БУЛУТЛИ ҲИСОБЛАШ ТИЗИМЛАРИДА ФОЙДАЛАНУВЧИЛАРНИ АУТЕНТИФИКАЦИЯЛАШ УСУЛЛАРИ ВА АЛГОРИТМЛАРИ

Раджабова Мадина Шавкатовна
Тошкент ахборот технологиялари университетининг
“Киберхавфсизлик ва криминалистика” кафедраси ўқитувчи-стажёр

Хафизов Шукурулло Файзулло ўғли,
Қурбонмуродов Диёрбек Улуғбек ўғли
Киберхавфсизлик факултети талабалари

Аннотация: Ушбу мақола мақсади булутли ҳисоблаш тизимларида, эллиптик эгри чизиққа, биргина фойдаланишли аутентификация тизими учун ишлаб чиқилган усуллар ва алгоритмлардан олинган реал ҳамда тажрибавий таҳлиллар билан изоҳланади.

Мақола натижаларининг илмий аҳамияти булутли ҳисоблаш тизимларида, эллиптик эгри чизиққа, биргина фойдаланишли аутентификация тизими учун усул ва алгоритмларни ишлаб чиқиш ва такомиллаштириш билан изоҳланади.

Булутли ҳисоблаш тизимларида фойдаланувчиларни ҳақиқийлигини тасдиқлашга қаратилган таҳдидларни камайтириш ва кўп сонли қайд ёзувлар учун аутентификация жараёнини ягона парол асосида амалга ошириш имконияти билан изоҳланади.

Калит сўзлар: эллиптик эгри чизиқ, скаляр қиймат, паролни алмаштириш.

КИРИШ

Ўзбекистон Республикаси Президентининг Фармони, 28.01.2022 йилдаги ПФ-60-сон фармонига асосан 2022 — 2026 йилларга мўлжалланган янги Ўзбекистоннинг тараққиёт стратегиясида Давлат дастурини амалга ошириш якунларига бағишланган ахборот-таҳлилий шарҳларни тайёрлаш, уларни хорижий тилларда эълон қилиш ва кенг тарқатишни таъминланиши, Ахборот ва оммавий коммуникациялар агентлиги, Ўзбекистон Миллий телерадиокомпанияси ва Ўзбекистон Миллий ахборот агентлиги оммавий ахборот воситалари билан биргаликда мунтазам равишда тараққиёт стратегияси ва Давлат дастурининг мақсад ва вазифаларини оммавий ахборот воситаларида, шу жумладан Интернет жаҳон ахборот тармоғида ва ижтимоий тармоқларда кенг

шарҳлаб борилишини ҳамда унинг мазмун-моҳияти жамоатчиликка тушунтирилишини кўзда тутилмоқда.

Жаҳонда булутли ҳисоблаш тизимларидан фойдаланиш ҳажмининг кескин суръатлар билан ортиши, булутли тизимлар билан боғлиқ хавфсизлик муаммоларини олдинги олиб чиқади. Бу булутли тизимларнинг заифлиги, нафақат фойдаланувчиларнинг шахсий маълумотларининг, балки, муҳим коорпоратив сирлар ва мулкка оид маълумотларининг ҳам ошкор қилиниши билан изоҳланади. Хусусан, Statista компаниясида “2019-2022 йилларда ташкилотнинг булутли ҳисоблаш тизимидаги муаммолар рўйхатида 85% кўрсаткич билан хавфсизлик муаммоси етакчилик қилган”[1]. Булутли ҳисоблаш тизимларида маълумотлар ва ресурслардан рухсатсиз фойдаланишни олдини олишда аутентификация усулларининг ўрни муҳим. Булутли тизимларни татбиқ этиш, булутли ҳисоблаш тизимларида маълумотларни ҳимоялаш, фойдаланувчиларни кафолатли аутентификациялаш усулларини ишлаб чиқиш соҳасига АҚШ, Япония, Германия, Жанубий Корея, Ҳиндистон ва бошқа ривожланган давлатларда катта эътибор қаратилмоқда.

Адлия вазирлиги ва Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги 2022 йил 1 октябрга қадар давлат хизматлари тизимини халққа янада яқинлаштириш, навбатларни қисқартириш, давлат хизматларини рақамлаштириш ва хусусий секторга ўтказиш чораларини назарда тутувчи қарор лойиҳасини Вазирлар Маҳкамасига киритиш жора таъдбирларини кўрилган.

Булутли ҳисоблаш тизимларида аутентификация одатда бирор нарсани билишга асосланган усуллардан (масалан, паролга асосланган) кенг фойдаланилади. Бироқ, бирор нарсани доимо эсда сақлашнинг мураккаблиги ва алдаб ўтишнинг кўплаб усулларининг мавжудлиги, амалда бошқа хавфсиз аутентификация усулларидан фойдаланишни тақазо этади. Шу сабабли, мазкур бобда булутли тизимларда ISO/IEC 29115:2013 стандартига мос, эллиптик эгри чизиқларга асосланган аутентификация усули ишлаб чиқилган.

