PROCEEDINGS OF
9th INTERNATIONAL CONFERENCE ON
INFORMATION SECURITY AND CRYPTOLOGY
(ISCTURKEY 2016)

9. ULUSLARARASI BİLGİ GÜVENLİĞİ VE
KRİPTOLOJİ KONFERANSI
BİLDİRİ KİTABI

ISC TURKEY 2016
BİLDİRİLER KİTABI
PROCEEDINGS BOOK

25-26 Ekim / ***October 2016***
ODTÜ Kültür ve Kongre Merkezi
METU Cultural & Convention Center

Ankara, TÜRKİYE / *TURKEY*

***Editors*/Editörler**
Prof. Dr. Şeref Sağıroğlu
Prof. Dr. Mustafa Alkan
Prof. Dr. Ersan Akyıldız
Doç. Dr. Sedat Akleylek

www.iscturkey.org
ISBN: 978-975-507-276-0

ABOUT / HAKKINDA

This paper in this book compromise the proceedings of the meeting mentioned on the cover title page. They reflect the author's opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by ISCTURKEY 2016 Organising Committee.

Bu bildiri kitabında yer alan bildiri tam metinleri konferans konu başlıklarına uygun olarak yazarlar tarafından hazırlanmıştır. Bildiri özetleri yazarların kendi fikirlerini yansıtır ve herhangi bir değişiklik yapılmadan aynı şekilde basılmıştır. Bu bildiri kitabında yayımlanan görüşler yazarlara ait olup bu görüşlerinden ISCTURKEY 2016 Düzenleme Kurulu sorumlu tutulamaz.

Contact to / İrtibat:

Bilgi Güvenliği Derneği

Adres : Maltepe Mahallesi Tuncer Sok. No.4/8 - Çankaya 06570 - Ankara - Türkiye
Tel : +90 312 231 1810
Fax : +90 312 231 1810
Eposta : bilgi@bilgiguvenligi.org.tr

ARTICLES PRESENTED IN ISCTURKEY 2016

ISCTURKEY 2016'DA SUNULAN BİLDİRİLER

İçindekiler / Contents

İKİ STEGANOGRAFİK İMGE KULLANAN LSB TABANLI GERİ DÖNÜŞÜMLÜ VERİ GİZLEME ALGORİTMASI..... 1

İMGE KİMLİKLENDİRME VE SALDIRI TESPİTİ İÇİN BLOK TABANLI KIRILGAN DAMGALAMA ALGORİTMASI . 5

SOSYAL MÜHENDİSLİK: YAYGIN ATAKLAR VE GÜVENLİK ÖNLEMLERİ 11

BİR BÜTÜN OLARAK M2M ve IOT GÜVENLİĞİ 19

ENDÜSTRİYEL KONTROL SİSTEMLERİNDE SİBER GÜVENLİK: PLC GÜVENLİĞİ ÜZERİNE BİR İNCELEME ... 26

SOME RESULTS ON MDS MATRICES 35

TÜRKİYE ADRESLİ HTTP GÜVENLİK BAŞLIKLARININ ANALİZİ 39

BİYOMETRİK KİMLİKLENDİRME PARMAK İZİ TABANLI YENİ BİR METOT VE YAZILIMI 47

MİKROSERVİSLER VE UYGULAMA YAZILIMLARI GÜVENLİK TESTLERİ 52

NFC TABANLI MOBİL ÖDEME SİSTEMLERİ İÇİN YENİ BİR GÜVENLİ KİMLİK DOĞRULAMA YAKLAŞIMI..... 60

H.265/HEVC VİDEO UYGULAMALARINDA İMZA TABANLI GİZLİYAZI ANALİZİNDE YENİ BİR YAKLAŞIM..... 65

TARAYICI TABANLI KATMAN 7 HİZMET ENGELLEME SALDIRILARINDAN KORUNMA..... 69

GELİŞMİŞ SÜREKLİ TEHDİTLER..... 79

IBM BLUEMIX BULUT PLATFORMUNDA IOT TEKNOLOJILERI TABANLI OTOMATIKLEŞTIRILMIŞ UZAKTAN GÜVENLIK KONTROL ORTAMLARI ÜZERINE BIR ÖRNEK ÇALIŞMA..... 88

