком приступа наслова поруке. Енкриптовани подаци се увек декриптују на серверу са тројком атрибута имејл, позиција и одсек ("email:ek", "role:manager" и "department:dk") који се извлаче из корисничке сесије, након чега се врши реконструкција поруке. Имплементација обезбеђује логовање на нивоу сваке од компоненти.

4.2.Коришћени алати и технологије у изради решења

- **Go програмски језик** - је статички јако типизиран, компајлирани програмски језик који је дизајниран да буде једноставан, ефикасан и робустан. Има уграђен скупљач ђубрета, уграђену подршку за конкурентно програмирање уз помоћ "горутина" (goroutines) и канала (channels). Синтактички је сличан C-у и има сличне перформансе. Долази са обимном стандардном библиотеком која покрива велики број области, од веб сервера до криптографије. Има највећу примену у имплементацији веб сервера, микросервиса, дистрибуираних система и DevOps алата.
- **Gin** – је познат као један од најбржих веб радних оквира[27] за Go, због своје ефикасне структуре и мале алокације меморије. Захваљујући једноставној и интуитивној API структури, Gin омогућава брз развој веб апликација. Има подршку за веб удице[28] кроз такозвани мидлвер, што корисницима омогућава лаку имплементацију функционалности као што су логовање, аутентификација и грешке. Омогућава лако дефинисање и руковање HTTP захтевима кроз различите путање и методе. Олакшава рад са JSON-ом, што га чини погодним за изградњу RESTful API-ja.
- **Fyne** - је модеран графички радни оквир за израду крос-платформских десктоп апликација у програмском језику Go. Омогућава развој апликација које се могу извршавати на различитим оперативним системима, укључујући Windows, macOS, Linux, iOS и Android. Дизајниран да буде интуитиван и једноставан за коришћење, са фокусом на брзом развоју графичких апликација.
- **Fentec project gofe библиотека** – је библиотека настала као део пројекта FENTEC[29]. Има имплементирано више различитих шема за функционалну енкрипцију, а и подржава 4 шеме енкрипције засноване на атрибутима: FAME (CP-ABE), GPSW (KP-ABE), DIPPE (енкрипција унутрашњих производа предиката) и MA-CP ABE.

---

[27] енг. *framework*

[28] енг. *webhooks*

[29] *Functional Encryption Technology*

- **PostgreSQL -** је релациони систем за управљање базама података (RDBMS) који користи SQL језик за упите. Он је отвореног кода и један је од најстаријих и најмоћнијих система за управљање базама података доступних данас. PostgreSQL нуди многе напредне функције које не налазимо у другим RDBMS системима, као што су материјализовани прикази, индекси на више колона и друго.
- **Bun ORM -** је модеран ORM[30] за Go програмски језик. Он пружа алате за интеракцију са релационим базама података, омогућавајући корисницима да моделирају, врше упите и мењају податке у бази без писања голог SQL кода. Развијен је са идејом да буде ефикасан, модуларан и лак за употребу.
- **Logrus** - је структурирани логер за Go, који пружа проширive и модуларне могућности за логовање. Он је дизајниран да буде компатибилан са стандардном библиотеком за логовање у Go-у, али додатно нуди богатији сет функционалности и форматера за напредну и подесиву обраду порука о логовању.
- **GoLand** - је интегрисано развојно окружење (IDE) од JetBrains-а специјално дизајнирано за програмски језик Go. Он комбинује интуитивни интерфејс са моћним сетом функционалности које обезбеђују ефикасан и продуктиван развој Go апликација. GoLand нуди код комплетирање, интелигентно преименовање, и рефакторизацију, помажући програмерима да пишу чист и исправан код.
- **DataGrip** - је интегрисано развојно окружење (IDE) за базе података које је креирао JetBrains. Намењен је професионалцима koji se баве базама података и пружа напредне алате за рад с бројним базама података.
- **Postman -** је популаран алат за тестирање и развој API-ја. Он омогућава развојним тимовима да креирају, тестирају, и документују API-је на једном месту, усмеравајући се на сарадњу и аутоматизацију.

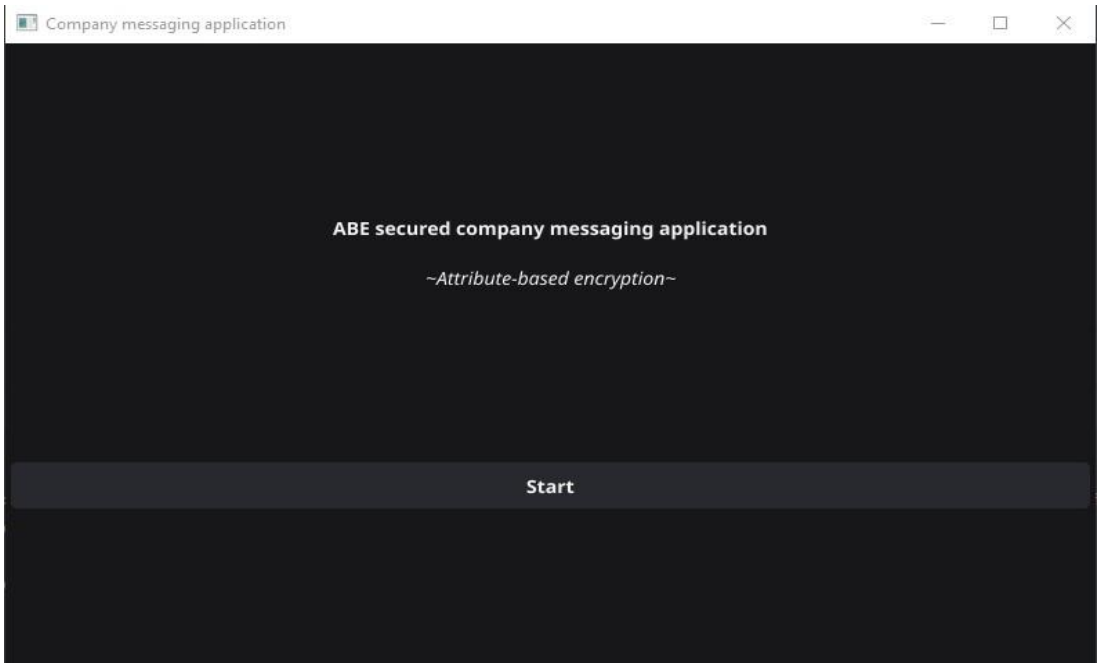
[30] *Object-Relational Mapping*

5. Опис система и његових функционалности

У наставку је дат преглед функционалности апликације и приказа у току коришћења, са детаљним објашњењем функционалности појединих компоненти.

