https://doi.org/10.53360/2788-7995-2025-2(18)-1

ҒТАХР: 81.93.29

Д. Төлеген*, Қ. Сейлханова, А. Жеткербай
Астана IT Университеті,
010000, Қазақстан Республикасы, Астана қ., Мәңгілік ел даңғылы, 55/11
*e-mail: D.Tolegen@astanait.edu.kz

ИНТЕРНЕТ ЗАТТАРЫ ҮШІН СЕНІМДІ БАСҚАРУҒА ШОЛУ

Аңдатпа: *Қазіргі әлемде Заттар интернеті (IoT) барған сайын маңызды рөл атқарады, бұл әртүрлі құрылғылар мен объектілердің нақты уақыт режимінде өзара әрекеттесуіне мүмкіндік береді. Дегенмен, қосылған құрылғылар санының өсуімен бұл жүйелерді сенімді басқаруды қамтамасыз ету қажеттілігі туындайды. Заттар интернеті (IoT) – бұл сенсорлармен жабдықталған құрылғылар желісінің тұжырымдамасы және интернетке қосылу мүмкіндігі, бұл оларға адамның тікелей қатысуынсыз байланысуға және өзара әрекеттесуге мүмкіндік береді. IoT тиімділікті арттыруға, автоматтандыруға және өмір сапасын жақсартуға айтарлықтай үлес қосады.Бұл жұмыста біз IoT үшін сенімді басқарудың қазіргі жағдайын жүйелі түрде қарастырамыз және талдаймыз. Біз сенімді басқару әдістерін қалыптастыру үшін қолданылатын құралдарға, әдістерге және технологияларға негізделген жіктеуді ұсынамыз (сенімді қалыптастыру үшін ақпарат жинау, сенімді құндылықтарды есептеу және сақтау). Мақала IoT-тегі қауіпсіздік пен басқарудың негізгі мәселелерін қарастырады, сонымен қатар құрылғылар мен деректердің сенімділігі мен қауіпсіздігін қамтамасыз ететін шешімдерді ұсынады. Қорытындылай келе, IoT құрылғыларының қауіпсіздігі мен тиімділігін қамтамасыз ету үшін сенімді басқарудың маңыздылығы туралы қорытынды жасалады. Біз оқырманға осы саладағы өзекті мәселелерді түсінуге, сенімді басқару жүйесін құруға және әдебиеттерді шарлауға көмектесуге тырысамыз.*

Түйін сөздер: *шабуылдар, Заттар интернеті(IoT), қауіпсіздік, сенімді бағалау, сенімді басқару, аналитика.*

Кіріспе

Заттар интернеті (IoT) – бұл біздің күнделікті өмірімізде кеңінен қолданылатын жаңа технология. Cisco-ның жылдық есебіне сәйкес (2018-2023), IP желілеріне қосылған құрылғылардың саны 2023 жылға қарай әлем халқының санынан үш еседен астам көп болады [1]. IoT терминін алғаш рет 1999 жылы Кевин Эштон жеткізу тізбегін басқару контекстінде енгізген [2], бірақ соңғы онжылдықта бұл тұжырымдама ауыл шаруашылығы [3], денсаулық сақтау [4], энергетика [5] және көлік [6] сияқты көптеген салаларда қолданылды. IoT интернет арқылы байланысатын RFID, сенсорлар, ұялы телефондар және басқалар сияқты құрылғылардың байланысты желісін жасайды. Бұл құрылғылар қоршаған ортадан ақпарат жинайды және өнеркәсіптік жүйелерге де, адамдарға да мәліметтер береді.

Бұл жұмыстың мақсаты-сенімді басқарудың қолданыстағы механизмдерін анықтау және әр санаттағы шектеулерді анықтау мақсатында оларды негізгі технологиялары бойынша жіктеу. Жұмыстың мақсаты-осы салаға шолу жасау және анықталған мәселелерді талқылау.

IoT желісі сияқты динамикалық ортада зиянды түйіндерді анықтау өте маңызды. Күнделікті өмірде біз жеке өмірімізде де, кәсіби өмірімізде де сенімді адамдармен ынтымақтасып, байланыс орнатқымыз келеді. Сол сияқты, IoT құрылғылары бірқалыпты жұмыс істеуі үшін оларға шынайы ақпарат беретін сенімді түйіндермен өзара әрекеттесуі қажет.

Сенімді есептеу IoT жүйелерінің қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Бұл жүйедегі әрбір құрылғы мен желі түйінінің сенімділігі мен сенімділік деңгейін бағалау процесін білдіреді. Сенімді есептеу жиналған деректерге және әртүрлі факторларға, соның ішінде әрекет тарихына, қол жеткізу деңгейіне және құрылғының орындалу сапасына негізделген.

Сенімді дұрыс бағалау IoT жүйесіне ықтимал қауіптер мен шабуылдардың алдын алуға көмектеседі. Сенімді есептеу зиянды бағдарламалар мен хакерлер сияқты күдікті мінез-құлық пен қауіпсіздік қатерлерін бөліп көрсетуге мүмкіндік береді. Бұл мұндай қауіптерге тез жауап беруге және олардың алдын алу үшін тиісті шараларды қабылдауға мүмкіндік береді.