TIBBİ GÖRÜNTÜLERDE BÜTÜNLÜK KONTROLÜ VE DAYANIKLILIK SAĞLAYAN YENİ BİR DAMGALAMA ALGORİTMASI..... 98

DİFERANSİYEL FAKTÖRLER ÜZERİNE BİR ÇALIŞMA..... 103

AKD İLE VİDEOLARDA ÇERÇEVE TEKRARLAMA SAHTECİLİĞİ TESPİTİ..... 111

SAYI TEORİK DÖNÜŞÜMÜNÜN HIZLANDIRILMASI: MODÜLER İNDIRGEMELERİN AÇIKLANMASI..... 115

EVRİMLEŞEN WEB SÜRECİ VE GÜVENLİK RİSKLERİ..... 119

KİŞİSEL VERİLERİN KORUNMASI İÇİN BİR ONAM YÖNETİM SİSTEMİ ÖNERİSİ 126

NESNELERİN İNTERNETİ UYGULAMALARINDA KİŞİSEL GÜVENİN ÖZENDİRİLMESİ 133

AKILLI SAATİNİZ NE KADAR GÜVENLİ? 138

SONLU CİSİMLER ÜZERİNDEKİ ÖZEL TİPTEKİ İNDİRGENEMEZ POLİNOMLARIN KARŞILIKLARI..... 143

RENK DÜZENİ TANIMLAYICI TABANLI VİDEO SAHTECİLİKLERİNİN TESPİTİ 148

İLİŞKİSEL VERİTABANLARI İÇİN NÜMERİK DÖNÜŞÜM TABANLI DAMGALAMA YÖNTEMİ..... 153

BGA BANK ULTIMATE WEB GÜVENLİK ZAFİYETLERİ EĞİTİM ORTAMI 159

SPROTT 94 S SİSTEMİ İLE KAOS-TABANLI BİR SİNYAL GİZLEME UYGULAMASI..... 166

NOSQLIA'NIN TEHDİTLERİ HUSUSUNDA AIC GÜVENLİK ÜÇLÜSÜ 172

MSER VE SURF TABANLI SAYISAL KOPYALA YAPIŞTIR SAHTECİLİĞİ TESPİTİ..... 177

FINGERPRINT TEMPLATE WITH RIDGE PATTERN 182

İNSANIN DUYUM VE ALGISINI KULLANAN SES TABANLI BİR CAPTCHA SİSTEMİ 187

GÜVENLİ IOT AĞ GEÇİDİ 191

MOBİL UYGULAMALARIN SINIFLANDIRILMASINDA KULLANILAN MAKİNE ÖĞRENMESİ ALGORİTMALARININ GÜVENİRLİLİK TESPİTİ 196

INTERNET OF THINGS (IOT) AND SECURITY ISSUES 201

ARNOLD'IN CAT DÖNÜŞÜMÜNÜ KULLANARAK SİNYAL ŞİFRELEME..... 206

AKILLI TELEVİZYONLAR ÜZERİNE GÜVENLİK İNCELEMESİ..... 211

WEB UYGULAMALARINDA SSL/TLS KULLANIMININ ANALİZİ..... 217

YAZILIMDAKİ SELF-CHECKSUMMING KORUNMALARININ TESPİT EDİLMESİ İÇİN BİR YÖNTEM..... 222

YAZILIM-TANIMLI AĞLAR VE SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ ÜZERİNE BİR İNCELEME..... 227

AKILLI ŞEBEKELER: VERİ MAHREMİYETİNE YÖNELİK TEHDİTLER 231

BİLGİ GÜVENLİĞİ ENDÜSTRİSİNİN ÜLKELERE GÖRE KARŞILAŞTIRMASI 236

ÇOK NİTELİKLİ FAYDA TEORİSİYLE SALDIRGAN PROFİLİNE YENİ PARAMETRELERİN EKLENMESİ..... 245

MOBİL AKILLI CİHAZLAR İÇİN CASUS YAZILIM İNCELEMESİ: FLEXISPY ÖRNEĞİ..... 252

AKILLI ŞEBEKELER: VERİ MAHREMİYETİNE YÖNELİK TEHDİTLER

SMART POWER GRIDS: THREATS TO DATA PRIVACY

Yılmaz Vural
Bilgisayar Mühendisliği Bölümü
Hacettepe Üniversitesi
06800, Ankara, Türkiye
yvural@hacettepe.edu.tr

