Fərdi məlumatların təhlükəsizliyinin təminatı üçün müasir metodlar

Aytən İsmayılqızı
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
aytan.ismayil@gmail.com

***Xülasə*— Sosial qarşılıqlı münasibətlər getdikcə daha çox şəbəkə üzərindən yaradılır – sosial platformalarda yaranmış yeni imkanlar, süni intellektin tətbiqinə əsaslanan sistemlər, eyni zamanda fərdi məlumatların gizliliyi üçün yeni risklər yaradır. Bu baxımdan fərdi məlumatların təhlükəsizliyi priotet məsələ olaraq qalır. Məqalədə fərdi məlumatların təhlükəsizliyinin təminatı üçün istifadə olunan bəzi müasir metodlar araşdırılmış və onların üstün və mənfi cəhətləri analiz edilmişdir.**

Açar sözlər— fərdi məlumatlar, məlumatların təhlükəsizliyi, süni intellekt, machine learning, privacy preserving machine learning

I. GİRİŞ

Fərdi məlumatlar – şəxsin kimliyini birbaşa və ya dolayısı ilə müəyyənləşdirməyə imkan verən istənilən məlumatlardır [1]. Təhlükəsizlik hər zaman fərdi məlumatların konfidensiallığının, tamlığının, əlyetərliyinin qorunması üçün diqqət mərkəzində olmuşdur. Demək olar ki, həyatımızın hər bir hissəsi məlumat ətrafında fəaliyyət göstərir. Sosial media şirkətlərindən tutmuş, banklara, satıcılara, hökümətə qədər – demək olar ki, istifadə etdiyimiz hər bir xidmət şəxsi məlumatların toplanması və təhlilini əhatə edir. Adımız, ünvanımız, bank nömrəmiz və başqa şəxsi məlumatlarımız şirkətlər tərəfindən toplanılır və analiz edilir. Belə şəraitdə fərdi məlumatların qorunmasının vacibliyi artır. Təqdim olunan iş bu sahədə tədqiqat məsələlərini dəqiqləşdirmək məqsədilə fərdi məlumatların təhlükəsizliyini təmin etmək üçün yeni metodların analizinə həsr olunmuşdur.

II. GDPR-İN TƏMƏL PRİNSİPLƏRİ

İnternet və mobil tətbiqlərin, süni intellektin və “Əşyaların İnterneti”nin (Internet of Things) inkişafı ilə yeni yaranmış sistem zəifliklərini və kiberhücum risklərini nəzərə alaraq fərdi məlumatların təhlükəsizliyinə ehtiyac hər zamankından daha çoxdur. Fərdi məlumatların qorunması üçün ilk növbədə hüquqi təminat lazimdir [2]. GDPR – General Data Protection Regulation (Verilənlərin Qorunması üzrə Əsas Qanun) Avropanın rəqəmsal konfidensiallıq qanunvericiliyinin əsaslarını təşkil edir. 2012-ci ilin yanvar ayında Avropa Komissiyası Avropanı “rəqəmsal əsrə uyğun” etmək üçün Avropa Birliyi daxilində məlumatların qorunması islahatları planlarını hazırladı. 4 ildən sonra bunun nəyə və necə tətbiq olunacağına dair razılıq əldə edildi. GDPR Avropa Birliyi vətəndaşlarına öz fərdi məlumatlara daha çox nəzarət etmək üçün hazırlanmış yeni qaydalar toplusudur. O, həm Avropa Birliyi daxilindəki vətəndaşlar, həm də müəssisələrin rəqəmsal iqtisadiyyatdan tam faydalana bilməsi üçün tənzimlənmə mühitini asanlaşdırmaq məqsədi daşıyır. İslahatlar hazırda yaşadığımız dünyanı əks etdirmək üçün hazırlanmışdır və İnternet əlaqəli bağlantıları sürətləndirmək üçün Avropa daxilindəki fərdi məlumatlar üzərinə konfidensiallıq və razılıq əhatəsində qanunlar və öhdəliklər gətirir.