5.1. Почетни екран

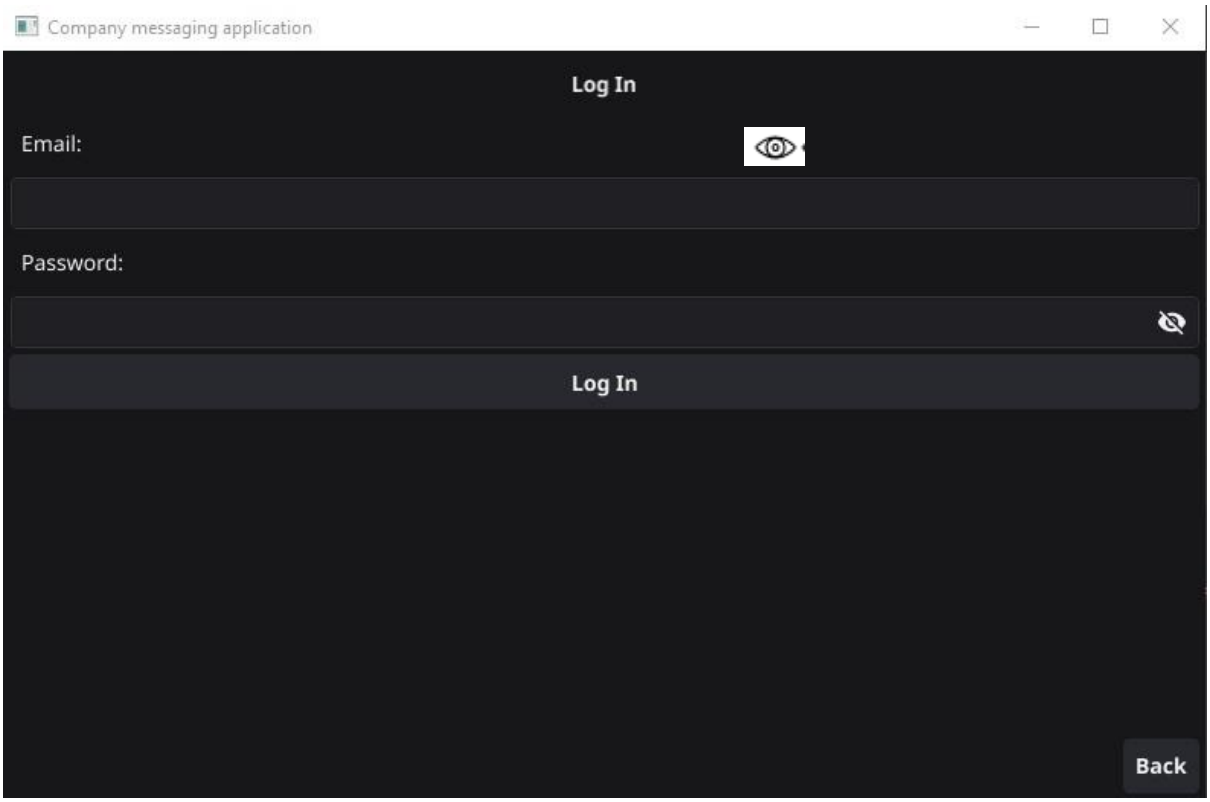
Запосленом се приликом покретања клијентске апликације приказује почетни екран. На њему се види назив апликације и дугме за отпочињање рада са апликацијом.



Слика 10 - Изглед почетног екрана апликације

Притиском на тастер *"Start"*, приказује се следећи екран (Екран за пријаву).