Сенімнің негізгі принципі-IoT құрылғыларын дәл анықтау. Әрбір құрылғыда желіде ерекшеленуге мүмкіндік беретін бірегей идентификатор болуы керек. Бұл бірегей идентификатор құрылғының желіге кіруін және оның басқа құрылғылармен өзара әрекеттесуін қамтамасыз етеді. Аутентификация процесі орнатылғаннан кейін қол жеткізуді басқару механизмдері әр құрылғы үшін қандай деректер мен әрекеттерге рұқсат етілгенін анықтайды.

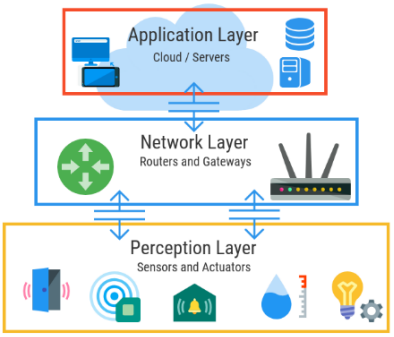
Тасымалдау кезінде де, оны пайдалану кезінде де рұқсатсыз кіруге және бұрмалануға жол бермеу үшін деректердің тұтастығы мен құпиялылығын қамтамасыз ету өте маңызды. Сенімді құрылғылар интернет заттарының үздіксіз жұмыс істеуі мен қауіпсіздігін қамтамасыз ету үшін қажет. Бұған құрылғылардың әрекетін бағалау, күдікті ауытқуларды бақылау және қажет болған жағдайда сенімді жою кіреді. Процесс басқа түйіндер үшін ақпаратты жинаудан, осы ақпаратты сенім деңгейін есептеу үшін пайдаланудан, содан кейін осы ақпаратты сақтаудан және пайдаланудан басталады. Сенім деңгейі түйіннің басқасына сене алатынын немесе онымен әрекеттесе алатынын анықтайды. Адамдар ретінде біз ешқашан сенбейтін адаммен мәміле жасамас едік; бұл желідегі IoT түйіндеріне де қатысты.

IoT-де әр түрлі сенім модельдерін қолдануға болады, мысалы, иерархиялық сенім модельдері, беделге негізделген сенім модельдері және нақты IoT қолдану мен архитектурасына байланысты сенім модельдері.

IoT-тегі сенімді басқару-бұл IoT құрылғылары мен қызметтерінің қызмет ету мерзімі ішінде сенімділікті орнату және қолдау үшін өндірушілер, қызмет көрсетушілер және соңғы пайдаланушылар арасындағы ынтымақтастықты қажет ететін үздіксіз процесс.

Зерттеушілердің көпшілігінің пікірінше, IoT-бұл үш қабатты архитектура [7, 8]. Бұл Қабылдау қабаты, Желі қабаты және Қолдану қабаты (сурет 1).

- Қабылдау қабаты (Perception Layer): бұл қабат IoT жүйесіне кіріс сенсорларын, датчиктерді және кіріс құрылғыларын қамтамасыз етеді. Олар ауқымдылық, температура, байланыс және басқа ақпараттарды алып, оны IoT жүйесіне жібереді. Мысалы, жылжымайтын сенсорлар, уақытты күзету және қазіргі уақытты санап алуға мүмкіндік береді.
- Желілік қабат(Network Layer): бұл деңгей құрылғылар мен серверлер, сондай-ақ басқа желілік құрылғылар арасындағы байланысты қамтамасыз етеді. Сонымен қатар, осы деңгейдегі хаттамалар құрылғылар арасында ақпарат алмасу үшін қолданылады. IoT деректерін басқарудың және оны өткізудің негізгі бөлігі. Ол деректерді жинап алу, өңдеу және оны көлемден көбіру үшін барлық тұрақтарды біріктіреді. Бұл қабатта мерзімдеулі түрде желілер, ұялар, байланыс құрылғылары, Wi-Fi, Zigbee, Bluetooth, LoRa, қатарына сәйкес технологиялар пайдаланылады.
- Қолдану қабаты (Application Layer): желі мен IoT қызметтері арасындағы аралық қабат ретінде қызмет етеді. Смарт құрылғылардан жиналған деректер қолданба деңгейіне тасымалданады. Бұл қабат IoT деректерін анықталған мақсаттар үшін пайдалануға арналған. Ол деректерді талдама, толтыру, талдау және кез келген мақсатқа сәйкес жасау үшін өнімдер мен қызметтерді қамтамасыз етеді. Мысалы денсаулық, энергия ұзындығы, қала жобалары, әуесқой жүйелер, орындау жүйелері, мониторинг және Smart health, smart home және т.б. сияқты қосымшалар осы қабатқа жатады.



Сурет 1 – IoT архитектурасы

Қабылдау қабаты сенсорлар мен датчиктерді алып, оларды араларындағы желілерден атқару жолымен жүйеге жібереді. Желі қабаты деректерді алу, өңдеу және сақтау үшін араларды біріктіреді. Қолдану қабаты анықталған мақсаттар үшін аралық тұрақтардағы деректерді өңдеуді және талдамаға арналған өнімдер мен қызметтерді ұсынады.