Murat Aydos
Bilgisayar Mühendisliği Bölümü
Hacettepe Universitesi
06800 Ankara Türkiye
maydos@hacettepe.edu.tr

Mehmet Tekerek
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü
Kahramanmaraş Sütçüimam Üniversitesi
46040, Kahramanmaraş, Türkiye
tekerek@ksu.edu.tr

Ahmet Serdar Yılmaz
Elektrik- Elektronik Mühendisliği Bölümü
Kahramanmaraş Sütçüimam Üniversitesi
46040, Kahramanmaraş, Türkiye
asyilmaz@ksu.edu.tr

Özet— Günümüzde kritik altyapı tehditlerinin başında siber saldırılar gelmektedir. Kritik altyapıların lokomotifi olan elektrik enerjisi iletim ve dağıtım şebekelerinin saldırı, sabotaj ve ihmallere karşı korunmasında, kaçakların tespitinde, maliyet etkin yönetiminde, akıllı şebekelerin önemli bir rolü vardır. Oldukça yeni bir çalışma alanı olan akıllı şebekelerin geliştirilerek kullanımının yaygınlaştırılması sürecinde tehditlerin tanımlanması, sınıflandırılması ve önlemlerin alınmasına yönelik çalışmalara ihtiyaç duyulmaktadır. Akıllı şebekelerin siber saldırılara maruz kalmaması için verilerin toplanmasında, paylaşılmasında güvenlik ve mahremiyet korumasının sağlanması gerekmektedir. Çeşitli sebeplerle verilerin işlenebilmesi amacıyla veri faydasının da mahremiyet önlemleri sırasında dikkate alınması gerekmektedir. Bu çalışmada akıllı şebekeler tanımlanmış, ürettiği hassas verilerin mahremiyetine yönelik tehditler sıralanmış ve değerlendirmeler yapılarak çözüm önerileri sunulmuştur.

Anahtar Kelimeler— Akıllı Şebekeler. Güç Sistemlerinde Haberleşme. Veri Mahremiyeti. Mahremiyete Yönelik Tehditler.

Abstract— Smart power grids have an important role in protecting power transmission and distribution grids which are locomotive of critical infrastructures against to sabotage and neglect, efficient cost administration, leakage determination. It is necessary to describe, classify certain threats and to take precautions to these threats in spreading use of smart power grids process. In this context, first threats to security and privacy come to the forefront during distributing and sharing of data produced by smart power grids. It is expected to include sensitive and non-sensitive data when data produced by smart power grids are examined and classified. It is necessary to distribute and share these sensitive data in the protection of privacy and data benefit in order to use for different purposes. In this study, smart power grids are described, the threats to sensitive data privacy are explained and solution suggestions are presented by evaluations.

Index Terms—Smart Grids. Power System Communication. Data Privacy. Threats to Privacy.