GDPR-ə görə Avropa Birliyi vətəndaşlarının fərdi məlumatlarının emalı ilə məşğul olan bütün təşkilatlar aşağıdakı razılaşmalara əməl etməlidir [3]:

1. Təşkilat fərdii məlumatları toplayarkən toplanmış məlumatların harada istifadə olunacağını bildirməlidir. Məlumatlar üçüncü tərəflərlə bölüşdürülməsini ehtiva edən başqa bir məqsəd üçün istifadə edilə bilməz.

2. Layihə və ya proses üçün yalnız minimum miqdarda məlumat toplamaq lazımdır. Məlumat yalnız məhdud müddətdə saxlanılmalıdır.

3. Təşkilat şəxslərə özləri haqqında hansı məlumatların olduğunu və bununla əlaqədar nələr edildiyini izah etməlidir.

4. Təşkilat tələb olunduğu zaman şəxsin fərdi məlumatlarını dəyişdirməli və ya ləğv etməlidir.

5. Fərdi məlumatlar insanlar haqqında avtomatlaşdırılmış qərarlar üçün istifadə edildikdə, təşkilat qərar qəbuletmə prosesinin arxasındakı məntiqi izah etməlidir.

III. BƏZİ METODLAR HAQQINDA

GDPR fərdi məlumatların təhlükəsizliyinin təminatı üçün 6 effektiv metod təklif etmişdir:

1. Riskin qiymətləndirilməsi
2. Ehtiyat nüsxələr (ing. Backups)
3. Şifrləmə
4. Psevdonimləşdirmə
5. Girişə nəzarət
6. Məhvetmə (ing. Destruction)

1.Riskin qiymətləndirilməsi – Məlumatlar nə qədər həssas olarsa, o qədər ciddi mühafizə edilməlidir. Təhlükə riski az olan informasiya daha az qorunma tələb edir. Bu baxımdan riskin qiymətləndirilməsi önəmlidir, çünki güclü mühafizə daha çox xərc tələb edir. Riskin qiymətləndirilməsində 2

DOI: 10.25045/NCInfoSec.2019.43

istiqamət oxu üzrə dəyərləndirmə aparılır: məlumat pozuntusu halında potensial təhlükə və pozuntu ehtimali. Bu oxlar üzrə risk nə qədər yüksək olarsa, məlumat o qədər həssas sayılır [4].

2. Ehtiyat nüsxələr – Ehtiyat nüsxələr texniki nasazlıq və ya istifadəçi ehtiyatsızlığı ucbatından baş verə biləcək məlumat itkisinin qarşısını almaq üçün istifadə olunur.

3. Şifrləmə – GDPR-də şifrləmə fərdi məlumatların təhlükəsizliyini təmin etmək üçün mümkün olan bir texniki və təşkilati tədbir olaraq açıq şəkildə qeyd edilmişdir. Məlumatların emalı ilə əlaqədar risklər nə qədər yüksək olarsa, təhlükəsizlik tədbirləri daha güclü olmalı və daha çox tədbirlər görülməlidir. Yüksək əhəmiyyətli məlumatların hər addımda şifrlənməsi ilə daha yüksək təhlükəsizliyə nail olmaq olar. Ancaq GDPR sürətlə inkişaf edən texnoloji tərəqqi üçün şifrləmə üsullarını qeyd etmir [5].

4. Psevdonimləşdirmə – Şəxslərin adları təsadüfi yaradılan sözlər (sətirlər) ilə əvəz edilir. Buna görə bir şəxsin şəxsiyyəti ilə verdikləri məlumatları bir-birinə bağlamaq mümkün olmur. İnsanları təxəllüs məlumatlarından birbaşa tanıya bilmədikləri üçün məlumatların pozulması və ya itkisi halında prosedurlar daha sadədir və risklər azaldılır.