ЭЛЛИПТИК ЭГРИ ЧИЗИҚЛАР ВА УЛАРНИ АУТЕНТИФИКАЦИЯДА ҚЎЛЛАНИЛИШИ

Очиқ калитли криптографик алгоритмлар амалда фойдаланувчиларни аутентификациялаш, хабар яхлитлиги таъминлаш ва DDoS хужумларидан ҳимоялаш учун қўлланилади. Очиқ калитли криптографик алгоритмлар орасида эллиптик эгри чизиққа (Elliptic curve cryptography, ECC) асосланганлари

[1] https://www.statista.com/statistics/511283/worldwide-survey-cloud-computing-risks/

бардошлигини йўқотмасдан юқори ҳисоблаш самарадорлигига эгалиги билан ажралиб туради [158]. Чекли Z_q $(q > 2^{160})$ майдонда $E_q(a,b)$ эллиптик эгри чизиқ тенгламаси $y^2 mod q = x^3 + ax + b(mod q)$ билан ифодаланиб, бу ерда q – катта туб сон ва a ва b лар икки ўзгармас $(a,b \in Z_q)$ бўлиб, $4a^3 + 27b^2 \neq 0$ шартни қаноатлантириши шарт. Агар P эллиптик эгри чизиқдаги n $(n > 2^{160})$ тартибга эга асос нуқта ва $\emptyset$ - чексизликдаги нуқта бўлса, у ҳолда $n \times P = \emptyset$ шарт ўринли. Бу ерда, P – ЕССдаги нуқта бўлиб, (x,y) координата қийматлари билан характерланади. × - нуқтани скалярга кўпайтириш амали бўлиб, чекли майдонда нуқталарни кўпайтиришни англатади ва маъно жихатдан P нуқтани n марта қўшишга тенг[2]: $n \times P = \overbrace{P + P + \ldots + P}^{n \text{ марта}}$.

Теорема. Фараз қилинсин $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ нуқталар $E_q(a,b)$ эллиптик эгри чизиқда ётсин. У ҳолда $E_q(a,b)$ эллиптик эгри чизиқда ётувчи $P_3 = P_1 + P_2 = (x_3, y_3)$ нуқта қуйидагича ҳисобланади [4]:

$$P_1 + P_2 = \begin{cases} O_\infty \text{ агар } x_1 = x_2 \& y_1 = -y_2 \\ (x_3, y_3) \text{ бошқа ҳолларда} \end{cases}$$

бу ерда,

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

ва

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} \text{ агар } P_1 = P_2 \\ \dfrac{y_2 - y_1}{x_2 - x_1} \text{ бошқа ҳолларда} \end{cases}$$

ЕСС нуқтасини скалярга кўпайтириш амали муҳим аҳамиятга эга , уни ҳисоблаш учун бир қанча усуллардан фойдаланилади. Бироқ, скаляр қийматнинг ортиши натижасида, ҳисоблаш вақти ҳам ортади. Шу сабабли, нуқтани скалярга кўпайтиришда кам вақт талаб қилувчи усуллардан фойдаланиш тавсия этилади. Булар орасида скалярни қўшни бўлмаган бирлардан иборат бўлган бинар шаклда ёзишга (Non-Adjacent Form, NAF) асосланган усул қўйилган талабга жавоб беради.

1- алгоритм *Скаляр k учун NAFни ҳисоблаш.*

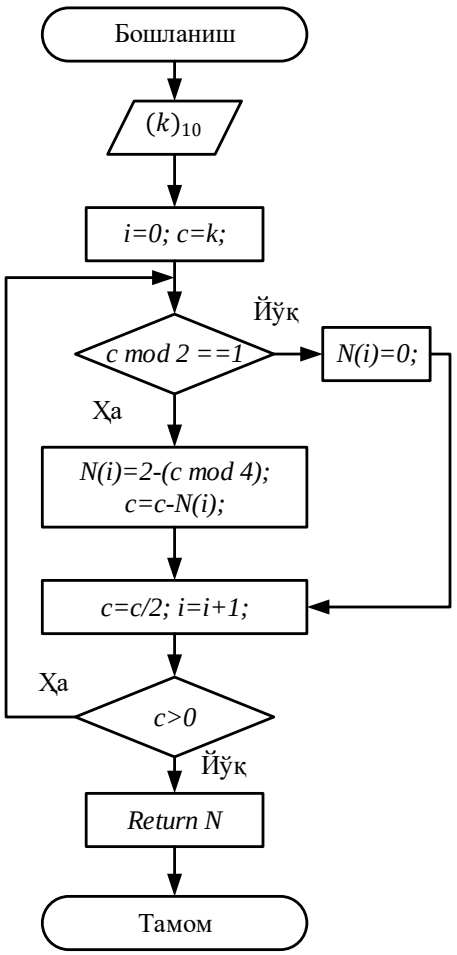
Кириш: скаляр қиймат $(k)_{10}$

Чиқиш: $N = (k_{l-1}, \ldots, k_1, k_0)_{NAF(k)}$

```
i=0; c=k;
while (c>0)
    if(c mod 2 ==1)
        N(i)=2-(c mod 4);
```

c=c-N(i);
else
N(i)=0;
End if
c=c/2; i=i+1;
End while
Return N;

Бу ерда, i қиймат k бутун сонини NAF шаклида ёзиш натижасидаги кетма-кетликнинг узунлиги, одатда k бутун соннинг бинар қийматига тенг ёки ундан битга ортиқ. масалан $(k)_{10} = 27$ учун $NAF(27) = 100\bar{1}0\bar{1}$ $(\bar{1} = -1)$. Ушбу алгортмнинг блок схемаси 2.1-расмда келтирилган.