I. GİRİŞ

Günlük hayatı ve kamu düzeninin sürdürülmesini doğrudan etkileyecek bileşenlerden oluşan kritik altyapıların (enerji, savunma, finans, hukuk, sağlık, ulaşım, bilişim vb.) güvenliğinin ve mahremiyetinin sağlanması ülke güvenliği açısından üst düzeyde önem arz etmektedir. Kritik altyapıların lokomotifi konumunda bulunan elektrik enerjisinin arz güvenliği hem stratejik hem de ticari olarak son yıllarda önem kazanan bir konu olarak araştırmacıların karşına çıkmaktadır. Ulusal enterkonnekte enerji iletim şebekelerinde siber saldırılar, sabotaj veya ihmallere bağlı olarak gelişebilecek süreksizlik ve kesintiler, tüm ülkedeki kritik altyapıları doğrudan etkileyerek kamu düzeninin sağlanmasında ve günlük yaşamda ciddi sorunlar ile hizmet kesintilerine yol açacaktır. Örnek olarak 31 Mart 2015 tarihinde Türkiye'de yaşanan şebeke çökmesi maddi ve manevi kayıplara yol açmıştır. Yaşanan bu enerji iletim şebeke kazasının 750 milyon dolarlık kayba sebep olmasının yanında vatandaşların kamuya duyduğu güvenin sarsılmasına da yol açtığı tespit edilmiştir. Ayrıca, Doğu ve Güneydoğu bölgelerinde elektrik dağıtım şebekelerindeki kayıp kaçakların yüksek değerlere ulaştığı ve ülke ekonomisine ciddi zararlar verdiği görülmektedir. Elektrik iletim ve dağıtım şebekelerinde muhtemel arızaların önceden tahmini, anomalilerin ölçülmesi, kaçak kullanımlarının tespiti ve önlenmesi ile diğer işletme sorunlarının giderilmesi amacıyla şebekelerin uluslararası standartlara uygun olarak yönetilebilmesini sağlayan "akıllı şebekeler" haline getirilmesi gerekmektedir.

Akıllı şebekeler gerek iletim gerekse dağıtım şebekesi olsun, tüm bağlantı noktalarında (baralarda) elektriksel tüm parametrelerin (akım, gerilim, güç ve frekans gibi) ölçülerek izlenmesini gerekli kılmaktadır. Alternatif akım elektrik enerjisinin depo edilememesi ve anlık üretim tüketim eşitliğinin zorunlu olmasından dolayı hızlı ve anlık değişmelerde şebekenin elektrik enerjisi arzını güvenle sağlayabilmesi zorunludur. Bu ve benzeri nedenlerle akıllılaştırılmış şebekelerin ülkemizde yaygınlaştırılarak kullanılması zaruri olmuştur. Bunun yanı sıra, özellikle

müşteri odaklı bakıldığında tüketicilerin elektrik tüketim karakteristiklerinin bilinmesi hem ticari ve hem de teknik kalite açısından önem arz etmektedir. Örneğin, bir enerji dağıtım şirketinin müşterilerinin elektrik kullanım alışkanlıklarını bilmesi ve bölgesindeki elektrik tüketim değişimlerini kestirebilmesi enerji dağıtım planlamasının sağlıklı yapılması açısından zorunludur. Serbest piyasa koşullarında elektriğin fiyatının günün belli saatlerine göre değişken olmasının sonucu olarak maliyetleri azaltmak için ucuz tarife zamanlarına tüketimin dağıtılarak kullanımın belirli saatlere yığılmasının engellenmesi gerekmektedir [1]. Bununla birlikte müşterilerin (konutlar, küçük-orta-büyük sanayi işletmeleri) elektrik faturalarının azaltılması akıllı şebekelerin ilgi alanına girmektedir. Elektrik kullanımının yüksek ve dolayısıyla pahalı olduğu puant saatler (akşam saatleri) yerine elektriğin kullanımının daha az ve ucuz olduğu gece yarısı, sabah saatlerinde kullanımının teşviki son yıllarda önemli çalışma alanlarından biri haline gelmiştir. Ülkemizde şebekeler akıllı hale getirildikçe, elektrik sarfiyat verilerinin takip edilmesi için akıllı şebeke verilerinin uzaktan okunarak ihtiyaca uygun işlenmesi gerekmektedir. Bu durumda verilerin mahremiyeti ile güvenliğinin sağlanmasına yönelik iki önemli problem öne çıkmaktadır. Kurumsal veya bireysel tüketicinin mahrem verilerini içeren elektrik kullanma alışkanlıklarına ait bilgilerin toplanması ve paylaşılması sırasında mahremiyet ve güvenlik önlemlerinin alınması gerekmektedir.