Təxəllüs nümunəsi kimi bir kompüter sistemində adlar, ünvanlar və doğum tarixləri kimi şəxsiyyəti müəyyənləşdirən məlumatların məlumat bazasının saxlanılmasını misal göstərə bilərik. Bu zaman ayrıca bir kompüter sistemində, onları uyğunlaşdırmaq üçün şifrəli kodlarla birlikdə, kredit tarixi, tibbi sənədlər və s. kimi fərdi məlumatlar saxlanılır.

5. Girişə nəzarət – Şirkətin məlumat axınına girişə nəzarət mexanizmlərinin tətbiqi çox səmərəli risk azaldılması metodudur. Belə ki, məlumatların miqdarı nə qədər az olarsa, məlumatların pozulması və ya itməsi riski o qədər azdır. Həssas məlumatlara giriş icazəsi yalnız daxil olmaq üçün əsaslı bir səbəbi olan etibarlı işçilərə verilməsi təmin edilməlidir. Xüsusilə, yeni işçilər işə götürüldükdən sonra mütəmadi olaraq məlumatlandırma kurslarına cəlb edilməli və sistemdə yeniləmələr yerinə yetirilməlidir.

6. Məhvetmə – Əlinizdə olan məlumatların məhv edilməli olduğu bir vaxt gələ bilər. Məlumatların məhv edilməsi ilk baxışdan qorunma metodu kimi görünməsəs də, əslində belədir. Məlumatlar bu şəkildə icazəsiz bərpa və girişlərdən qorunur. GDPR-a əsasən ehtiyacınız olmayan məlumatları silmək öhdəliyiniz var və həssas məlumatlar daha geniş məhvetmə üsullarına zəmanət verir.

IV. MAŞIN TƏLİMİ VƏ FƏRDİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

Axtarış sorğularımız, satınalma əməliyyatları, izlədiyimiz videolar gündəlik olaraq toplanan və saxlanan məlumatların yalnız kiçik bir hissəsidir. Bu kimi fərdi məlumatlar müxtəlif Maşın təlimi (MT, ing. Machine Learning) tətbiqlərində istifadə olunur. Belə fərdi məlumatlar mərkəzləşdirilmiş yerlərə yüklənilir, onlardan maşın təlimi alqoritmləri yaradılır və həmin alqoritmlər əsasında modellər düzəldilir [6]. Həmin fərdi məlumatlara olan təhlükələr təkcə məlumat mərkəzləri və şirkətlərə hakerlər hücum edən zaman ortaya çıxan problemlərlə məhdudlaşmır. Əlavə olaraq yaranan təhlükə ondan ibarətdir ki, MT modelləri üçün istifadə olunan fərdi məlumatlar anonim olsa da, emal zamanı müəyyən xətalar (alqoritmdəki, operatorun səhlənkarlığı və s.) nəticəsində kənara sıza bilər. Əsas məqsəd MT və fərdi məlumatların təhlükəsizliyi texnologiyaları arasındakı boşluğu doldurmaqdır [7,8]. Bunun üçün Privacy-Preserving Machine Learning (PPML, Gizliliyi qoruyan maşın təlimi) anlayışı daxil edilmişdir. PPML-ə nail olmaq üçün bir sıra üsullar mövcuddur. Bunlardan ən geniş istifadə edilənləri homomorf şifrləmə, sirr paylaşımı (ing. secret sharing), təhlükəsiz prosessorlar (ing. secure processors) hesab edilir.