1-расм. Сколяр К учун NAFни ҳисоблаш алгоритмининг блок - схемаси

2 - алгоритм *NAF асосида нуқтани скалярга кўпайтириш.*

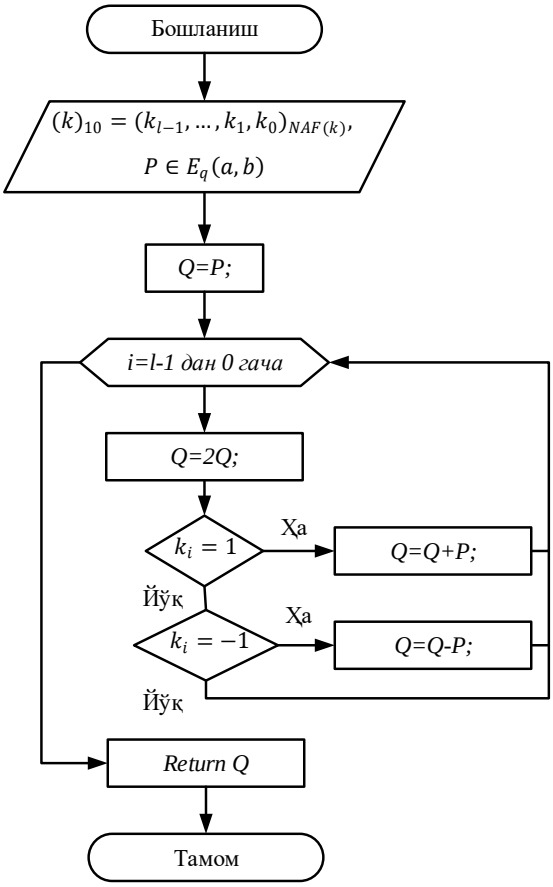
Кириш: $(k)_{10} = (k_{l-1}, \dots, k_1, k_0)_{NAF(k)}, P \in E_q(a, b)$.

Чиқиш: $Q = kP$.

Q=P;
For i=l-1 дан 0 гача
Q=2Q;

If($k_i = 1$) *then Q=Q+P;*
If($k_i = -1$) *then Q=Q-P;*
Return Q;

Нуқтани скалярга кўпайтириш алгоритмининг блок - схемаси 2 – расмда келтирилган.



2-расм. Нуқтани скалярга кўпайтириш алгоритмининг блок - схемаси

Қуйида ECC га асосланган фойдаланувчиларни аутентификациялаш протоколларининг таҳлили келтирилган.

Таъриф. *Эллиптик эгри чизиқда дискрет логарифм муаммоси ((ECDLP: Elliptic Curve Discrete Logarithm Problem):* берилган $P, Q \in E_g$ нуқталар учун $Q = m \times P$ тенгликдан $m \in [1, n-1]$ бутун сонни топиш мураккаб [3].

Юқоридаги таърифдан, $Q = m \times P$ тенгликдан Q, P берилган ҳолда m ни топиш мураккаб ҳисоблашларни талаб қилиши, яъни исботланган бардошликка эгалигини кўриш мумкин. Мазкур бардошлик асосида кўплаб электрон рақамли имзо алгоритмлари яратилган ва амалда кенг қўлланилмоқда. Бундан ташқари, эллиптик эгри чизиқдаги дискрет логарифмлашда m скалярнинг узунлиги хэш қиймат узунлигига тенг бўлса, уларнинг бардошлиги ҳам тенг бўлади. Бу эса эллиптик эгри чизиқда дискрет логарифм муаммосини хеш функциялардан

фойдаланилган аутентификация тизимларида ҳам қўллаш мумкинлигини кўрсатади.

ECC асосида аутентификациялаш усуллари, кичик калит узунлигида ҳам юқори бардошликни таъминлаши сабабли, булутли ҳисоблаш тизимларидаги турли ҳисоблаш имкониятига эга воситалар учун ҳам мос ҳисобланади. Хусусан, С.К.Ҳафизул, Ж.Янг, Е.Ж.Юн, Й.П.Лиао, Р.Питерс, С.Р.Мусави, Д.Аббасинезҳад-Муд ва бошқалар томонидан турли тизимлар учун EEC асосидаги аутентификация усуллари ва схемалари таклиф этилган. 1-жадвалда мазкур соҳага оид сўнги йилларда таклиф этилган EEC асосидаги аутентификация усулларининг таҳлили келтирилган.

1-жадвал

EEC асосидаги аутентификация усулларининг таҳлили

Муаллиф	Аутентификация схемаси	Афзаллиги	Камчилиги
1	2	3	4
С.К.Ҳафизул ва бошқалар.	Мобил қурилмалар учун икки томонлама аутентификация ва калитларни алмашиниш	-вақтни синхронлаш муаммоси йўқ; -мукаммал хавфсизлик ва икки томонлама аутентификациялаш; -такрорлаш, обрўсизлантириш ҳужумларига бардошли;	-юқори ҳисоблаш имкониятини талаб қилади
Ю.П.Лиао ва бошқалар.	RFID асосидаги аутентификация схемаси	-такрорлаш ва кўплаб қурилмалар орқали кириш ҳужумига бардошли; -мукаммал хавфсизликни таъминлайди;	-икки томонлама аутентификациялаш имконияти мавжуд эмас.
С.Калра ва бошқалар.	IOT ва булутли серверлар учун аутентификация схемаси	-такрорлаш ҳужумига бардошли;	-икки томонлама аутентификацияни мавжуд эмас; -қурилма анонимлигини таъминланмайди;
С.Чанг ва бошқалар.	IOT ва булутли серверлар учун аутентификация схемаси	-такрорлаш ҳужумига бардошли; -мукаммал хавфсизликни таъминлайди; -икки томонлама аутентификациялаш имконияти;	-паролни фараз қилиш, обрўсизлантирилиши, кўплаб қурилмалар орқали кириш ҳужумига бардошсиз; -қурилма анонимлигини таъминланмаслиги;