Toplanan ve paylaşılan abonelere ait enerji kullanım bilgileri hem özel hayat hem de ticari açıdan hassas bilgiler içermektedir. Aboneleri doğrudan veya dolaylı yönden tanımlayan, ad, soyad, adres gibi bilgiler hassas bilgilerin başında gelmektedir. Geriye dönük yıllık, aylık, haftalık, günlük saatlik tüketim bilgileri ise mahrem olmayan ancak veri faydası açısından önem arz eden bilgilere örnek olarak verilebilir. Mahremiyetin sağlanmasında, hassas bilgilerin korunmasının yanında hassas olmayan bilgilerin işlenmesini mümkün kılacak çözümlere ihtiyaç vardır. Veri mahremiyetine yönelik korunmasızlıklar sonucunda ifşa olan bilgiler bir işletmenin rekabet ve pazar gücünü doğrudan etkileyebilir. Diğer husus ise sayaçtaki verinin dağıtım şirketine aktarılması sırasında verilerin bütünlüğünü bozabilecek saldırılara maruz kalma riskidir. Aktarılacak veriler faturlandırmada kullanılan elektrik tüketim verileri olduğundan bütünlüğünün korunması gerekmektedir. Aksi halde bütünlüğü korunamayan bu veriler değiştirilerek şirket yada son kullanıcı aleyhine maddi zararların doğmasına neden olacaktır.

Yukarıda, enerji kullanım bilgilerinin toplanması ve dağıtılmasında veri mahremiyetinin korunarak güvenliğinin sağlanmasının gerekliliğini ve önemi ortaya konmaya çalışılmıştır. Ayrıca bir tüzel veya gerçek kişinin enerji kullanım bilgileri gerek ticari açıdan ve gerekse kişisel açıdan önemlidir. Bu çalışmada, elektrik enerjisi tüketim alışkanlıkları ile fiyatlandırma verilerini içeren hassas bilgilerin mahremiyetine yönelik tehditler ele alınmıştır. Tehditler incelenerek değerlendirmeler yapılmış ve çözüm önerileri sunulmuştur. Bu amaçla çalışmanın ikinci bölümünde veri mahremiyeti konusu incelenmiş ve mahremiyetin korunması ile ilgili önerilen yöntemler tanımlanmıştır. Üçüncü bölümde ise bu çalışmaya konu olan akıllı şebekelerde veri mahremiyetine yönelik muhtemel tehditler sıralanmaya çalışılmıştır. Sonuç olarak akıllı şebekelere yönelik mahremiyet unsurları ve olası tehditler konusunda değerlendirmeler yapılmıştır.

II. VERİ MAHREMİYETİ

Akıllı şebekelerin üretmiş olduğu sayısal ortamlarda kullanılan ve işlenebilen tüketim verileri işletmelerin işlerini kolaylaştırırken yeni tehdit ve tehlikeleri de beraberinde getirmektedir [4]. Tüketim verilerinin toplanmasında ve paylaşımında meydana gelebilecek saldırıları engelleyebilmek amacıyla mahremiyeti koruyan tedbirlerin zamanında alınması gerekmektedir. Veri mahremiyeti, veri sahiplerinin mahremiyeti ile veri paylaşımının taraflara sağlayacağı fayda arasındaki en iyi dengeyi bulmaya çalışan zor bir problemdir [5].

İşletmelerde mahremiyet bilincinin oluşturularak, yeterli düzeyde kültürel ve teknik önlemlerin alınması birçok mahremiyet odaklı saldırının önünü kesecektir. Ülkemizde ve dünyada yaşanan birçok olayda mahremiyet bilincinin eksikliğine bağlı ihlaller yaşanmıştır.1990 yılında ABD'de sayım uygulamasıyla toplanan cinsiyet, posta kutusu ve doğum tarihi gibi hassas olmayan verilerin kullanılarak ABD nüfusunun %87'sinin kimliklerinin tespit edilebileceği Sweeney tarafından raporlanmıştır [6]. 2006 yılında AOL firması 21 milyon web sorgusunu içeren 500 bin kullanıcının 3 aylık arama kayıtları anonim kimlik numarasıyla yayınlamıştır [5,7]. Bu sayede saldırganlar bu verilerle mahremiyet saldırıları yapmışlardır.

