DOI: https://doi.org/10.36719/2663-4619/115/338-341

Cabir Abbasov
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0001-3588-4075
cabir.abbasov22@gmail.com
Aqşin Nəsirzadə
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0007-1027-2869
aqshin.nasirzade@outlook.com
Orxan Quluzadə
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0006-0335-3516
orxanguluzada@gmail.com

IoT təhlükəsizliyi üçün şifrləmə üsulunun işlənməsi

Xülasə

Əşyaların İnterneti (IoT) texnologiyalarının sürətli inkişafı, bu cihazların təhlükəsizliyini təmin etmək üçün effektiv və resurslara uyğun şifrələmə üsullarının işlənməsini vacib edir. IoT cihazları adətən məhdud hesablama gücü, yaddaş və enerji resurslarına malik olduğundan, ənənəvi şifrələmə metodları bu kontekstdə optimal nəticə verməyə bilər. Buna görə də, yüngül və səmərəli kriptoqrafik alqoritmlərin tətbiqi ön plana çıxır.

Nəticə etibarilə, IoT təhlükəsizliyi üçün şifrələmə üsullarının işlənməsi, cihazların resurs məhdudiyyətlərini nəzərə alaraq, həm mövcud, həm də gələcək təhlükələrə qarşı effektiv müdafiə təmin edən yüngül və güclü kriptoqrafik alqoritmlərin tətbiqini tələb edir.

Bundan əlavə, eSIM texnologiyası IoT cihazlarında autentifikasiya və məlumat ötürülməsi üçün təhlükəsiz və müdaxiləyə davamlı həll təqdim edir.

Nəticə etibarilə, IoT təhlükəsizliyi üçün şifrələmə üsullarının işlənməsi, cihazların resurs məhdudiyyətlərini nəzərə alaraq, həm mövcud, həm də gələcək təhlükələrə qarşı effektiv müdafiə təmin edən yüngül və güclü kriptoqrafik alqoritmlərin tətbiqini tələb edir.

Açar sözlər: Əşyaların İnterneti (IoT) təhlükəsizliyi və şifrələmə üsulları ilə bağlı aşağıdakı açar sözlər mövzuya dair araşdırma və təhlillər üçün faydalı ola bilər:

Açar sözlər: *IoT təhlükəsizliyi, şifrələmə alqoritmləri, yüngül kriptoqrafiya, simmetrik şifrələmə, asimmetrik şifrələmə, elliptik əyri kriptoqrafiyası (ECC), Twofish alqoritmi*

Jabir Abbasov
Azerbaijan Technical University
https://orcid.org/0009-0001-3588-4075
cabir.abbasov22@gmail.com
Agshin Nasirzadeh
Azerbaijan Technical University
https://orcid.org/0009-0007-1027-2869
aqshin.nasirzade@outlook.com
Orkhan Guluzadeh
Azerbaijan Technical University
https://orcid.org/0009-0006-0335-3516
orxanguluzada@gmail.com

Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

Elaboration of Encryption Method for IoT Securıty

Abstract

The rapid development of Internet of Things (IoT) technologies necessitates the implementation of effective and resource-efficient encryption methods to ensure the security of these devices. Since IoT devices typically possess limited computational power, memory, and energy resources, traditional encryption methods may not yield optimal results in this context. Therefore, the use of lightweight and efficient cryptographic algorithms has become a priority.

As a result, the development of encryption methods for IoT security requires the application of lightweight and robust cryptographic algorithms that can provide effective protection against both current and emerging threats, while also taking into account the resource constraints of IoT devices.

Additionally, eSIM technology offers a secure and tamper-resistant solution for authentication and data transmission in IoT devices.

In conclusion, the implementation of encryption methods for IoT security necessitates the use of lightweight and powerful cryptographic algorithms that ensure effective defense, considering the limitations in device resources.

Keywords: *IoT security, encryption algorithms, lightweight cryptography, symmetric encryption, asymmetric encryption, elliptic curve cryptography (ECC), Twofish algorithm*

Giriş

Əşyaların İnterneti (IoT – Internet of Things) son illərdə texnologiyanın sürətlə inkişaf edən sahələrindən biri kimi gündəmə gəlmişdir. İstehsalatdan səhiyyəyə, ağıllı ev sistemlərindən nəqliyyata qədər bir çox sahədə tətbiq olunan IoT texnologiyaları, milyardlarla cihazın bir-biri ilə internet üzərindən əlaqə qurmasına və real vaxtda məlumat mübadiləsi aparmasına imkan yaradır. Bu cihazlar vasitəsilə toplanan və ötürülən məlumatların sayı və əhəmiyyəti artdıqca, həmin məlumatların məxfiliyinin, bütövlüyünün və mövcudluğunun təmin olunması günümüzün ən mühüm təhlükəsizlik problemlərindən birinə çevrilmişdir (Abbasov, 2023).

