Қазақстан Республикасы Тәуелсіздігінің 30 жылдығына арналған «Сейфуллин оқулары – 17: «Қазіргі аграрлық ғылым: цифрлық трансформация» атты халықаралық ғылыми – тәжірибелік конференцияға материалдар = Материалы международной научно – теоретической конференции «Сейфуллинские чтения – 17: «Современная аграрная наука: цифровая трансформация», посвященной 30 – летию Независимости Республики Казахстан.- 2021.- Т.1, Ч.4 - С.145-148

# ЗАТТАР ИНТЕРНЕТІ ТҮЙІНДЕРІН АУТЕНТИФИКАЦИЯЛАУ МӘСЕЛЕЛЕРІ

*Каженова Ж.С.,*

Заттар интернетіндегі (IoT) аутентификация әдістері компьютерлік индустрияның маңызды бөлігі болып табылады, өйткені IoT күнделікті өмірде көптеген құрылғыларға әсер етеді, сондықтан ондағы қолданушылар қорғалуы және шабуылдар мен заңсыз қолданушылар алдында осал болмауы өте маңызды [1, 2].

Аутентификация күнделікті терминдерде аутентификация үрдісінен өтпеген нысанның жеке басын өзі атағандай нысан екендігін анықтау, орнату ретінде сипатталады. Мысалы, төлқұжатты саяхатқа пайдаланған кезде сериялық нөмір оның заңды екендігіне тексеріліп, содан кейін куәландыратын адам оны көзімен көріп салыстырады. Сонымен қатар, аутентификация проблемасы Интернетте сәл қиындауы мүмкін, себебі желілер әрдайым өздері растайтын объектілерге физикалық қол жетімділікке ие бола бермейді. Шабуыл жасаушыларға аутентификация ұсынылған кезде үлкен проблема туындайды, шабуылдаушылар құпия ақпарат алуға, желіні / бағдарламаларды бұзуға, тіпті қызметтің жарамды қолданушылары ретінде көрсететін жалған деректерді ұсынуға тырысуы мүмкін [3].

IoT ортасында IoT соңғы түйіндеріндегі шектеу келесі аспектілерді қамтиды:

- есептеу қуаты, CPU (MCU), RAM;
- сақтау орны; желінің сыйымдылығы;
- пайдаланушы интерфейсінің және дисплейдің болмауы;
- электр қуатын тұтыну;

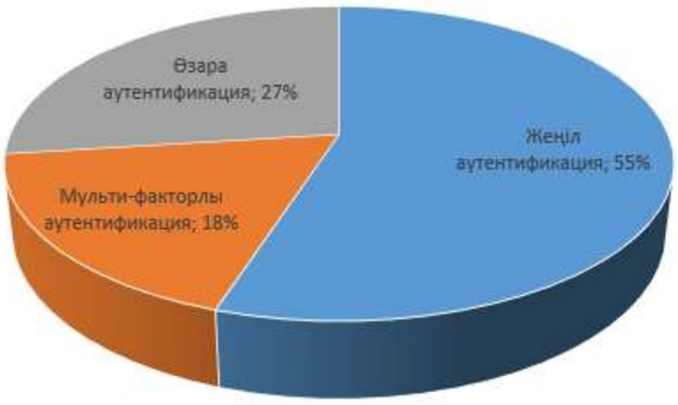
Аутентификация - IoT жүйелеріне шабуылдарды, мысалы, жауап шабуылдары, ортадағы адам шабуылдары, имитациялық шабуылдар және сибил сияқты шабуылдарды азайтудың бір әдісі. Қазіргі уақытта аутентификация қолданушыға қосымша деңгейдегі қол жетімділікті қамтамасыз ететін, сонымен бірге IoT желісіндегі құрылғыға қол жеткізуді қамтамасыз ететін ең танымал әдіс болып табылады (60%). Транстпорттық деңгей қауіпсіздігі (TLS) байланыс аутентификациясы мен шифрлауы үшін кеңінен қолданылады [4].

Арнайы шектелген құрылғылар үшін TLS алдын-ала ортақ кілттерді пайдаланатын TLS-PSK және RSA кілттермен алмасу және Diffie-Hellman (DH) ашық кілттер мен криптографиялық хаттамалар болып табылатын TLS-DHE-RSA аутентификация әдісін ұсынады. Бұл схемада өзара аутентификациялауды жүзеге асыруы керек екі нысан алдымен құпия ақпаратпен (алдын-ала ортақ кілттермен) алмасу арқылы бір-біріне заңдылығын дәлелдеуі керек. Аутентификация процесінде кілттердің тек симметриялық шифрлауы қолданылатындықтан, схема мүмкіндіктері шектеулі датчиктер сияқты құрылғыларға жарамды [5].