5.2.Екран за пријаву

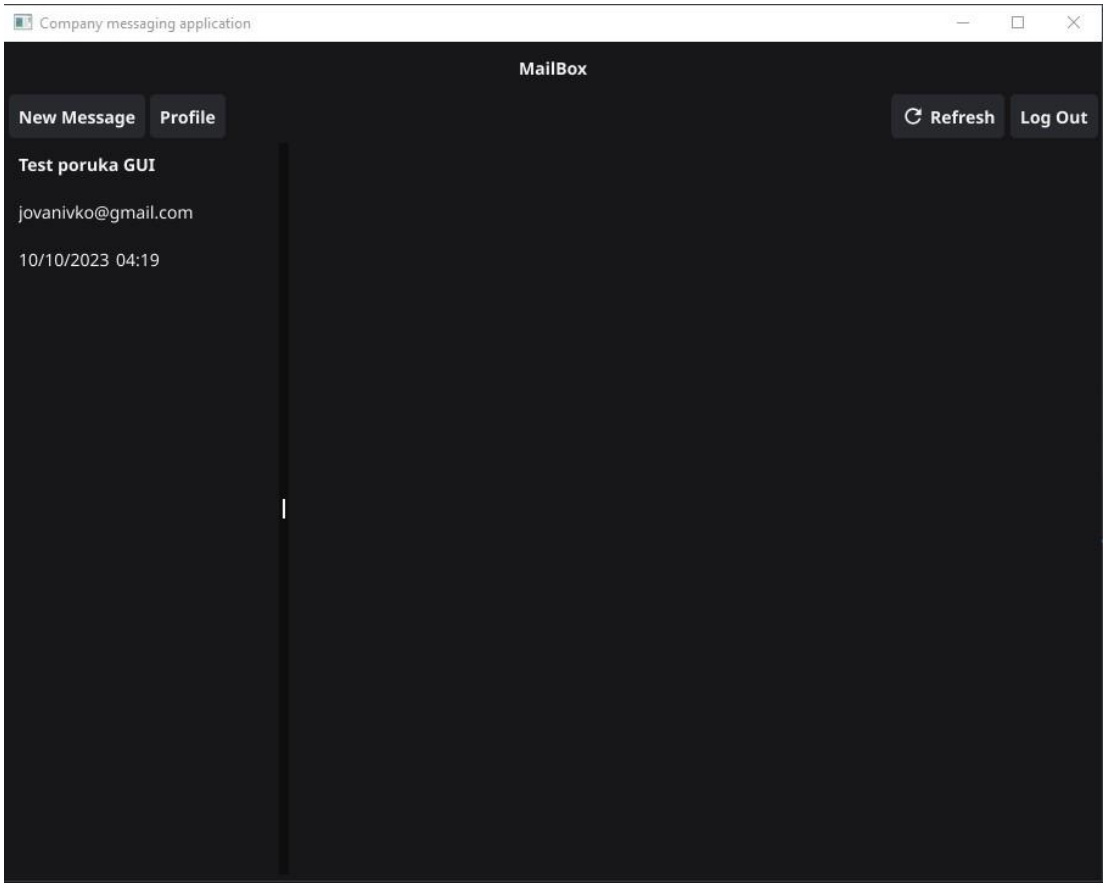


Слика 11 - Изглед екрана за пријаву

Неопходно је да се запослени аутентификује својим *e-mail* налогом и шифром и након тога притисне тастер *Log In* како би покренуо апликацију. Омогућена је провера укуцане лозинке притиском на иконицу где је нацртано око.

5.3. Сандуче за поруке

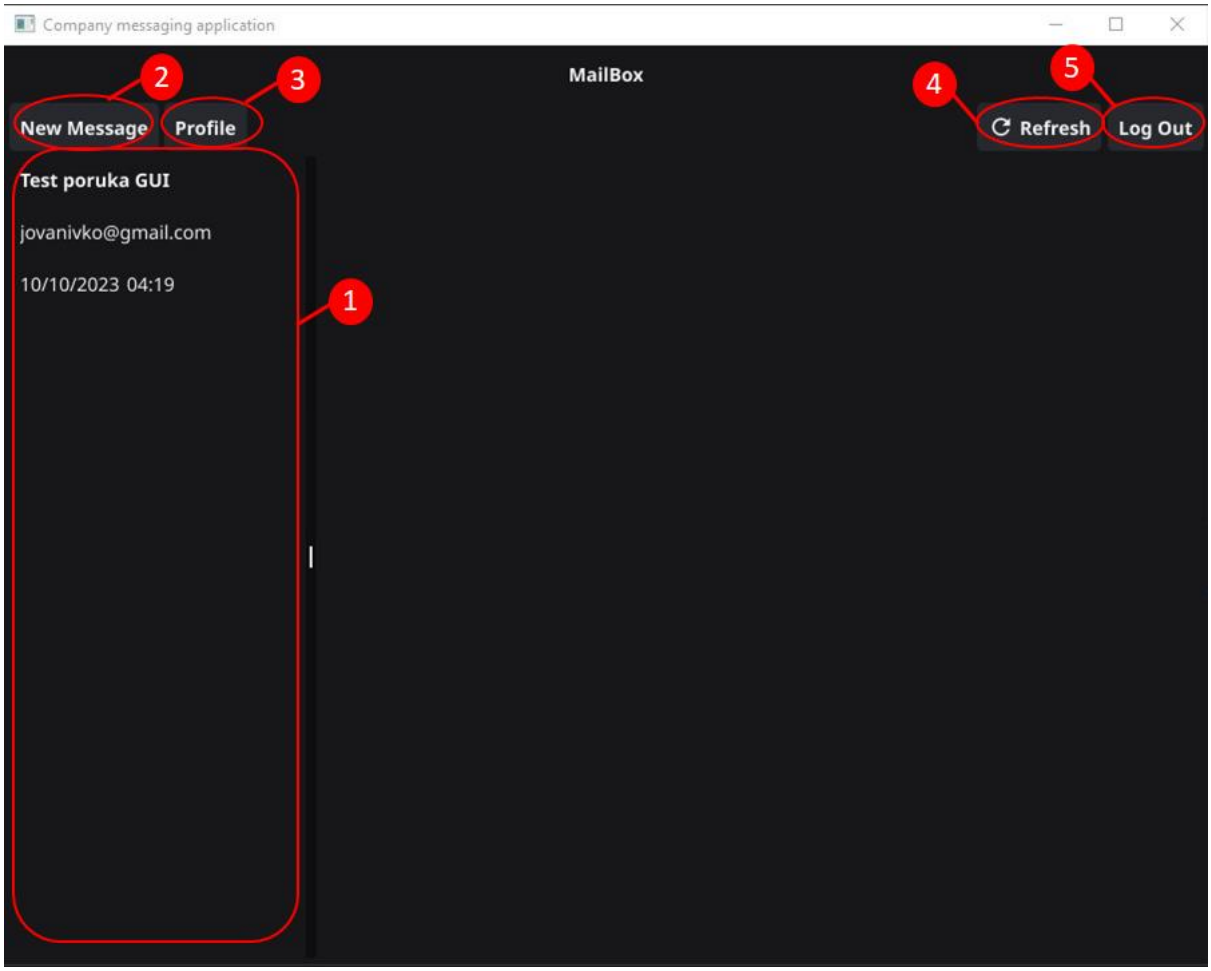
Након успешног логовања на апликацију, кориснику се приказује екран са свим пристиглим порукама. Јавни кључ за енкрипцију порука се чува у меморији апликације.



Слика 12 - Изглед сандучета за поруке

На слици број 14 је приказано значење области и тастера који су означени редним бројевима како је дато у наставку:

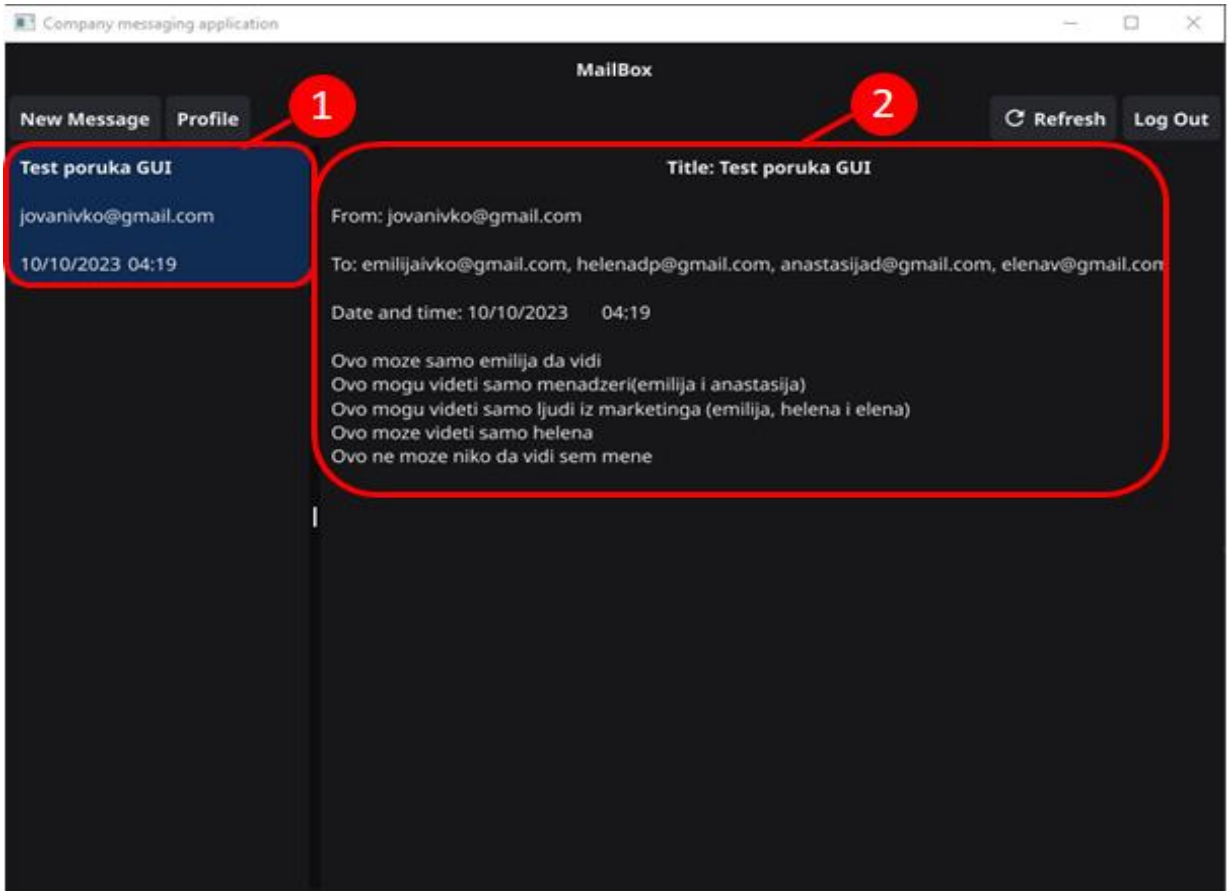
1. Заокружен је прозор у коме се врши приказ листе свих порука које је корисник примио или послао са следећим информацијама: наслов поруке, ко је пошиљалац мејла, датум и време када је порука стигла.
2. Тастер *New Message* чијим се избором отвара прозор за креирање нове поруке
3. Притиском на дугме *Profile* се отвара посебан прозор за преглед профила свих корисника
4. Дугме *Refresh* служи за ажурирање порука у сандучету
5. Дугме *Log Out* служи за одјаву са апликације



Слика 13 - Приказ прозора за сандуче порука

5.3.1. Приказ поруке

Кликом миша на одговарајућу поруку у листи порука (означено редним бројем 1), приказује се садржај поруке у празном простору који заузима већину екрана. Приказ садржи наслов поруке, мејл пошиљаоца, листу мејлова прималаца раздвојених знаком ;, датум и време када је порука настала, као и сам садржај поруке.



Слика 14 - Изглед приказа поруке

5.3.2. Прозор за слање порука

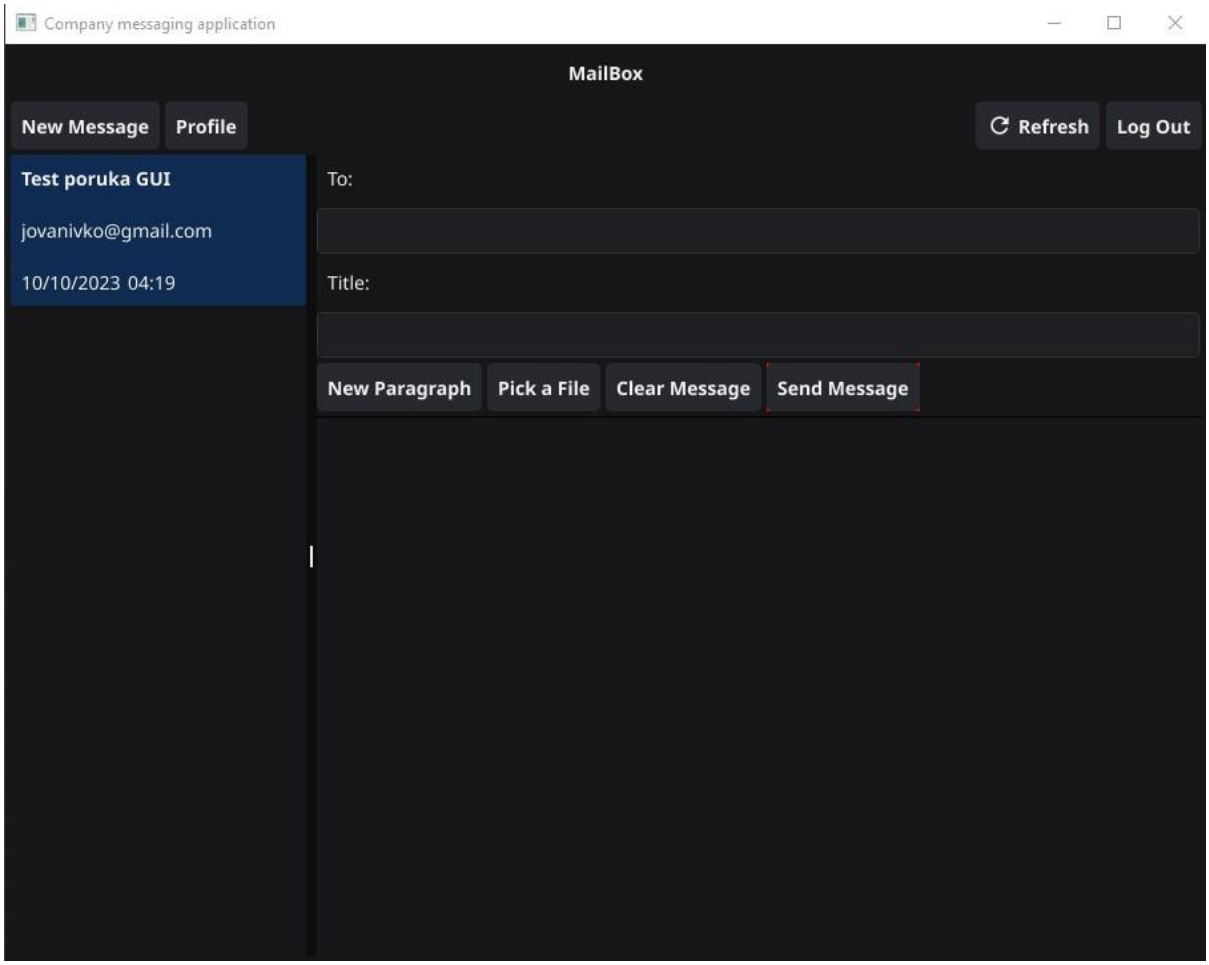
Избором тастера *"New message"* у десном делу прозора приказује се одељак за слање порука у коме су дата следећа поља:

1. *"To"* поље где се уписује мејл адреса примаоца поруке
2. *"Title"* поље где се уписује наслов мејла
3. *"New paragraph"* чијим избором се отвара форма за унос новог параграфа поруке и то на начин да се врши:

   а) избор ко од примаоца има могућност да види конкретан параграф

   б) које атрибуте који се налазе у његовом профилу треба да испуни прималац да би имао могућност да види конкретни параграф (пример: позиција у фирми на којој се налази)
4. *"Pick a file"* где се врши избор фајла који се додаје у прилог мејла
5. *"Clear message"* који служи да се сви параграфи уклоне у прозору уклоне

6. *"Send message"* чијим се избором шаље порука

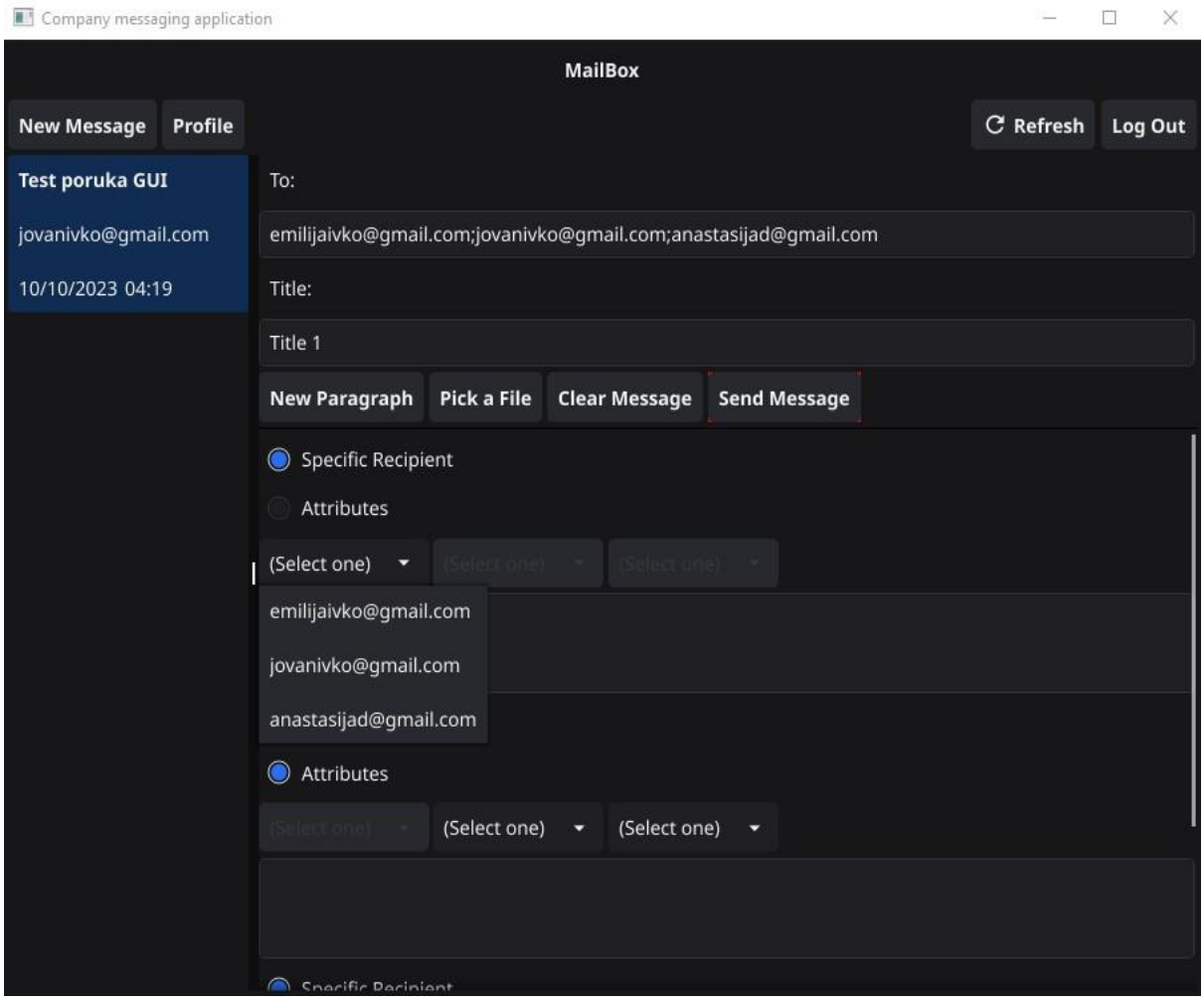


Слика 15 - Прозор за слање порука

Кликом на дугме *"New Paragraph"* прави се, и убацује на екран у листу, нова група графичких елемената која се састоји од два радио дугмета (*"Specific Recipients"* и *"Attributes"*), три опадајуће листе и једно поље за више-линијски текстуални унос.

Уколико је фајл одабран, слање поруке преко фајла узима предност над слањем поруке преко графичког корисничког интерфејса.