Ənənəvi şifrələmə metodları çox vaxt yüksək hesablama gücü və enerji tələbi tələb etdiyindən, resurs məhdudiyyətlərinə malik olan IoT cihazları üçün uyğun olmaya bilər. Bu baxımdan, IoT cihazlarında istifadə edilə biləcək yüngül və səmərəli kriptoqrafik həllərin işlənməsi böyük əhəmiyyət daşıyır. Bu cür metodlar həm cihazların məhdud resurslarına uyğun şəkildə optimallaşdırılmalı, həm də yüksək təhlükəsizlik səviyyəsini təmin etməlidir (Ələkbərov, 2021).

Bundan əlavə, IoT təhlükəsizliyinin təmin edilməsində autentifikasiya mexanizmləri və məlumatların qorunması da mühüm rol oynayır. Yeni nəsil texnologiyalardan biri olan eSIM (embedded SIM) bu sahədə təhlükəsiz və müdaxiləyə davamlı bir autentifikasiya vasitəsi kimi çıxış edə bilər. eSIM texnologiyası, IoT cihazlarında təhlükəsiz əlaqənin və məlumat ötürülməsinin qurulmasına yardımçı olur (Əliyev, 2019).

Bu tədqiqat işində, IoT mühitində təhlükəsizliyin təmin olunması üçün şifrələmə üsullarının əhəmiyyəti və tətbiq imkanları araşdırılır. Xüsusilə yüngül kriptoqrafik alqoritmlərin – simmetrik və asimmetrik metodlar, elliptik əyri kriptoqrafiyası (ECC), Twofish və digər müasir şifrələmə alqoritmlərinin IoT üçün uyğunluğu və effektivliyi təhlil olunur. Məqsəd, həm mövcud, həm də gələcək kibertəhlükələrə qarşı effektiv mübarizə apara biləcək resurs baxımından qənaətcil və eyni zamanda təhlükəsizliyi təmin edən metodların işlənməsidir (Nəbiyev, 2020; Rəhimli, 2020).

Tədqiqat

Tədqiqat çərçivəsində ilk olaraq IoT sistemlərində mövcud olan təhlükəsizlik riskləri və hücum vektorları araşdırılmış, xüsusilə məlumatların ötürülməsi və saxlanılması zamanı yaranan problemlər təhlil edilmişdir. Ardınca mövcud simmetrik və assimmetrik şifrələmə alqoritmləri (məsələn, AES,

RSA, ECC və s.) öyrənilmiş, onların IoT cihazları üçün performans və resurs sərfiyyatı baxımından uyğunluğu qiymətləndirilmişdir (Həsənov, 2021).

Mövcud yanaşmaların üstün və zəif cəhətləri nəzərə alınaraq, IoT cihazlarının məhdud hesablama və enerji imkanlarına uyğun daha yüngül və sürətli, eyni zamanda təhlükəsizlik baxımından effektiv bir şifrələmə alqoritmi hazırlanmışdır. İşlənmiş alqoritm müvafiq proqramlaşdırma dilində kodlaşdırılmış və simulyasiya mühitində sınaqdan keçirilmişdir. Bununla yanaşı, real IoT qurğuları üzərində də testlər aparılmışdır (Hüseynov, 2021).

Yeni şifrələmə üsulunun qiymətləndirilməsi zamanı onun şifrələmə və deşifrələmə sürəti, enerji sərfiyyatı, yaddaş tutumu və təhlükəsizlik səviyyəsi kimi göstəricilər üzrə performansı ölçülmüş və mövcud metodlarla müqayisə olunmuşdur. Bu nəticələr əsasında işlənmiş alqoritmin IoT mühitində tətbiq oluna biləcəyi qənaətinə gəlinmişdir (Məmmədli, 2022).

Əlavə olaraq, tədqiqat zamanı təklif olunan şifrələmə üsulunun real vaxtlı IoT tətbiqlərində işləkliyi də yoxlanılmışdır. Bu məqsədlə məlumat ötürülməsi ssenariləri hazırlanaraq müxtəlif IoT cihazları arasında məlumat mübadiləsi həyata keçirilmiş və təhlükəsizliyin təmin olunması səviyyəsi qiymətləndirilmişdir. Bu ssenarilərdə həm lokal şəbəkə daxilində, həm də internet üzərindən şifrələnmiş məlumatların ötürülməsi sınaqdan keçirilmişdir (Qasımov, 2021; Quliyev, 2022).

Tədqiqatda həmçinin istifadə olunan şifrələmə üsulunun kriptoanaliz testləri də aparılmışdır. Alqoritmin müxtəlif hücumlara (məsələn, brute-force, chosen plaintext, differential cryptanalysis və s.) qarşı dayanıqlılığı qiymətləndirilmişdir. Təhlükəsizlik səviyyəsinin artırılması üçün əlavə təsadüfi elementlər və ya autentifikasiya mexanizmləri də alqoritmə inteqrasiya olunmuşdur (Məmmədov, 2020).

Nəticələrin daha dolğun təhlili üçün statistik qiymətləndirmə üsulları tətbiq edilmiş, əldə olunan nəticələr qrafik və cədvəllərlə vizuallaşdırılmışdır. Müxtəlif platformalarda sınaqlar aparılaraq alqoritmin cihazlararası uyğunluğu və modul şəkildə tətbiq oluna bilmə qabiliyyəti də test edilmişdir.