1	2	3	4
K.Wang ва бошқалар.	IOT учун аутентификация схемаси	-такрорлаш ҳужумига бардошли; -мукаммал хавфсизликни таъминлайди; -икки томонлама аутентификациялаш имконияти;	- обрўсизлантириш, кўплаб қурилмалар орқали кириш ҳужумига бардошсиз;
С.Кумари ва бошқалар.	IOT ва булутли серверлар учун аутентификация схемаси	-такрорлаш, паролни фараз қилиш ва ички ҳужумларга бардошли; -икки томонлама аутентификация ва мукаммал хавфсизликни таъминлайди; -қурилма махфийлигига эришилади.	- обрўсизлантириш, кўплаб қурилмалар орқали кириш ҳужумига бардошсиз;
С.Бҳубанешвари ва бошқлар.	Булутли ҳисоблаш тизимлари учун аутентификация схемаси	-такрорлаш, паролни фараз қилиш ва ички ҳужумларга бардошли; -қурилма махфийлигига эришган.	-икки томонлама аутентификацияни таъминламайди; -обрўсизлантириш, кўплаб қурилмалар орқали кириш ҳужумига бардошсиз; -мукаммал хавфсизликни таъминламайди.

Бошқа аутентификация протоколлари каби ECCга асосланган протоколларни баҳолашда қатор омилларни инобатга олиш талаб этилади. Хусусан, протокол турли хавфсизлик талабларига жавоб бериши, ҳисоблашлардаги, тармоқдаги юклама, сақлашдаги юкламалар ва ҳисоблаш вақти каби омиллар асосида баҳоланади. Бундан ташқари, расмий хавфсизликни тасдиқлашнинг автоматлаштирилган воситаларидан (масалан, AVISPA, Scyther) кенг фойдаланилади.

БУЛУТЛИ ҲИСОБЛАШ ТИЗИМЛАРИДА ЭЛЛИПТИК ЭГРИ ЧИЗИҚҚА АСОСЛАНГАН ФОЙДАЛАНУВЧИЛАРНИ АУТЕНТИФИКАЦИЯЛАШ УСУЛИ

Қуйида эллиптик эгри чизиққа асосланган аутентификация усули таклиф этилади.

Белгилашлар:

CC_i –булутли ҳисоблаш тизими мижози (Cloud Client);

CS – булутли ҳисоблаш тизими сервери (Cloud Server);

ID_i – мижоз идентификатори;

PW_i – фойдаланувчи пароли;

PV_i- парол тасдиғи (password verifier);

P – эллиптик эгри чизиқдаги нуқта;

Ушбу протокол рўйхатдан ўтиш, аутентификациядан ўтиш ва паролни алмаштириш босқичларидан иборат.

Рўйхатдан ўтиш босқичи

1-қадам. $(MCC_i \rightarrow CS): ID_i, PV_i$

Булутли хизмат серверидан рўйхатдан ўтишни истаган мижоз CC_i тизим ичида ноёб идентификатор ID_iни танлайди. Шундан сўнг, мижоз учун PW_i бардошли парол ҳосил қилинади ва бу паролнинг тасдиқловчиси (Password Verifier) $PV_i = P \cdot PW_i = (PV_x, PV_y)$ ҳисобланади. $\{ID_i, PV_i\}$ жуфтлиги CS булут серверига хавфсиз алоқа канали орқали юборилади.

2-қадам. $(CS \rightarrow MCC_i): CK'$

Булут сервери CS дастлабки $\{ID_i, PV_i\}$ маълумотларни қабул қилади ва сақлайди.

Тасодифий қиймат R_S ва у асосида мижоз куки қиймати CK ҳосил қилинади: $CK = H(R_S||K_{CS}||E_T||ID_i)$. Бундан ташқари қуйидагиларни ҳам ҳисоблайди:

- $CK' = CK \times P;$
- $T_i = R_S \oplus H(K_{CS});$
- $A_i = H(R_S \oplus H(K_{CS}) \oplus H(CK'));$
- $A_i' = A_i \times P;$
- $ET_i = T_i \oplus K_{CS};\ EA_i' = A_i' \oplus R_S;\ EE_T = E_T \oplus R_S.$

Ҳисобланган ET_i, EA_i' ва EE_T параметрлар ID_i параметрга боғланган ҳолда сақланади (3.2-жадвал). Шундан сўнг, хавфсиз канал орқали CK' параметри CC_i га юборилади.