5.3.3. Слање порука кроз графички кориснички интерфејс

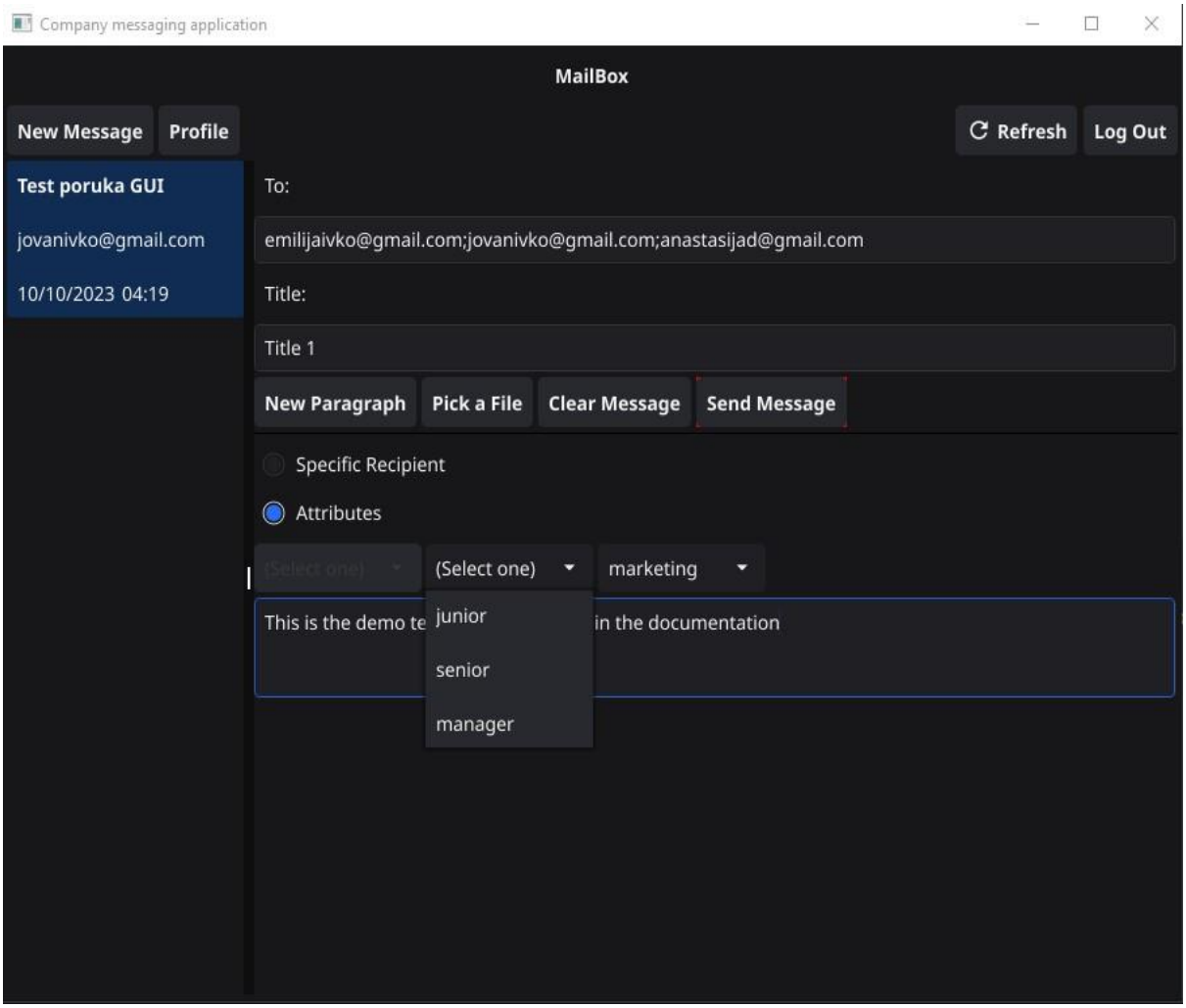


Слика 16 - Екран за избор корисника који виде одговорајући параграф

Уколико је у новом параграфу одабрана вредност радио дугмета *"Specific Recipients"* друге две опадајуће листе биће онемогућене, а прва ће узимати вредности имејлова из листе мејлова прималаца порука. Уношење новог, или избацивање већ постојећег имејла, из листе прималаца, ажурирају се вредности и у овој опадајућој листи.

Избор имејла из опадајуће листе значи да ће у послатој поруци, само корисник са датим имејлом, моћи да прочита дати параграф (осим пошиљаоца). Уколико се не изабере ниједна вредност из опадајуће листе, то значи да ће сви примаоци моћи да прочитају дати параграф.

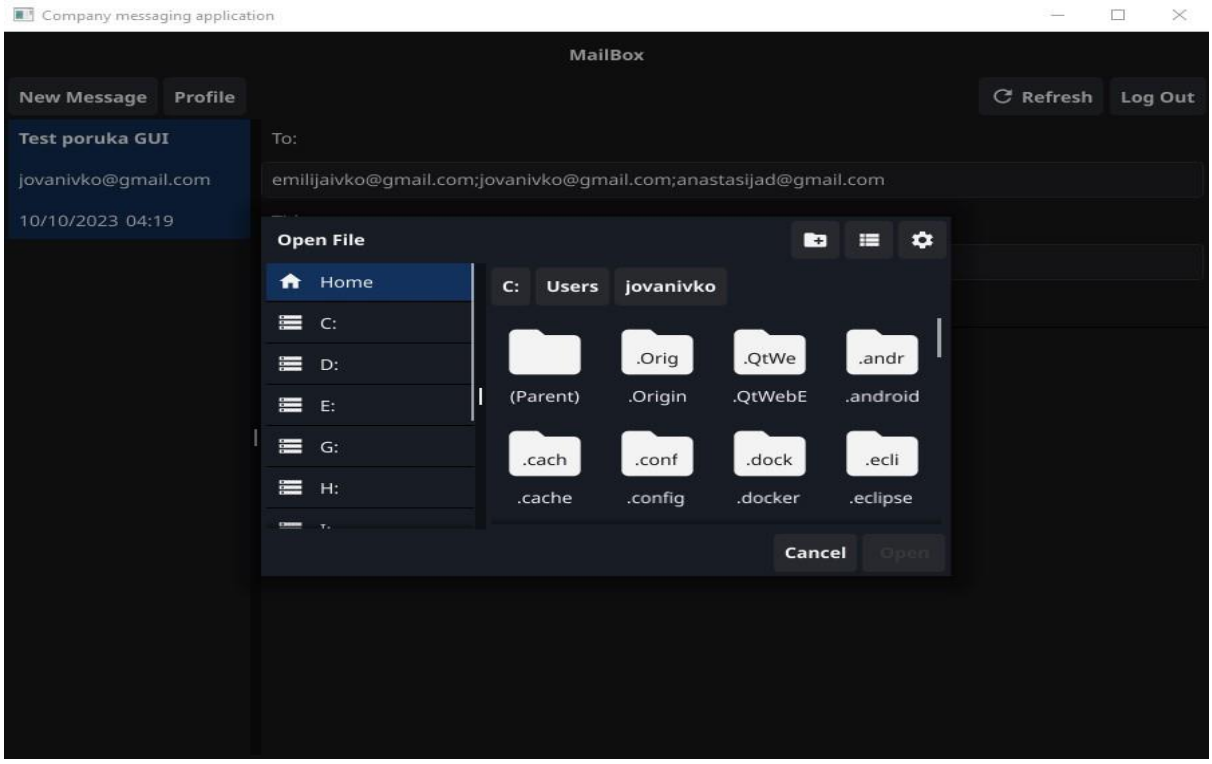
Уколико је изабрана вредност радио дугмета *"Attributes"*, прва опадајућа листа биће онемогућена, док ће друге две бити омогућене. Оне узимају вредности из могућих скупова вредности за позицију и одсек респективно.