Материалдар мен тәсілдер

Сенімді басқару жүйесі сенімді есептеулерді орындау үшін деректерді жинауы керек. Ақпаратты жинау-сенімді есептеудің алғашқы қадамы. Бұл сенім параметрлері туралы білім жинау процесін білдіреді. Ақпарат жинауды екі санатқа бөлуге болады:

1. Тікелей(Direct) сенім: сенім сенім қатынастарына қатысушы екі тараптың тікелей бақылаулары мен өзара әрекеттестігі негізінде қалыптасады.
2. Жанама(Indirect) сенім: сенімгер мен сенім білдірілген тұлға бұрынғы өзара әрекеттесулерді бөліспейді. Сенім басқа түйіндердің ұсыныстары негізінде қалыптасады [9], [10].

Сенімнің таралуы сенім дәлелдерінің жүйеге қатысатын түйіндерге қалай таралатынын білдіреді және ол екі санатқа бөлінеді:

1. Таратылған(Distributed): әрбір түйін басқа түйіндердің сенім мәндерін сақтайды. Түйіндер өзара әрекеттеседі және сенім дәлелдерін басқа түйіндермен алмасады. Түйіндер процедураға орталық органның қатысуынсыз сенімгерлік құндылықтарды дербес сақтайды және есептейді.
2. Орталықтандырылған (Centralized): сенім құндылықтарын есептеу және сақтау үшін орталық орган қатысады. Бұл ұйым сенімгерлік дәлелдемелерді таратуға және өңдеуге жауапты [9, 10].

Зерттелген әдебиеттер негізінде IoT түйіні 1-кестеде келтірілген шабуылдарды орындай алады. Шабуыл сенімге байланысты болуы мүмкін немесе IoT архитектурасының басқа қабатына жатуы мүмкін. Осы кесте IoT жүйесінің әр қабатында кездесетін қауіптерді жіктеп көрсетеді және қауіпсіздік шараларын нақты қай деңгейде күшейту қажет екенін айқындауға көмектеседі. Мақала аясында сенімге қатысты шабуылдарға көбірек көңіл бөлініп отыр, себебі олар желі ішіндегі түйіндердің өзара әрекеттесу сапасына және жалпы жүйе қауіпсіздігіне тікелей әсер етеді.

Кесте 1 – Әрбір шабуылдың санаты

Шабуыл	Сенімге қатысты	Application Layer	Network Layer	Perception Layer
BMA	✓			
BSA	✓			
SPA	✓			
OSA	✓			
OOA	✓			
EA				
NCA		✓		
RA				✓
SA			✓	
WA				
DoS			✓	
SFA			✓	
BA			✓	
WHA			✓	
IA		✓		
SDA				

IoT жүйесінде түйіндер бағаланатын сенімді басқару әдісін қолдана отырып, түйіннің сенімділік деңгейі олардың имиджінде маңызды рөл атқарады. Жақсы сенім деңгейі бар түйін бірнеше серіктестерге ие бола алады және жүйеге әсер ете алады. Демек, біз сенімге байланысты шабуылдарға алаңдаймыз. Біріншіден, біз осы уақытқа дейін әдебиетте анықталған шабуылдардың осы түрлерін егжей-тегжейлі қарастырамыз [9, 11]:

* Bad mouthing шабуылдары (BMA): зиянды түйін оның беделін түсіруге тырысып, адал түйінге жаман ұсыныстар бере алады. Бұл шабуылдың мақсаты-адал түйіннің беделін түсіру.

* Ballot stuffing шабуылдары (BSA): зиянды түйін басқа зиянды түйіндерге оң ұсыныстар береді. Мұндай шабуылдың мақсаты-басқа зиянды түйіндерге деген сенімділікті арттыру, бұл олардың желідегі әсерін арттыруға көмектеседі.

* Self-promoting шабуылдары (SPA): зиянды түйін желідегі ықпалын арттыру үшін өзіне жақсы ұсыныстар бере алады.

* Opportunistic service шабуылдары (OSA): зиянды түйін сенімнің жоғары деңгейін алу үшін жақсы қызмет көрсете алады, содан кейін басқа зиянды түйіндермен ынтымақтаса отырып, жаман сөздер мен бюллетеньдерді толтыру шабуылдарын жасай алады.

* On-Off шабуылдары (OA): зиянды түйін кейде жосықсыз, кейде сапалы қызметтерді ұсына алады. Бұл шабуыл кезінде түйін сенімсіз түйін ретінде белгіленуден аулақ болады.

Осы мақаланың аясында біз осы сауалнамаға енгізілген әдебиеттерде айтылған шабуылдардың келесі түрлерін талқылаймыз:

– Eclipse шабуылы (EA): Бұл шабуыл сценарийінде зиянды түйін жәбірленушіні желінің қалған бөлігінен оқшаулайды.

– Node Capture шабуылы (NCA): байланыс сілтемелері, жалған деректерді енгізу және т. б. тұрғысынан IoT физикалық құрылғыларына бағытталған [8]

– Replay шабуылы (RA): шабуылдың бұл түрінде зиянды түйін ақпарат алу және қабылдағышты дұрыс бағыттамау үшін байланысты тыңдайды. [8] Мысалы, Егер Алиса Бобпен ақпараттың бір бөлігін бөліссе (оның жеке басын дәлелдеу үшін), онда Ева әңгімені тыңдап, Алиса бөліскен ақпаратты сақтайды. Енді Ева Бобпен арам пиғылмен сөйлесіп, өзін Алиса етіп көрсете алады.

– Sybil шабуылы (SA): зиянды түйін бірнеше идентификаторларға ие және бір уақытта желінің әртүрлі жерлерінде бола алады.