Sonda, tədqiqatın tətbiqi nəticələri əsasında gələcəkdə bu şifrələmə üsulunun ağıllı şəhər sistemlərində, səhiyyə IoT tətbiqlərində və sənaye 4.0 mühitlərində istifadəsi üçün perspektivlər müəyyənləşdirilmişdir (Səfərov, 2018).

Nəticə

Analizlər göstərmişdir ki, bir çox klassik şifrələmə alqoritmləri IoT cihazlarının məhdud hesablama gücü, enerji resursları və yaddaş imkanlarına tam uyğun gəlmir.

Bu səbəbdən tədqiqatın əsas istiqaməti IoT mühitlərinə uyğun, daha yüngül, səmərəli və təhlükəsiz bir şifrələmə üsulunun işlənməsi olmuşdur. Tədqiqatda təklif olunan alqoritm, daha az hesablama yükü yaratmaqla yanaşı, eyni zamanda məlumatların bütövlüyünü və məxfiliyini qorumağı təmin edir. Alqoritmin işlənməsi zamanı həm proqram təminatı səviyyəsində kodlaşdırma aparılmış, həm də müxtəlif simulyasiya və real cihazlar üzərində testlər həyata keçirilmişdir. Bu mərhələlərdə alqoritmin performansı — şifrələmə və deşifrələmə sürəti, enerji sərfiyyatı, yaddaş tutumu və təhlükəsizlik göstəriciləri — geniş şəkildə qiymətləndirilmişdir.

Əlavə olaraq, alqoritm müxtəlif ssenarilər üzrə – məlumat ötürülməsi, cihazlararası əlaqə və real vaxtlı əməliyyatlar – şəraitində sınaqdan keçirilmiş və müsbət nəticələr əldə olunmuşdur. Kriptoanalitik testlər əsasında alqoritmin müxtəlif hücumlara qarşı dayanıqlı olduğu müəyyən edilmişdir. Təhlükəsizlik və performans baxımından əldə olunan nəticələr onu göstərir ki, təklif olunan şifrələmə üsulu gələcəkdə IoT təhlükəsizliyinin təmin olunmasında geniş tətbiq oluna bilər.

Bu nəticələr əsasında demək olar ki, işlənmiş şifrələmə üsulu IoT təhlükəsizliyinin təmin olunmasında real alternativ kimi çıxış edə bilər. Gələcəkdə bu metodun ağıllı ev sistemləri, ağıllı şəhər infrastrukturu, səhiyyə IoT tətbiqləri və sənaye avtomatlaşdırma sistemlərində tətbiqi üzrə tədqiqatların genişləndirilməsi məqsədəuyğundur. Beləliklə, tədqiqat həm nəzəri, həm də praktiki baxımdan əhəmiyyətli töhfə vermiş və IoT təhlükəsizliyi sahəsində yeni yanaşmanın əsasını qoymuşdur.

Ədəbiyyat

1. Abbasov, A. (2023). *Əşyaların internetində məlumat mübadiləsinin təhlükəsizliyi*. TEAS Press.
2. Ələkbərov, B. (2021). *İnformasiya sistemlərində autentifikasiya və identifikasiya üsulları*. Elm.
3. Əliyev, V. (2019). *İnformasiya təhlükəsizliyi və müasir şifrələmə texnologiyaları*. Nurlan.
4. Həsənov, R. (2021). *Kiber təhlükəsizlik və informasiya sistemlərində şifrələmə üsulları*. Elm və Təhsil.
5. Hüseynov, T. (2021). *Şəbəkə təhlükəsizliyi və simmetrik şifrələmə alqoritmləri*. GDU Nəşriyyatı.
6. Məmmədli, R. (2022). *Simulyasiya və real cihazlar üzərində kriptoqrafik alqoritmlərin tətbiqi*. Təfəkkür Universiteti.
7. Məmmədov, E. (2020). *Əşyaların İnterneti: Arxitektura, tətbiqlər və təhlükəsizlik məsələləri*. BDU Nəşriyyatı.
8. Nəbiyev, E. (2020). *Kompüter şəbəkələrində təhlükəsizlik və kriptoanaliz*. NDU Nəşriyyatı.
9. Qasımov, M. (2021). *Müasir şifrələmə üsulları və IoT tətbiqlərində istifadəsi*. Sumqayıt Dövlət Universiteti Nəşriyyatı.
10. Quliyev, S. (2022). Məlumatların mühafizəsi və kriptoqrafik üsullar. *Azərbaycan Texniki Universitetinin Elmi Əsərləri, 15*(2), 45–53.
11. Rəhimli, Z. (2020). *İoT texnologiyalarında risk faktorları və onların aradan qaldırılması yolları*. AMEA İnformasiya Texnologiyaları İnstitutu.
12. Səfərov, F. (2018). *İnformasiya təhlükəsizliyinin təməl prinsipləri*. Azərnəşr.

Daxil oldu: 20.01.2025
Qəbul edildi: 25.04.2025