Təhlükəsiz prosessorlar – Intel SGX kimi prosessorlar əvvəllər həssas kodun daha yüksək imtiyaz səviyyələrində konfidensiallığını və tamlığını təmin etmək üçün təqdim edilsə də, gizliliyin qorunması hesablamalarında da istifadə olunur [6]. Hazırda bəzi MT alqoritmləri SGX prosessorlarına əsaslanır. Əsas ideya ondan ibarətdir ki, bu sistemlərdə hər bir məlumat sahibi müstəqil olaraq anklav (kod və məlumatları saxlayan sahə) vasitəsi ilə təhlükəsiz kanal qurur, özlərini autentifikasiya edir, buluddakı MT kodunun tamlığını yoxlayır və fərdi məlumatları təhlükəsiz şəkildə anklava yükləyir. Bütün məlumatlar yükləndikdən sonra MT tapşırığı təhlükəsiz prosessor tərəfindən yerinə yetirilir və nəticələr autentifikasiya edilmiş kanallar vasitəsilə lazımi tərəflərə göndərilir.

MT həyata keçirərkən fərdi məlumatları qorumaq üçün yuxarıda göstərilən üsullara baxmayaraq, məlumatların təhlükəsizliyini təmin etməyən MT alqoritmləri hələ də mövcuddur və geniş istifadə edilir. Bu baxımdan mövcud qanunlara əsasən şirkətlər istifadəçilərə öz fərdi məlumatlarının toplanması haqqında məlumatlandırılmaq və hətta bundan imtina etmək seçimi verməlidir.

NƏTİCƏ

Dövrümüz Süni İntellekt inqilabına şahid olduğu bir zamanda fərdi məlumatların təhlükəsizliyinin təminatında ənənəvi üsullar özünü doğrultmur. İnternetin və şəbəkələrin mürəkkəbləşən, artan istifadəsi hücum edənlərin sistemdəki boşluqları istismar etmək imkanlarını artırır. Təhlükəsizlik üzrə ənənəvi qaydalara əsaslanan vasitələr bütün mümkün ola biləcək təhlükələrin öhdəsindən gəlməyə qadir deyil. Maşın təliminin tətbiqinə əsaslanan texnologiyalar yaradılarkən fərdi məlumatların təhlükəsizliyi də nəzərə alınmalı və onu pozmayan alqoritmlər və üsullar işlənməlidir.

İSTİNADLAR

[1] Fərdi məlumatlar haqqında Azərbaycan Respublikasının Qanunu. 11 may 2010-cu il.

[2] Y. İmamverdiyev, “Big Data və fərdi məlumatların təhlükəsizliyi,” “Big data: imkanları, multidissiplinar problemləri və perspektivləri” I respublika elmi-praktiki konfransı, s. 109-113, 2016.

[3] https://eugdpr.org/the-regulation/

[4] N. Fabiano, “Ethics and the protection of personal data,” 10th International Multi-Conference on Complexity, Informatics and Cybernetics, 2019.

[5] C.Tikkinen-Piri, A.Rohunen, J.Markkula, “EU General Data Protection Regulation: Changes and implications for personal data collecting companies,” Computer law and security review, Vol. 34, No 1, 2018, pp. 134-153.

[6] M. Al-Rubaie, J. M. Chang, “Privacy-preserving machine learning: Threats and solutions,” IEEE Security and Privacy, Vol. 17, No 2, 2019.

[7] P.Mohassel, Y.Zhang, “SecureML: A system for scalable privacy-preserving machine learning,” IEEE Symposium on Security and Privacy, 2017.

[8] B.J.Chiphers, A system for privacy-preserving machine learning on personal data. MSc dissertation, Massachusetts Institute of Technology, 2017, 86 p.

NEW METHODS FOR PROVIDING SECURITY OF PERSONAL DATA

Aytan Ismayil gizi

Institute of Information Technology of ANAS, Baku, Azerbaijan

aytan.ismayil@gmail.com

Abstract— Social interactions are increasingly created over the network – with new opportunities created on social platforms, systems based on artificial intellegence also create new risks for the privacy of personal information. From this point of view, the security of personal data remains a top priority. The article explores some contemporary methods to ensure the security of personal data and analyzes their pros and cons.

Keywords— *personal data, data security, artificial intelligence, mashine learning, privacy preserving machine learning*