– Whitewashing шабуылы (WA): нашар беделге ие түйін өзінің беделін қалпына келтіру үшін жаңа идентификатормен желіге қайта қосылған кезде.

– Denial of Service шабуылы (DoS): зиянды түйін басқа пайдаланушыларға қол жетімсіз ету үшін желіге көптеген сұраулар жіберген кезде.

– Spoofing шабуылы (SFA): түйін басқа сәйкестікті пайдаланып, өзін басқа біреу ретінде көрсеткенде.

– Blackhole шабуылы (BA): түйін барлық хабарларды жойған кезде, ол қайта жіберілуі керек. Бұл шабуыл желіде бос орын тудырады.

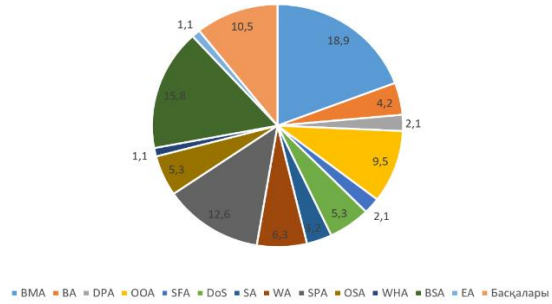
– Wormhole шабуылы (WHA): бұл шабуылға қатысатын түйіндер ұзақ қашықтықта байланысатын күшті түйіндер болып табылады. Пакеттер туннель арқылы бір зиянды түйіннен екіншісіне жіберіледі. Осылайша, олар желінің басқа түйіндерін осы екі түйіннің жақын екендігіне сендіре алады.

– Инъекциялық шабуылдар (IA): желінің үздіксіз жұмысын бұзу үшін зиянды код енгізіледі.

– Sleep deprivation шабуылы (SDA): зиянды түйін оны сергек ұстау және батареяның барлық ресурстарын жылдам тұтыну үшін түйінге жиі сұраулар жасайды [12].

Нәтижелер

Бұл бөлімде біз берілген қауіп үлгісіне қатысты кейбір деректерді ұсынамыз. 2-суретте әдебиетте қарастырылған шабуылдарға қатысты статистикалық ақпарат көрсетіледі. Статистикалық мәліметтер жүйелік қауіпсіздік саласындағы ғылыми мақалалар мен зерттеулерден жинақталған.



Сурет 2 – Әрбір қауіп үлгісінде айтылған әрбір шабуылдың пайызы

Бұл мәліметтер 30-дан астам академиялық дереккөзді шолу нәтижесінде алынған, оның ішінде IoT (Интернет заттар желісі) жүйесіне арналған қауіпсіздікке қатысты басылымдар қамтылды. Әрбір дереккөзде келтірілген шабуыл түрлері сандық түрде тіркеліп, жиілік бойынша есептелді.

Мәліметтерді өңдеу процесі төмендегі қадамдарды қамтыды:

- Әдебиеттерді шолу; Google Scholar, IEEE Xplore, Springer, Elsevier секілді ғылыми платформалардан 30-дан астам мақала іріктелді. Негізгі критерий – IoT жүйесіне қатысты қауіпсіздік шабуылдарын сипаттайтын зерттеулер.
- Әр мақалада көрсетілген шабуыл түрлерін тіркеу; Әрбір мақалада айтылған шабуыл түрлері жеке-жеке тіркеліп, сандық түрде белгіленді. Мысалы, бір мақалада BMA мен SPA айтылса, екеуіне де 1 бірлік қосылды.
- Әр шабуылдың қайталану жиілігін есептеу; Барлық тіркелген шабуылдар біріктіріліп, әр шабуылдың жиілік саны есептелді. Мысалы, BMA 18 рет кездессе, оның жиілігі 18 болып тіркелді.
- Жалпы жиынтық бойынша пайыздық үлесін шығару; Әр шабуыл түрінің жиілігі жалпы жиынтыққа бөліп, 100-ге көбейту арқылы пайыздық көрсеткіш алынды. Мысалы, BMA = (18 / 95) * 100 ≈ 18.9%.

Бұл процесс библиометриялық талдауға ұқсас әдіспен жүзеге асырылды. Эксперименттік тестілеу жүргізілген жоқ, себебі мақсатымыз – қолданыстағы зерттеулердегі шабуыл түрлерінің жиілігін талдау арқылы сенімді басқару жүйелерінің әлсіз тұстарын анықтау болды. Біз сенімге байланысты шабуылдар – BMA, BSA, SPA, OSA, OOA – әдебиеттерде ең егжей-тегжейлі қарастырылғанын байқаймыз. Сенімді басқару жүйесі үшін сенімге байланысты шабуылдарды жеңе білу өте маңызды, бірақ бұл тек негіз болып табылады. Жақсы ойластырылған сенімді басқару жүйесі шабуылдардың барлық түрлерімен күресуге қабілетті болуы керек. Біз құжаттардың тек 1,10%-ы EA, RA, SDA және WHA-ны қарастыратынын көреміз. Мұндай шабуылдар Интернет Заттарының желісіне елеулі зақым келтіруі мүмкін.

Жоғарыда келтірілген талдауларға сүйене отырып, біз байқаған осалдықтардың кейбір маңызды сәттерін ұсынамыз.