Қазіргі уақытта IoT үшін жасалған аутентификация хаттамаларының үш түрі бар: асимметриялық криптожүйеге негізделген хаттамалар, симметриялы криптожүйеге негізделген хаттамалар және гибридтік хаттамалар. IoT ортасындағы қолданушылар мен құрылғылар екі жақты байланыс жасайтын болғандықтан, құрылғы мен серверлер арасында өзара байланыс болады. Құрылғы серверге деректерді жібереді, сонымен қатар сервер жіберген басқару деректерін алады. Осылайша, құрылғының да, сервердің де жұмыс қабілеттілігін растау үшін өзара аутентификацияның IoT жүйесінде шешуші маңызы бар.

Соңғы кездерде жеңіл аутентификация мен шифрлауға үлкен сұраныс бар. Мақсаты - қол жетімділікті басқару және қауіпсіз байланыс үшін жеңіл аутентификациямен қамтамасыз ету [6].

Био-хэштеуді және анонимділікті қолданатын мультифакторлы аутентификация IoT аутентификациясы мақсатына жетудің басқа тәсілдері болып табылады [7]. IoT аутентификация әдістерінің қазіргі бағыттары 1-суретте ұсынылған [4].




Сурет 1. Аутентификация бағытындағы зерттеулер.

Жеңіл аутентификация - бұл заттар Интернетіндегі танымал аутентификация әдісі. Мысал ретінде қарастыратын болсақ, [8] -де машиналар арасындағы байланыс үшін жеңіл аутентификация әдісі туралы, яғни келесі өндірістік революция болуы керек өндірістік IoT ортадағы M2M байланысы туралы жазылған, бұл осы тапсырманы өте маңызды етеді. Ұсынылған идея болашақ өндіріс жүйелеріндегі шектеулерді алып тастай отырып, M2M

байланысын қамтамасыз ету үшін жеңіл аутентификация механизмін қолдану болды, байланыс құралдары интеллектуалды сенсор және қауіпсіздікті білдіретін сенімді платформа модулі бар маршрутизатор болды, бұл құрылғыларға кіріктірілген криптография процесі болып табылады.

Тіркеуді аяқтау үшін 3 қадамды орындау қажет болды. Біріншіден, олар зиянды тосқауылдың ықтималдығы ең төменгі деңгейге жету үшін әр ақылды сенсордың бірегей идентификаторды қауіпсіз арна арқылы аутентификация серверлеріне (AS) жіберуін қамтамасыз етуі керек еді. Келесі қадам AS процестің әрбір бірегей параметрін есептейтін етіп ақпарат алу қажеттілігіне байланысты біріншіден кейін жасалады. Орындаған есептеу сенсор идентификаторы мен AS арасындағы байланысты құру болып табылады. Бұл байланыс орнатылғаннан кейін, AS оларды ақылды датчикте сақтайтын параметрлерді жібереді. Бұл бөлік өндірістік IoT үшін жеңіл аутентификация жасау үшін қалған жұмыс процесі үшін өте маңызды.

Енді әрбір интеллектуалды сенсор маршрутизаторда аутентификациядан өте алады. Содан кейін аутентификацияның негізгі кезеңдері тіркеу кезеңінен кейін өңделді. Осы қадамдарды орындау кезінде өзара аутентификация қолданылды. Біріншіден, интеллектуалды сенсор кездейсоқ санды жасайды және оны қорғаныс элементінде сақтайды. Қол жеткізілгеннен кейін ол 1-хабарламаны құруды жалғастырады, ол XOR-хэш функциясы жасақтаған кездейсоқ саннан, сонымен қатар хэш функциясының шифрлауын пайдаланып жасалған id идентификаторы псевдонимінен тұрады. Содан кейін 2-хабарлама жасалды, оның құрамында қазіргі уақытта жасалған барлық ақпарат бар шифрланған хабарлама бар. Екінші қадам маршрутизатор туралы барлық ақпаратпен хабарлама алғандай қарапайым. 3-хабарлама алғаннан кейін маршрутизатор алдын-ала жалпы кілт арқылы дешифрлайды. Алдын ала жалпы кілт қолдану - маршрутизатордың шифрлау кілтін беру үшін жасаушылардың көптеген әдістерінің бірі. Шифрланғаннан кейін маршрутизатор дұрыс ақпараттың алынғанын тексереді, яғни хабарлама 2 декодталғаннан кейін, ол құрылған хэш функцияларына сәйкес келеді ме? Егер олар сәйкес келсе, сіз аутентификацияның келесі сатысын бастай аласыз. Егер олар сәйкес келмесе, сұрау жойылады. Процесс жалғасып, келесі қадам қосымша ақпаратты сенсорға қайта жібереді, онда олар ортақ кілттер жасайды. Содан кейін сенсор басқа хабарлама жібереді, соның ішінде маршрутизатор туралы ақпарат алғаннан кейін жалпы кілт жібереді; Оның есептелген теңдеулермен сәйкестігін тексеру керек. Егер бәрі сәйкес келсе, сенсордың жарамды кілті бар және аутентификация процесі аяқталғанын дәлелдейді [8].