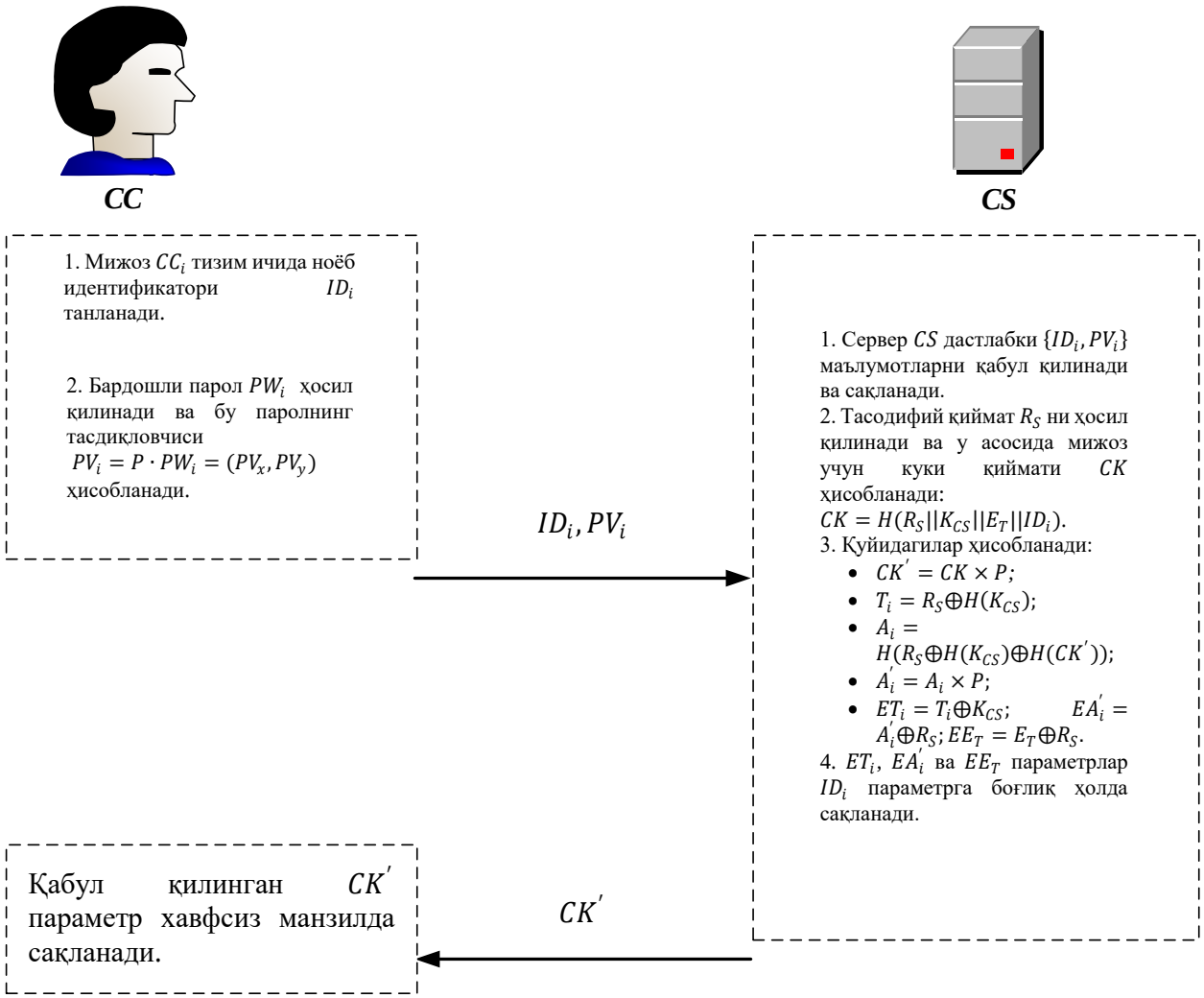
2 - жадвалда ҳолат бити устунида келтирилган қийматлар фойдаланувчини серверга боғлангани ёки боғланмаганлигини кўрсатади. Яъни, агар мижоз CC_i сервер CS га уланган бўлса холат 1 қийматга, акс ҳолда, 0 қийматга тенг бўлади.

2-жадвал

Сервер CS томонида мижоз CC_i маълумотларининг сақланиши

№	Мижоз идентификатори	Парол тасдиғи	Ҳолат бити	Хавфсизлик параметрлари
1.	ID_1	$PV_1 = P \cdot PW_1$	0/1	ET_1, EA_1' ва EE_T
2.	ID_2	$PV_2 = P \cdot PW_2$	0/1	ET_2, EA_2' ва EE_T
3.	ID_3	$PV_3 = P \cdot PW_3$	0/1	ET_3, EA_3' ва EE_T
-	-	-	-	-

3-қадам. Мижоз CC_i қабул қилинган CK' параметрни хавфсиз манзилда сақлайди (3.3-расм).



3-расм. Протоколнинг рўйхатдан ўтиш босқичи

Изоҳ. ISO/IEC 29115:2013 стандартининг 4 даражасига мос келувчи, юқори хавфсизлик талаби қўйилганида CK' параметр смарт карталарда сақланади. Бошқа ҳолларда фойдаланувчи мобил қурилмасида ёки веб браузерлар куки сақлагичларида ҳам сақланиши мумкин.

Аутентификациядан ўтиш босқичи

1-қадам. $(CC_i \rightarrow CS)$: P_1, P_2, ID_i.

Мижоз CC_i дастлаб R_1 тасодифий сонни генерациялайди ва P_1, P_2 қийматлари қуйидагича ҳосил қилинади:

$P_1 = R_1 \times PW_i \times P$;

$P_2 = H(R_1 \times PW_i \times CK')$.

Шундан сўнг, P_1, P_2 ва ID_i қийматлар булутли серверга юборилади.

2-қадам. $(CS \rightarrow CC_i)$: P_3, P_4, T_i'.

Сервер CS тизимга кириш сўровини қабул қилганидан сўнг, мижоз ID_i сини ўз базасида мавжудлигини текширади. Шундан сўнг, ET_i, EA_i' ва EE_T параметрлар асосида қуйидагилар ҳисобланади:

$T_i = ET_i \oplus K_{CS}$;

$R_S = T_i \oplus H(K_{CS})$;

$A_i' = EA_i' \oplus R_S$;

$E_T = EE_T \oplus R_S$;

$CK = H(R_S || K_{CS} || E_T || ID_i)$.