* Масштабталу: жоғарыда келтірілген талдаудан байқағанымыздай, эксперименттерді жүргізу кезінде жұмыстардың көпшілігінде масштабталу коэффициенті ескерілмеген. Көптеген сенсорлар қосылған және бір-бірімен байланысатын кеңейтілген IoT желілерінде сенімді басқару жүйесі тиімді жауап бере алуы керек. Әсіресе, түйіндер саны бекітілмеген динамикалық желілерде сенімгерлік басқару схемасы өсіп келе жатқан жұмыс көлеміне бейімделе алуы керек.

– Құпиялылық: құпиялылық әр жүйеде, әсіресе ресурстары шектеулі IoT құрылғыларында шешуші рөл атқарады. Сенімді басқару жүйесі түйіндер арасындағы сенімді есептеу және сақтау үшін құпия деректерді өңдеуге қабілетті, мысалы, олардың арасындағы байланыс жиілігі арқылы. Блокчейн технологиясы көптеген мәселелерді шеше алады, дегенмен орталықсыздандыруды көздейтін қоғамдық блокчейндер құпиялылықты қамтамасыз етпейді. Егер қандай да бір құпия ақпарат ақылды келісімшартқа қосылуы немесе блокчейнде сақталуы керек болса, ол барлық қатысушыларға қол жетімді болады.

– Контекст: сенім процесінде контекст шешуші рөл атқарады. Кейбір адамдар немесе құрылғылар белгілі бір контексттерде немесе жағдайларда ғана сенімді бола алады. Мысалы, зиянды түйін белгілі бір контекстте ғана сенімділікті көрсете алады. Әр түрлі IoT желілерінің реакциясы контекстке байланысты айтарлықтай өзгеруі мүмкін.

– Энергия: энергия ресурстармен қамтамасыз етілген Интернет Заттары құрылғылары үшін шынымен маңызды фактор болып табылады. Зерттеу қауымдастығы жеңіл салмақты сенімді басқару жүйесін жобалау мәселесін жан-жақты зерттеген жоқ. Біз кейбір жұмыстарда сенімді басқарудың жұмысынан туындаған энергия шығынын өлшеу бойынша эксперименттер жүргізіліп жатқанын байқадық.

– Шабуылдар: сенімді басқару жүйелері қауіп-қатер моделіне кейбір сенімді шабуылдарды қосады. Мұндай шабуылдарды Интернет Заттары желісі үшін құнды болу үшін сенімгерлік басқару жүйесі шешуі керек. Талдау барысында біз жұмыстардың көпшілігі негізінен сенімге негізделген шабуылдарға арналғанын көрдік. Зерттеу қауымдастығының назарын аударған шабуылдар-BMA, BSA және SPA.

OA және OSA соншалықты жан-жақты зерттелмеген. Дегенмен, сенімді басқару схемасы сенімге бағытталған шабуылдарды ғана емес, бірнеше шабуылдарды да анықтай алуы керек. Әсіресе, IoT түйіндерін жеңіл түйіндер деп атайтын блокчейн негізіндегі жұмыстар EA-ны ескеруі керек.

Талдау

Болашақ жұмыста сенімге байланысты шабуылдармен күресетін, сонымен қатар басқа да көптеген шабуылдармен күресетін сенімді басқару әдістерін зерттеу жақсы болады.

– Ұтқырлық: IoT ұтқырлығы жоғары тапсырмаларға да қатыса алады (мысалы, смарт көліктер). Ұтқырлығы жоғары ортаға бейімделетін сенімгерлік басқару жүйесін жобалау маңызды. Бұл мәселені шешуде көп жұмыс атқарылмайды.

– Қауіп-Қатер моделі: біз қауіп-қатер моделіне жатпайтын көптеген жұмыстардың бар екенін байқадық. Біздің ойымызша, сенімді басқарудың ұсынылған әдістемесі қандай қауіп-қатер моделін және қандай шабуылдармен күресетінін көрсету өте маңызды. Әр жүйе үшін әр түрлі шабуылдар қолайлы.

– Алдын ала сенімді субъектілер: кейбір тәсілдер кейбір алдын ала сенімді субъектілерді қажет етеді. Бұл нақты өмірлік сценарийлерде қолданылмауы мүмкін болжам. Мұндай болжам болған жағдайда, алдын-ала сенімді субъектілердің қайсысы екендігі және олардың жүйедегі рөлі нақты көрсетілуі керек. Алайда, бұл тәсілдер әрдайым қолданыла бермейді.

– Қолданылатын технологияларға егжей-тегжейлі шолу: жүйеде қолданылатын барлық компоненттер туралы толық ақпарат берілуі керек, әсіресе жоба блокчейн және машиналық оқыту сияқты қосымша технологияларды қолданса. Блокчейннің сипаттамалары егжей-тегжейлі берілуі керек, өйткені оқырман тарапынан шамалы болжам бүкіл жүйені өзгерте алады.

– Қорғаныс Механизмдері: егер зиянды түйін анықталса, онда кейбір қорғаныс механизмдері болуы керек. Кейбір жұмыстар желінің түйінін алып тастауды ұсынады. Жақсырақ баламаларды ұсыну үшін зерттеу қауымдастығы осы тақырыпқа көбірек көңіл бөлуі керек.