IoT ортасында түйіндер мен инфрақұрылым түйіні арасындағы байланыс жүктемені азайту үшін ашық кілтті қолдану арқылы кілттерді таратудың қарапайым әдісін қажет етеді; дегенмен, бұл әдісті Advanced Encryption Standard (AES), RSA, Elliptic Curve Cryptography (ECC) сияқты шифрлау модулі орнатыла алмайтын жеңіл құрылғыға қолдану қиын. Internet Engineering Task Force (IETF) IP желілерінде қабылданған Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), IPSec және т.б. қолдануды қарастыруда. Негізгі тұжырымдама DTLS-ді IoT-тегі негізгі

протокол болып табылатын Шектелген қолдану хаттамасына (CoAP) қолдану болып табылады.

Симметриялы кілт жүйесі хабарламаның таралуы, сақталуы және өңделуі кезінде құпиялылығын қамтамасыз ету үшін қолданылады. Симметриялы кілт алгоритмі екі немесе одан да көп тараптар қолданатын бір кілт негізінде шифрлау / дешифрлеу операцияларын орындайды. Симметриялы криптографияның қиындығы - кодтаушыдан декодерге қауіпсіз кілтті жеткізу қауіпсіздікке қауіп төндіруі мүмкін. Симметриялық кілтке қол жеткізген кез-келген адам хабарламаның өзгертілгендігін алушының білместен хабарламаға қол жеткізе / өзгерте / жібере алады. Осы мәселелерді шешу үшін ашық кілт криптографиясы немесе асимметриялық кілт криптографиясы жасалды. Симметриялық криптографиялық алгоритмдер әдетте ағын шифрлары мен блоктық шифрларға топтастырылады. AES - желілік қауіпсіздік шешімдерінде кеңінен қолданылатын блоктық шифрлау алгоритмі.

IoT аутентификациясын дұрыс енгізу IoT қауіпсіздігі үшін көптеген артықшылықтарға ие. Алайда дұрыс әдісті таңдау қиынға соғуы мүмкін, ал дұрыс емес әдісті таңдау тәуекелді он есе арттыруы мүмкін.

Симметриялық кілтті құрылғыға қауіпсіз сақтау және кілттерді сақтаудың озық тәжірибелерін қолдану арқылы кейбір қауіптерді азайтуға болады. Бұл мүмкін, бірақ симметриялы кілттер ғана қолданылған кезде, олар асимметриялық криптографиялық енгізулерге қарағанда қауіпсіз бола алмайды.

## Әдебиеттер тізімі


1. Atwady, Y. and Hammoudeh, M. (2017). A survey on authentication techniques for the internet of things. In Proceedings of the International Conference on Future Networks and Distributed Systems, ICFNDS ’17, New York, NY, USA. ACM.

2. Aloraini, A. and Hammoudeh, M. (2017). A survey on data confidentiality and privacy in cloud 451 computing. In Proceedings of the International Conference on Future Networks and Distributed 452 Systems, ICFNDS ’17, pages 10:1–10:7, New York, NY, USA. ACM.

3. Lopez-Research (2017). An introduction to the internet of things (iot). https: //www.cisco.com/c/dam/en_us/solutions/trends/iot/introduction_to_IoT_november .pdf. Accessed: 15-01-2018.

4. Current research on Internet of Things (IoT) security: A survey. Mardiana binti Mohamad Noor, Wan Haslina Hassan Computer Systems and Networks (CSN), Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Kuala Lumpur Computer Networks Volume 148, 15 January 2019, Pages 283-294

5. T. Shinzaki, I. Morikawa, Y. Yamaoka, Y. Sakemi, IoT security for utilization of big data: Mutual authentication technology and anonymization technology for positional data, Fujitsu Sci. Tech. J. 52 (4) (2016) 52–60.

6. F. Wu, X. Li, L. Xu, S. Kumari, M. Karuppiah, J. Shen, A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server, Comput. Electr. Eng. 63 (2017) 168–181.

7. S. Shin, T. Kwon, Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks, IEEE Access 6 (2018) 11229–11241.

8. Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M., Schmittner, C., and Bastos, J. (2017). A lightweight authentication mechanism for m2m communications in industrial iot environment. IEEE Internet of Things Journal.