Слика 17 - Прозор за избор атрибута које мора да испуњава пошиљалац да би примио поруку

Уколико се изабере вредност за једну, односно обе, опадајуће листе, то знаћи да ће дати параграф моћи да прочитају само они примаоци који имају тај један, односно оба, атрибута. Уколико није селектована ниједна вредност ни у једној листи, то значи да ће дати параграф моћи да прочитају сви примаоци.

5.3.4. Слање порука учитавањем фајла



Кликом на дугме *"Pick a File"* отвара се прозор приказан на слици. Навигацијом по фајл систему и избором одговарајућег .txt фајла, и кликом на дугме *Open*, учитава се путања до фајла. Фајл мора бити у формату:

Слика 18 – Прозор за избор фајла

/** услов1**/

садржај1

/** услов2 **/

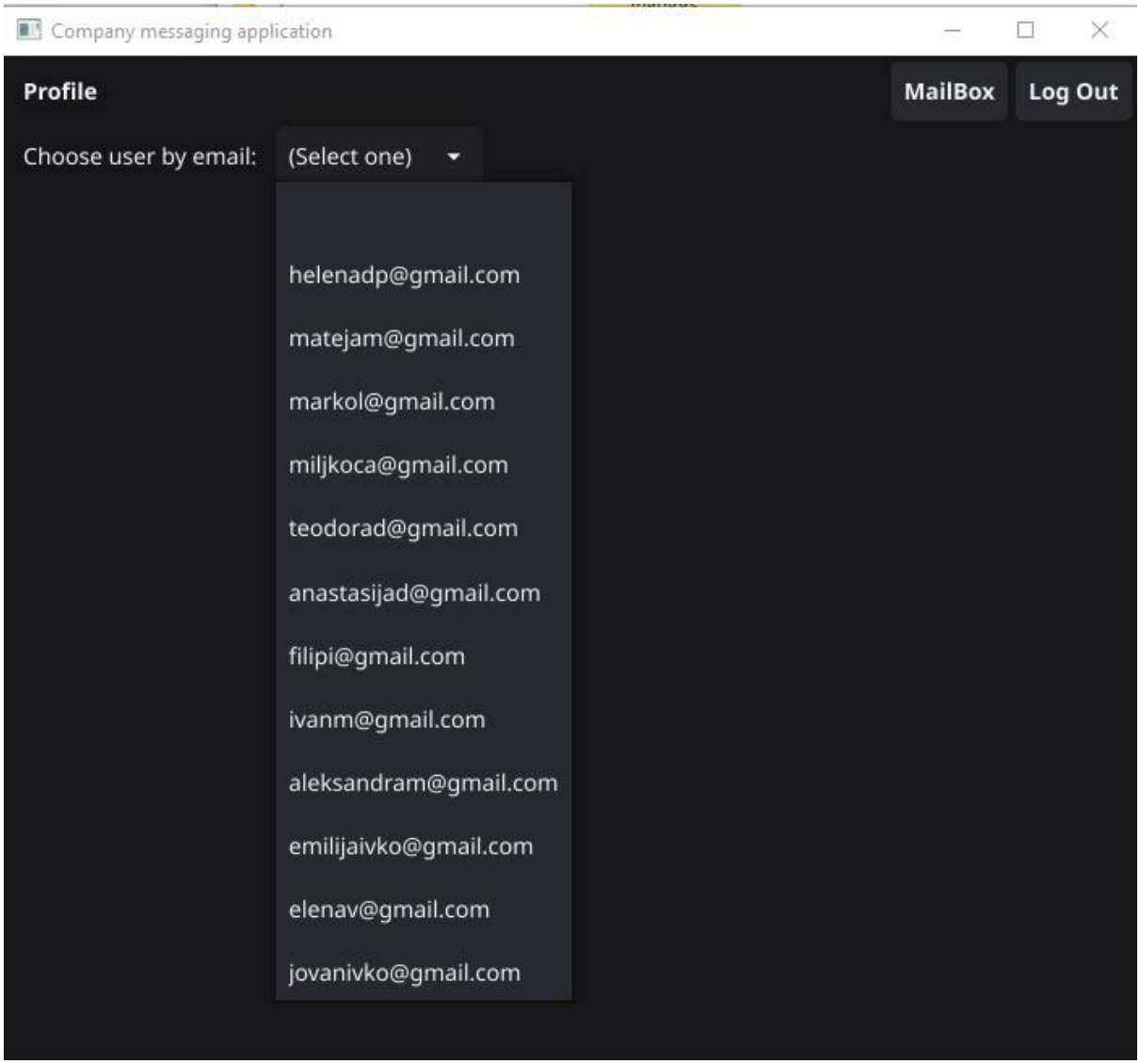
садржај2

итд.

Слање поруке, примењује дати услов на њему присвојен садржај. Слање поруке се одвија на исти начин. Остављање празног услова значи да ће одговарајући садржај видети сви примаоци.