– Сүзу Бойынша Ұсыныстар: сүзу бойынша ұсыныстар жанама сенім қосылған жағдайларда маңызды. Сүзу бойынша ұсыныстар сенімге байланысты шабуылдардың алдын алуға көмектеседі.

– Деректер сенімі: кейбір жұмыстар деректер сенімін ескереді. Бұл тұжырымдама жалпы шабуылдарды ескеретін сенімді басқару әдістерін жасауға көмектеседі (тек сенімге байланысты емес). Деректерді бұрмалау қолданбаның функционалдығына қатысты күрделі мәселелерді тудыруы мүмкін (мысалы, ehealth).

– Сақтау: тағы бір маңызды мәселе-сақтау болып табылады. Кейбір жағдайларда түйіндерде сенімге қатысты ақпараттың үлкен көлемі болуы керек. Бұл мәселеге қатысты кейбір тиімді сақтау механизмдерін ұсынатын кейбір жұмыстар бар, бірақ бұл сала қосымша зерттеуді қажет етеді.

– Желілік Трафик: IoT желілеріндегі зиянды трафикті анықтауға бағытталған бірқатар әдістер бар [13]. Біздің ойымызша, бұл әдістер трафикті жіктеу параметрлерін сенім мен бедел көрсеткіштерінің негізі ретінде пайдалана алатын сенімді басқарудың жаңа әдістерінің негізін құра алады.

Қорытынды

IoT жүйелерінде қауіпсіздік пен сенім өте маңызды, өйткені құрылғылар көбінесе ықтимал дұшпандық ортада жұмыс істейді. Түйіннің сенімділігін бағалаудың бір әдісі-сенімді басқару әдістерін қолдану. Шынында да, соңғы онжылдықта Интернет Заттарына деген сенімгерлік басқару зерттеушілердің үлкен назарын аударды, нәтижесінде шарлау оңай емес көптеген әдебиеттер пайда болды. Осы сынаққа түрткі болған біздің жұмысымыз бірнеше зерттеу сұрақтарын қарастырды:

• C1 – қазіргі уақытта бұл салада қандай әдістер қолданылады? Біздің жұмысымыз бұл сұраққа осы саладағы әдебиеттердің жан-жақты жиынтығына құрылымдық шолу жасау арқылы жауап береді. Біздің сауалнамамыз кез келген мүдделі зерттеушіге біздің негізгі нәтижелерімізді жаңартуға және қайталауға мүмкіндік беретін әдебиеттерді жүйелі шолуға жақсы тәртіпті көзқарасты ұстанады. Біздің шолуымыздың құрылымы алдын-ала талдау нәтижесінде пайда болған категориялар мен өлшемдерге негізделген жіктеуге сәйкес келеді. Негізгі нәтиже-бұл қолданыстағы жұмыстарға арналған нұсқаулық қана емес, сонымен қатар

тәсілдердің қай кластары басым болатынын (мысалы, тікелей және жанама ақпарат жинау әдістерін қолданатын әлеуметтік негізделген тәсілдер) және қайсысы аз зерттелетінін (мысалы, орталықтандырылған тәсілдер) көрсетеді.

• С2 – бұл ұсыныстардың қауіп моделі қандай?

Біз бұл сұраққа IoT қауіпсіздігі туралы әдебиеттерде анықталған шабуылдардың кең класын және сауалнамада қарастырылған ұсынылған тәсілдердің оларға қалай қатысы барын қарастыру арқылы жауап береміз. Біздің басты тұжырымымыз-ұсыныстардың көпшілігі қарастырылып отырған қауіп-қатер моделіне тән емес және жұмыстардың көпшілігі деректердің тұтастығына және сенімге байланысты шабуылдарға бағытталған. Жалпы алғанда, көптеген ықтимал шабуылдар болжамды қауіп үлгілерімен кеңінен қамтылмаған.

• С3 – қандай міндеттер мен болашақ бағыттар бар? Біз бұл сұраққа жауап беру үшін құпиялылық, ауқымдылық және жүктеу сияқты салалардың тізімін, сондай-ақ Интернет Заттарындағы сенімді басқаруға қатысты мәселелерді талқылаймыз. Қиындықтар мен болашақ бағыттардың бір мысалы-қолданыстағы тәсілдердің шектеулерін бағалау нәтижесінде пайда болған қауіптердің нақты үлгілерін пайдаланбау.

Тұтастай алғанда, біздің жұмысымыз оқырмандарға IoT сенімді басқарудың белгілі бір механизміне неғұрлым сәйкес келетін әдістер мен технологияларды және осындай жүйені жобалау кезінде ескерілетін мәселелерді шешуге көмектеседі деп сенеміз. Біздің жұмысымыз зерттеушілерге болашақ зерттеу бағыттарын анықтауда да қолдау көрсете алады. Мысал ретінде барлық ықтимал шабуылдар мен қарсы шараларды қамтитын сенімді басқару жүйелерін құру үшін шабуылға қарсы ағаштарды пайдалану болады.