Шундан сўнг, $P_2^* = H(P_1 \times CK)$ ҳисобланади ва $P_2^* ? = P_2$ шарти текширилади. Агар шарт қаноатлантирилмаса, уланиш тўхтатилади. Акс ҳолда, R_2 тасодифий сони генерация қилиниб, қуйидагилар ҳисобланади:

$P_3 = R_2 \times P$;

$P_4 = H(P_1 \parallel R_2 \times A_i')$;

$T_i' = T_i \oplus K_{PV}$.

Шундан сўнг, мижоз P_3, P_4 ва T_i' параметрларни CC_iга юборади.

3-қадам. $(CC_i \rightarrow CS): V_i$.

Сервер CS томонидан P_3, P_4 ва T_i' параметрлари қабул қилингач, қуйидагилар ҳисобланади:

$T_i = T_i' \oplus K_{PV}$;

$A_i = H(T_i \oplus H(CK'))$.

$P_4^* = H(P_1 \parallel A_i \times P_3)$ қиймат P_4 га тенг бўлса ($P_4^* = P_4$), мижоз серверни аутентификациядан ўтказади. Акс ҳолда, уланиш тўхтатилади. Шундан сўнг, мижоз томонидан сессия калити SK ва V_i параметрлар қуйидагича ҳосил қилинади:

$SK = R_1 \times PW_i \times P_3 = R_1 \times R_2 \times PW_i \times P$;

$V_i = H(SK \parallel R_1 \times PW_i \times P_3)$.

4-қадам.

Сервер CS V_i параметрни қабул қилганидан сўнг, сессия калитини ва V_i^* параметрни ҳисоблайди:

$SK = R_1 \times PW_i \times P_3 = R_2 \times P_1 = R_1 \times R_2 \times PW_i \times P$;

$V_i^* = H(SK \parallel R_2 \times P_1)$.

Агар $V_i^* = V_i$ шарт қаноатлантирилса, икки томонлама аутентификация муваффаққиятли ўтган ҳисобланади ва сервер CS мижоз билан бир хил сессия калитига эгалигини билади. Акс ҳолда, уланиш тўхтатилади (2.4-расм).

Паролни алмаштириш босқичи

1-қадам. $(CC_i \rightarrow CS): ID_i, PV_i, PV'_i$.

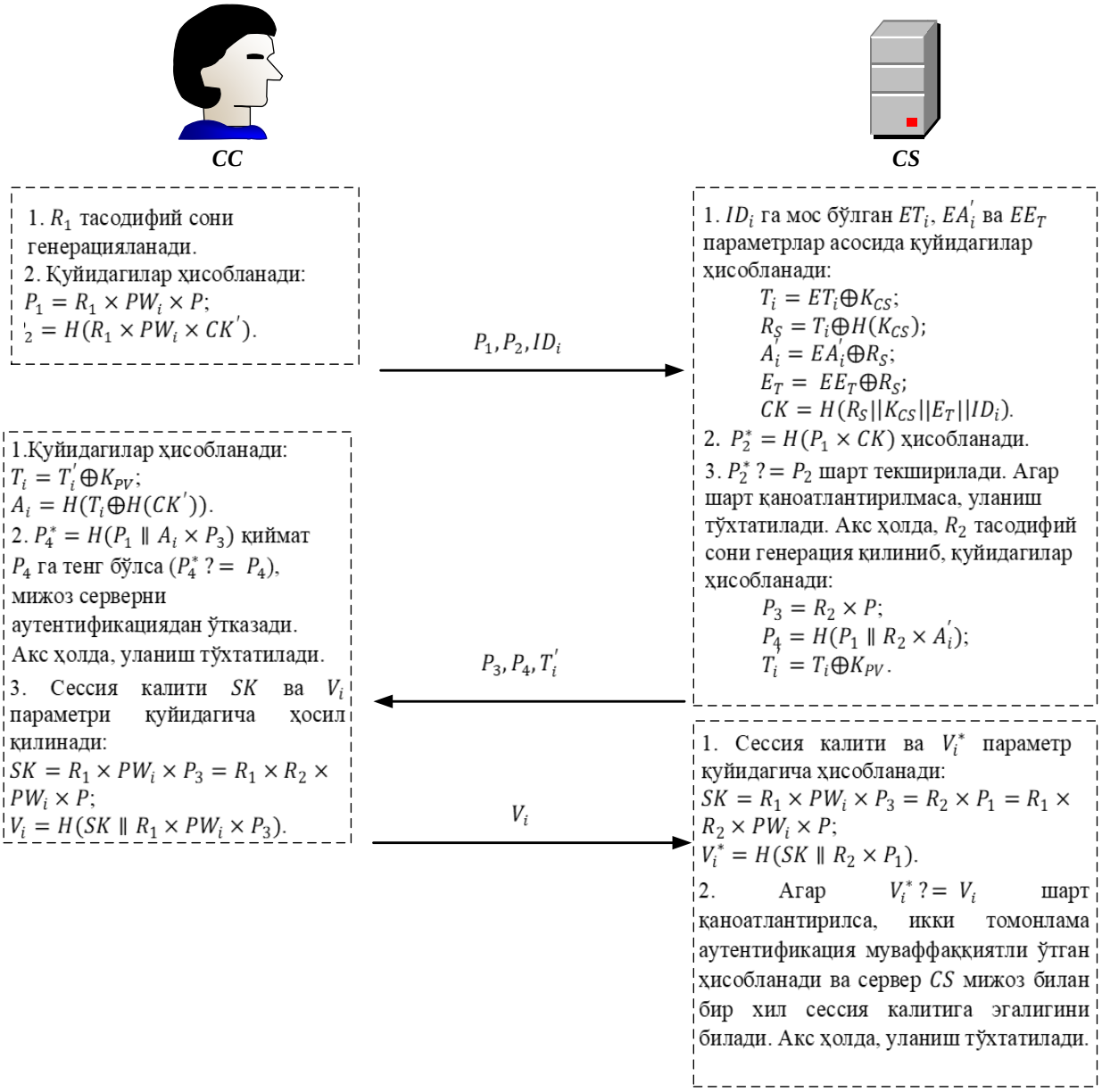
Мижоз CC жорий PW_i паролни ва PW'_i янги паролни ни киритган ҳолда, қуйидагиларни ҳосил қилади ва идентификатори ID_i билан биргаликда сервер CS га юборади.