5.4. Приказ профила

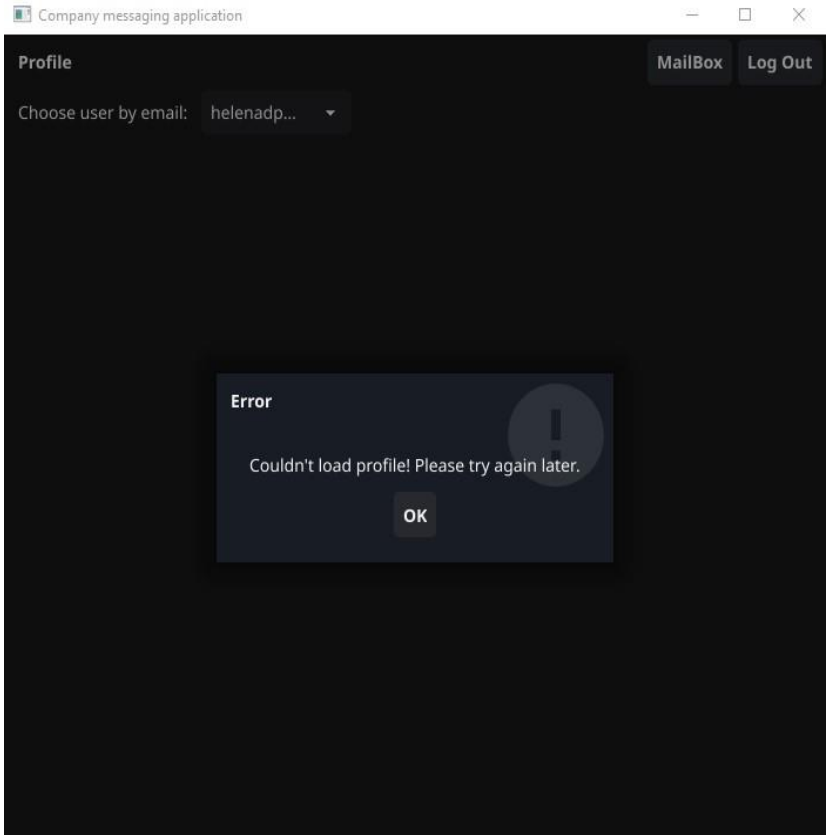
На страници *Profile* најпре се врши избор корисника чији профил треба приказати. Избор се врши одабиром мејл адресе из опадајуће листе свих мејлова корисника, како је приказано на следећој слици.



Слика 19 – Опадајућа листа избора имејла корисника

Након тога, приказује се екран са приказом карактеристика профила, а то су: име, презиме, позиција запосленог, одсек у ком ради, број телефона, адреса пребивалишта и уговорена зарада. Зарада и адреса ће се приказати само корисницима који имају право да их виде а према спецификацији решења.

Слика 20 – Приказ информација о кориснику



Слика 21 – Изглед прозора упозорења у случају необрађене грешке

6. Закључак

На основу демонстрације концепта ABE и прегледа његових карактеристика, можемо закључити да је у одговарајућим ситуацијама систем енкрипције врло ефикасан и поуздан.

ABE нуди елегантан, и по корисника, транспарентан начин контроле приступа садржају као и његове дистрибуције, уз заштиту самог садржаја. Видели смо да се ABE може користити и са другим врстама енкрипције како би комплементирале једна другу.

Главна препрека за широку примену овог система енкрипције је што је он још релативно неразвијен и неутврђен. Нове имплементације се још увек конструишу, а постоји и опасност да ће неке његове верзије могле постати несигурне са увођењем квантних рачунара.

На крају можемо приметити да је узрок скепсе у употреби ове енкрипције на системима великих размера, за које је и створен, управо мањак стандардизације у координисању, депоновању и повлачењу кључева, као и у непостојању развијених и тестираних механизама доделе атрибута и система њиховог именовања. Уколико се ови проблеми отклоне и ABE добије стандардизацију може се предвидети да ће доживети велику експанзију примена и употребе.

Референце

[1] Statista, „Internet of Things (IoT) and non-IoT active device connections worldwide,“ 2023. [На мрежи]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

[2] Microsoftcorp, „What is Access Control?,“ [На мрежи]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-access-control.

[3] NTT Research, „Attribute-based Encryption,“ NTTResearch, 2021. [На мрежи]. Available: https://ntt-research.com/ntt-research-cis-cryptography-attribute-based-encryption/.

[4] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li и D. Zheng, „Attribute-based Encryption for Cloud Computing Access Control: A Survey,“ Assosiation for Computing Machinery, 3 8 2020. [На мрежи]. Available: https://dl.acm.org/doi/10.1145/3398036.

[5] YanMichalevsky, M. Joye, A. S. a. S. University(USA) и 2NXPSemiconductors(USA), „Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy,“ 2018. [На мрежи]. Available: https://eprint.iacr.org/2018/753.pdf.

[6] Y. Liu, Y. Pan, L. Gu, Y. Zhang и D. An, „Attribute-Based Fully Homomorphic Encryption Scheme from Lattices with Short Ciphertext,“ Hindawi, 2021. [На мрежи]. Available: https://www.hindawi.com/journals/mpe/2021/6656764/.

[7] M. Chase, „Multi-authority Attribute Based Encryption,“ [На мрежи]. Available: https://link.springer.com/chapter/10.1007/978-3-540-70936-7_28.

[8] D. Boneh, AmitSahai и BrentWaters, „Functional Encryption: Definitions and Challenges,“ 2010. [На мрежи]. Available: https://eprint.iacr.org/2010/543.pdf.

[9] T. Bouabana-Tebibel и A. Kaci, „Parallel search over encrypted data under attribute based encryption on the Cloud Computing,“ 8 12 2015. [На мрежи]. Available:

https://www.sciencedirect.com/science/article/abs/pii/S0167404815000577?via%3Dihub#preview-section-cited-by.

[10] „MA-ABE access control system model.," ResearchGate, [На мрежи]. Available: https://www.researchgate.net/figure/MA-ABE-access-control-system-model_fig1_359925402.

[11] „Identity-based encryption," wikipedia, [На мрежи]. Available: https://en.wikipedia.org/wiki/Identity-based_encryption .

[12] ReseacrhGate, [На мрежи]. Available: https://www.researchgate.net/figure/Interaction-scenario-in-Homomorphic-Encryption_fig1_370392930.

[13] ResearchGate, 2018. [На мрежи]. Available: https://www.researchgate.net/figure/Scenario-of-Functional-Encryption_fig1_325982256 .