Әдебиеттер тізімі

1. Singh S. A comprehensive survey on trust management in fog computing / S. Singh, M. Kandpal // In S. Fong, N. Dey, and A. Joshi, editors, ICT Analysis and Applications. – 2022. – P. 87-97.
2. Internet of things (iot): A vision, architectural elements, and future directions / J. Gubbi et al // Future Generation Computer Systems. – 2013. – № 29(7). – P. 1645-1660.
3. Bansal N. IoT Applications in Agriculture / N. Bansal // Apress, Berkeley, CA. – 2020. – P. 93-114.
4. Lin Q. IoT Applications in Healthcare / Q. Lin, Q. Zhao // Springer International Publishing. – Cham, 2021. – P. 115-133.
5. Bansal N. IoT Applications in Energy / N. Bansal. // Apress, Berkeley, CA. – 2020. – P. 115-134.
6. Bansal N. IoT Applications in Transportation / N. Bansal // Apress, Berkeley, CA. – 2020. – P. 239-262.
7. IoT Architecture / M. Jabraeil et al // 2020. – P. 9-31.
8. Kumar R. Leveraging blockchain for ensuring trust in iot: A survey / R. Kumar, R. Sharma // Journal of King Saud University. – Computer and Information Sciences. – 2021.
9. Guo J. A survey of trust computation models for service management in internet of things systems / J. Guo, I. Chen, J.J.P. Tsai // Computer Communications. – 2017. – № 97. – P. 1-14.
10. Towards trustworthy internet of things: A survey on trust management applications and schemes / A. Sharma et al // Computer Communications. – 2020. – № 160. – P. 475-493.
11. Trust management model in iot: A comprehensive survey / M. Saeed et al // Innovations in Bio-Inspired Computing and Applications. – 2022. – P. 675-684.
12. The sleep deprivation attack in sensor networks: Analysis and methods of defense / M. Pirretti et al // International Journal of Distributed Sensor Networks. – 2006. – № 2(3). – P. 267-287.
13. Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city / Muhammad Shafiq et al // Future Generation Computer Systems. – 2020. – № 107. – P. 433-442.

Д. Толеген*, К. Сейлханова, А. Жеткербай
Astana IT University,
010000, Республика Казахстан,г. Астана, проспект Мангилик ел, 55/11
*e-mail: D.Tolegen@astanait.edu.kz

ОБЗОР НАДЕЖНОГО УПРАВЛЕНИЯ ДЛЯ ИНТЕРНЕТА ВЕЩЕЙ

В современном мире интернет вещей (IoT) играет все более важную роль, позволяя различным устройствам и объектам взаимодействовать в режиме реального времени. Однако с

увеличением количества подключенных устройств возникает необходимость в обеспечении надежного управления этими системами. Интернет вещей (IoT) – это концепция сети устройств, оснащенных датчиками и возможностью подключения к интернету, что позволяет им общаться и взаимодействовать без прямого участия человека. IoT вносит значительный вклад в повышение эффективности, автоматизацию и улучшение качества жизни.В этой статье мы систематически рассмотрим и проанализируем текущее состояние доверительного управления для IoT. Мы предлагаем классификацию на основе инструментов, методов и технологий, используемых для формирования надежных методов управления (сбор информации для формирования надежных, расчет и хранение надежных ценностей). В статье рассматриваются основные проблемы безопасности и управления в IoT, а также предлагаются решения, обеспечивающие надежность и безопасность устройств и данных. В заключение делается вывод о важности надежного управления для обеспечения безопасности и эффективности устройств IoT. Мы стремимся помочь читателю понять насущные проблемы в этой области, создать надежную систему управления и ориентироваться в литературе.

Ключевые слова: *атаки, Интернет вещей(IoT), безопасность, надежная оценка, надежное управление, аналитика.*

D. Tolegen*, K.Seilkhanova, A.Zhetkerbay
Astana IT University,
050040, Republic of Kazakhstan, Astana, Mangilik El avenue, 55/11
*e-mail: D.Tolegen@astanait.edu.kz

OVERVIEW OF TRUST MANAGEMENT FOR INTERNET OF THINGS

In today's world, the Internet of Things (IoT) plays an increasingly important role, allowing various devices and objects to interact in real time. However, with an increase in the number of connected devices, there is a need to ensure reliable control of these systems. The Internet of Things (IoT) is the concept of a network of devices equipped with sensors and the ability to connect to the internet, which allows them to communicate and interact without direct human participation. IoT makes a significant contribution to improving efficiency, automation and improving the quality of life.In this paper, we systematically consider and analyze the current state of trust management for IoT. We propose a classification based on the tools, methods and technologies used to form trust management methods (collection of information for the formation of trust, calculation and storage of trust values). The article addresses the main issues of security and management in IoT, and also provides solutions that ensure the reliability and security of devices and data. In conclusion, it is concluded about the importance of trust management to ensure the safety and efficiency of IoT devices. We will try to help the reader understand current issues in this area, build a reliable management system and navigate the literature.

Key words: *attacks, Internet of Things(IoT), Security, Trust assessment, trust management, analytics.*

Авторлар туралы мәліметтер

Дана Жомартқызы Төлеген* – «Зияткерлік жүйелер және киберқауіпсіздік» департаментінің оқытушысы; Astana IT University, Қазақстан Республикасы, Астана қ.; e-mail: D.Tolegen@astanait.edu.kz.

Қымбат Жұмағұлқызы Сейлханова – «Зияткерлік жүйелер және киберқауіпсіздік» департаментінің оқытушысы; Astana IT University, Қазақстан Республикасы, Астана қ.; e-mail: K.Seilkhanova@astanait.edu.kz.