$PV_i = P \cdot PW_i = (PV_x, PV_y);$

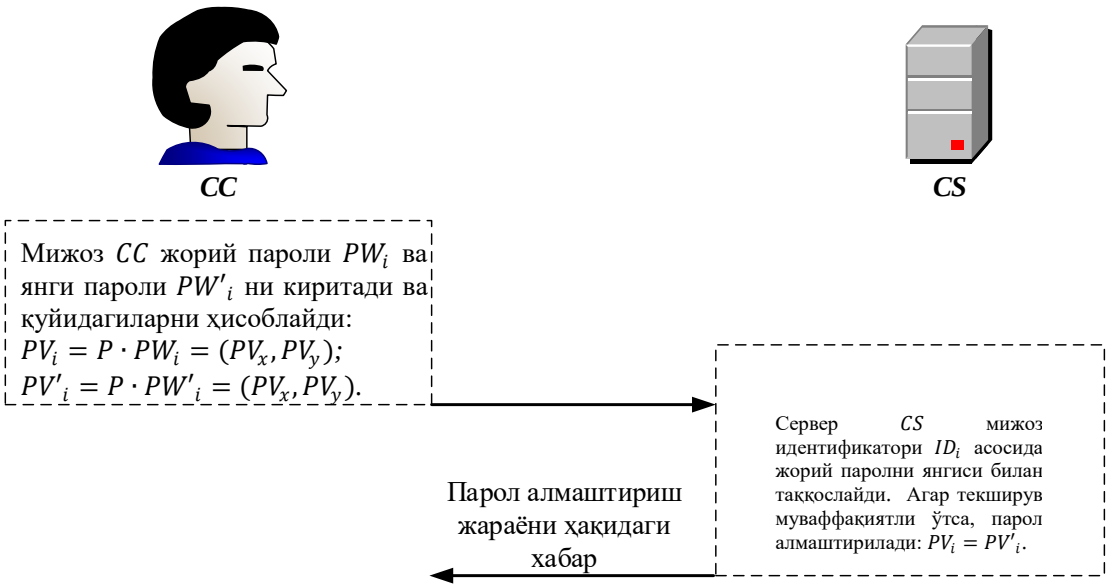
$PV'_i = P \cdot PW'_i = (PV_x, PV_y).$

2-қадам. $(CS \rightarrow CC_i)$: Парол алмаштириш жараёни ҳақидаги хабар

Сервер CS мижоз идентификатори ID_i асосида жорий паролни таққослайди. Агар текширув муваффақиятли ўтса, парол алмаштирилади: $PV_i = PV'_i$ (2.5-расм).



4-расм. Протоколнинг аутентификациядан ўтиш босқичи



2.5-расм. Протоколнинг паролни алмаштириш босқичи

Хулоса

1. Фойдаланувчиларни аутентификациялашда паролга нисбатан хавфсизлиги юқори бўлган эллиптик эгри чизиқлардан фойдаланиш кичик ҳисоблаш имкониятига эга қурилмалар ёрдамида ҳам амалга ошириш имкониятини кўрсатди.

2. Таклиф этилган протокол хавфсизлигининг формал ва ноформал тасдиқлари уни такрорлаш, паролга фараз бўйича, ўртага турган одам ва обрўсизлантириш ҳужумларига бардошлигини ҳамда сеанс калитини тақсимлаш имкониятини ва тўла тўкис хавфсизлик талабини қаноатлантиришини кўрсатди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.

2. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши // Тошкент, 2008, -Б. - 394.

3. Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Давлатов А.Б. “Криптотаҳлил ва унинг махсус усуллари” электрон ўқув қўлланма. 2010 й.

4. Акбаров Д.Е., Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П. “Криптографиянинг математик асослари” электрон ўқув қўлланма. 2010 й.

5. С.К.Ганиев, М.М.Каримов, З.Т.Худойқулов, М.М.Кадиров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках. –Т.: «Иқтисод-молия», - 2017, 480 с.

6. С.К.Ганиев, М.М.Каримов, К.А.Ташев. Ахборот хавфсизлиги. –Т.: «Фан ва технология», 2016, 372 бет.

7. Mersaid A., Gulom T. The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1 //International Journal of Electronics and Information Engineering. – 2016. – Т. 4. – №. 1. – С. 1-11.

8. Dejamfar S. M., Najafzadeh S. Authentication Techniques in Cloud Computing: A Review //International Journal of Advanced Research in Computer Science and Software Engineering. – 2017. – Т. 7. – №. 1.

9. Mell P. et al. The NIST definition of cloud computing. – 2011.

10. Leila M., Abdelhafid Z., Mahieddine D. A New Framework of Authentication Over Cloud Computing //Proceedings of the Computational Methods in Systems and Software. – Springer, Cham, 2017. – С. 262-270.

11. Patel K., Alabisi A. Cloud Computing Security Risks: Identification and Assessment //The Journal of New Business Ideas & Trends. – 2019. – Т. 17. – №. 2. – С. 11-19.