Асхат Мергенбайұлы Жеткербай – «Зияткерлік жүйелер және киберқауіпсіздік» департаментінің оқытушысы; Astana IT University, Қазақстан Республикасы, Астана қ.; e-mail: A.Zhetkerbay@astanait.edu.kz.

Сведения об авторах

Дана Жомартқызы Төлеген* – преподаватель департамента «Интеллектуальные системы и Кибербезопасность» ; Astana IT University, Республика Казахстан, г. Астана; e-mail: D.Tolegen@astanait.edu.kz.

Қымбат Жұмағұлқызы Сейлханова – преподаватель департамента «Интеллектуальные системы и Кибербезопасность»; Astana IT University, Республика Казахстан, г. Астана; e-mail: K.Seilkhanova@astanait.edu.kz.

Асхат Мергенбайұлы Жеткербай – преподаватель департамента «Интеллектуальные системы и кибербезопасность»; Astana IT University, Республика Казахстан, г. Астана; e-mail: A.Zhetkerbay@astanait.edu.kz.

Information about the authors

Dana Zhomartkyzy Tolegen* – teacher of the Department of Intelligent Systems and Cybersecurity; Astana IT University, Astana, Republic of Kazakhstan; e-mail: D.Tolegen@astanait.edu.kz.

Kymbat Zhumagulkyzy Seilkhanova – teacher of the Department of Intelligent Systems and Cybersecurity; Astana IT University, Astana, Republic of Kazakhstan; e-mail: K.Seilkhanova@astanait.edu.kz.
Askhat Mergenbaiuly Zhetkerbay – teacher of the Department of Intelligent Systems and Cybersecurity; Astana IT University, Astana, Republic of Kazakhstan; e-mail: A.Zhetkerbay@astanait.edu.kz.

Редакцияға енуі 17.01.2025
Өңдеуден кейін түсуі 04.04.2025
Жариялауға қабылданды 07.04.2025

https://doi.org/10.53360/2788-7995-2025-2(18)-2

МРНТИ: 81.93.29

С. Адилжанова, М. Кунелбаев, Д. Сыбанова*
Казахский национальный университет имени аль-Фараби,
050040 Республика Казахстан, г. Алматы, пр. аль-Фараби, 71
*e-mail:dsybanovaa@gmail.com

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА КИБЕРАТАК: ИССЛЕДОВАНИЕ НА ОСНОВЕ ДАТАСЕТА RT-IOT 2022

Аннотация: *Статья посвящена исследованию применения машинного обучения для анализа кибератак. В исследовании рассматриваются алгоритмы Random Forest, SVM и Logistic Regression, которые успешно справляются с задачами выявления аномалий и минимизации ложных срабатываний. Адаптация моделей к работе с несбалансированными данными, таких как использование LabelEncoder для категориальных признаков и StandardScaler для стандартизации данных, позволила значительно улучшить их производительность. На основе анализа данных из набора «Real-Time Internet of Things (RT-IoT 2022)» представлены результаты точности и устойчивости моделей. Основное внимание уделяется защите от киберугроз, включая утечки информации, DDoS-атаки и другие виды угроз. Анализ различных алгоритмов машинного обучения для исследования кибератак показал значимые результаты. Random Forest продемонстрировала наивысшую точность – 99,86%, обеспечивая высокую стабильность и эффективность в классификации различных видов угроз. SVM показала точность 99,29%, справляясь с большинством сложных классов. Logistic Regression продемонстрировала удовлетворительные результаты с точностью 97,71%, хотя в некоторых редких случаях точность была ниже. Таким образом, Random Forest и SVM продемонстрировали наилучшую эффективность для задач безопасности и анализа кибератак в цифровых системах, обеспечивая высокую точность и надежность. В дальнейшем планируется внедрение более сложных методов, таких как глубокое обучение, для более точного определения и анализа угроз.*

Ключевые слова: *Кибератака, алгоритмы машинного обучения,Random Forest, SVM, Logistic Regression, RT-IoT 2022, обнаружение атак.*

Введение

Данное исследование комбинирует правила обнаружения с методами машинного обучения для снижения Distributed Denial of Service (DDoS) атак в киберфизических производственных системах (CPPS), демонстрируя высокую точность и эффективность в реальном времени при обучении на реальном сетевом трафике [1]. Кроме того, предлагается гибридная глубокая нейронная сеть (DNN) для обнаружения и классификации DDoS атак в Software-Defined IIoT сетях, используя XGBoost для выбора признаков и сочетая CNN и LSTM сети. Этот подход обеспечивает высокую точность и низкую латентность, что критично для среды IIoT [2]. Для детекции аномалий в системах Индустрии 4.0 предлагается гибридная объединенная машина для обучения, включающая модели LOF, One-Class SVM и автоэнкодеры для повышения точности обнаружения. Эффективность системы подтверждается посредством оценок производительности на промышленных машинах [3]. Также представлен человеко-кибер-физический комплекс (HCPS) для реального времени обнаружения аномалий, объединяющий знания человека с киберфизическими системами для улучшения принятия решений, надежности системы и создания рабочих мест в Индустрии 5.0 [4]. Роль глубокого обучения в детекции мошенничества с использованием кредитных карт также анализируется, выделяя различные архитектуры и их влияние на улучшение точности детекции мошенничества, с фокусом на преодоление таких вызовов, как несбалансированность данных и переобучение [5]. Машинное обучение и глубокое обучение