12. Tanash R. M., Ala'F K., Darabkh K. A. Communication over Cloud Computing: A Security Survey //2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). – IEEE, 2019. – С. 496-501.

13. Rizwan S., Zubair M. Basic Security Challenges in Cloud Computing //2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST). – IEEE, 2019. – С. 1-4.

14. Al_Janabi S., Hussein N. Y. The reality and future of the secure mobile cloud computing (SMCC): survey //International Conference on Big Data and Networks Technologies. – Springer, Cham, 2019. – С. 231-261.

15. Information Supplement: PCI SSC Cloud Computing Guidelines. Cloud Special Interest Group PCI Security Standards Council. April 2018. https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

16. Siyakha N. Mthunzi, Elhadj Benkhelifa, Tomasz Bosakowski, Chirine Ghedira Guegan, Mahmoud Barhamgi, Cloud computing security taxonomy: From an atomistic to a holistic view, Future Generation Computer Systems, Volume 107, 2020, Pages 620-644.

17. Ashish Singh and Kakali Chatterjee, Cloud security issues and challenges: a survey, Journal of Network and Computer Applications http://dx.doi.org/10.1016/j.jnca.2016.11.027

18. Hubbard D, Sutton M. Top threats to cloud computing v1. 0. Cloud Security Alliance. 2010 Mar.

19. Hong J. B. et al. Systematic identification of threats in the cloud: A survey //Computer Networks. – 2019. – T. 150. – C. 46-69.

20. Ramachandra G., Iftikhar M., Khan F. A. A comprehensive survey on security in cloud computing //Procedia Computer Science. – 2017. – T. 110. – C. 465-472.

21. Khan M. A. A survey of security issues for cloud computing //Journal of network and computer applications. – 2016. – T. 71. – C. 11-29.

22. Abdurachman E. et al. Survey on Threats and Risks in the Cloud Computing Environment //Procedia Computer Science. – 2019. – T. 161. – C. 1325-1332.

23. Lim S. Y., Kiah M. L. M., Ang T. F. Security Issues and Future Challenges of Cloud Service Authentication //Acta Polytechnica Hungarica. – 2017. – T. 14. – №. 2. – C. 69-89.

24. Sood SK. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications. 2012 Nov30; 35(6): pp. 1831-1838.

25. Tang Y, Lee PP, Lui J, Perlman R. Secure overlay cloud storage with access control and assured deletion. Dependable and Secure Computing, IEEE Transactions on. 2012 Nov; 9(6): pp. 903-916.

26. Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Information Sciences. 2014 Feb 10; 258:371-86.

27. Gennaro R, Gentry C, Parno B. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. InAdvances in CryptologyCRYPTO 2010 2010 Jan 1 (pp. 465-482). Springer Berlin Heidelberg.

28. Li S, Sadeghi AR, Heisrath S, Schmitz R, Ahmad JJ. hPIN/hTAN: A lightweight and low-cost e-banking solution against untrusted computers. InFinancial Cryptography and Data Security 2012 Jan 1 (pp. 235-249). Springer Berlin Heidelberg.

29. Wang C, Wang Q, Ren K, Cao N, Lou W. Toward secure and dependable storage services in cloud computing. Services Computing, IEEE Transactions on. 2012 Apr;5(2):220-32.

30. J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019.

31. J. Xiong et al., "A Secure Data Self-Destructing Scheme in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 448-458, 1 Oct.-Dec. 2014.

32. P. Mishra, K. Khurana, S. Gupta and M. K. Sharma, "VMAnalyzer: Malware Semantic Analysis using Integrated CNN and Bi-Directional LSTM for Detecting VM-level Attacks in Cloud," 2019 Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-6.

33. S. Muthurajkumar, M. Vijayalakshmi, S. Ganapathy and A. Kannan, "Agent based intelligent approach for the malware detection for infected cloud data storage files," 2015 Seventh International Conference on Advanced Computing (ICoAC), Chennai, 2015, pp. 1-5.

34. J. Darrous, S. Ibrahim, A. C. Zhou and C. Perez, "Nitro: Network-Aware Virtual Machine Image Management in Geo-Distributed Clouds," 2018 18th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Washington, DC, 2018, pp. 553-562.

35. H. Liu, B. He, X. Liao and H. Jin, "Towards Declarative and Data-Centric Virtual Machine Image Management in IaaS Clouds," in IEEE Transactions on Cloud Computing, vol. 7, no. 4, pp. 1124-1138, 1 Oct.-Dec. 2019.

36. S. M. Neamul Islam and M. Rahman, "Securing virtual machine images of cloud by encryption through Kerberos," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, 2017, pp. 1074-1079.

37. X. Yue, L. Xiao, W. Zhan, Z. Xu, L. Ruan and R. Liu, "An Optimized Approach to Protect Virtual Machine Image Integrity in Cloud Computing," 2016 7th International Conference on Cloud Computing and Big Data (CCBD), Macau, 2016, pp. 75-80.

38. F. Zhang, J. Wang, K. Sun and A. Stavrou, "HyperCheck: A Hardware-AssistedIntegrity Monitor," in IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 4, pp. 332-344, July-Aug. 2014.

39. Wu C, Wang Z, Jiang X. Taming Hosted Hypervisors with (Mostly) Deprivileged Execution. InNDSS 2013 Feb.

40. Li C, Raghunathan A, Jha NK. A trusted virtual machine in an untrusted management environment. Services Computing, IEEE Transactions on. 2012 Sep 1;5(4): pp. 472-483.