Dünyada olduğu gibi ülkemizde de çok sayıda mahremiyet ihlalleri yaşanmaktadır. 2008 yılında Resmi Gazetede sekiz milyon beş yüz bin kişinin TC Kimlik Numarası ve sigorta numarasını içeren KEY ödemeleri listesinin yayınlanması mahremiyet bilincinin oluşmamasından kaynaklanmıştır [8]. 2010 yılına ait, 50 milyona yakın Türk vatandaşının TC Kimlik Numarası, ad-soyad, anne- baba adı, cinsiyet, doğum tarihi, doğum yeri ve açık adres gibi kimlik bilgileri 2016 yılında internette yayınlanmıştır [9].

Mahremiyet ihlallerinin ve saldırılarının en aza indirgenmesi amacıyla güncel saldırıların analizi ve veri faydası ihtiyaçlarına göre yeni mahremiyet koruyucu yaklaşımlara ihtiyaç duyulmaktadır [10].

Mahremiyetin korunmasıyla ilgili literatürde yapılan çalışmalar şu şekilde sıralanabilir.

A. Veri Anonimleştirme

Anonimleştirme, verinin tipi ve biçimi korunarak veri faydası açısından kabul edilebilir düzeyde yapılan mahremiyet koruyucu işlemlerdir. Veri anonimleştirme ilk defa 1981 yılında Chaum tarafından önerilmiş ve ilk uygulama Jakobsson tarafından yapılmıştır [12,13].Veri anonimleştirilmesinin seviyesinin iyi belirlenmesi gerekmektedir. Gereğinden fazla yapılacak anonimleştirme veriden sağlanacak faydayı olumsuz etkilerken, yeteri kadar yapılmayan anonimleştirme ise ihlallere yol açacaktır.

B. Veri Madenciliğinde Mahremiyetin Korunması (Privacy Preserving Data Mining-PPDM)

PPDM, veri sahiplerinin kimliklerinin veya hassas bilgilerinin ifşa edilmesini engelleyen veri kümesi üzerinde birden fazla araştırmacının birlikte çalışmasını mümkün kılan yeni bir madencilik yöntemidir [14,15,16,17,18].Veri madenciliğinde mahremiyetin korunmasını sağlamak amacıyla istatistiksel ve kriptografik temelli yaklaşımlar geliştirilmiştir. [19]. İstatistiksel yaklaşımlar genellikle verilerin anlamlı olarak bozulmasına dayanmaktadır. Diğer yöntemde mahremiyetin korunmasında kriptografik fonksiyonlar kullanılmaktadır.

C. Veri Yayınlanmasında Mahremiyetin Korunması (Privacy Preserving Data Publishing-PPDP)

Veri yayınlama yöntemi, veri paylaşımında kolay ve ekonomik bir yöntem olduğu için veri toplayıcılar tarafından yaygın olarak kullanılmaktadır[20]. Bu yöntemde mahremiyet modelleri kullanılarak anonimleştirilen veriler ihtiyaç sahiplerinin doğrudan ulaşabileceği kamuya açık ortamlardan yayınlanmaktadır.

D. Veri Toplanmasında Mahremiyetin Korunması (Privacy Preserving Data Collection-PPDC)

Üçüncü tarafların doğrudan veri sahiplerinden veri toplama ihtiyacı olduğu durumlarda mahremiyetin korunması daha önemli ve zor hale gelmektedir. PPDC ile ilgili literatürde yapılan bir çok çalışmada veriler üzerinde bozma algoritmaları kullanarak elde edilen anonim verilerin veri sahipleri tarafından doğrudan veri toplayıcıya gönderildiği C2S (client to user) mimarisinin önerildiği görülmüştür [21,22,23]. Ancak bu yöntem veri sahiplerinin mahremiyet bilincinin yüksek seviyede olmasını zorunlu kılmaktadır. Ayrıca bu yöntem dışında veri sahipleri hazır veya kendilerinin geliştireceği mahremiyet araçlarını kullanarak verileri doğrudan ihtiyaç sahiplerine gönderebilmektedir.

III. AKILLI ŞEBEKELERDE VERİ MAHREMİYETİNE YÖNELİK TEHDİTLER VE ÖNERİLER

Akıllı şebekelerde üretilen bilgilerin mahremiyet saldırılarından korunabilmesi amacıyla hassas (H), yarı hassas(YH) ve hassas olmayan (HO) şeklinde sınıflandırılması gerekmektedir. Bu bilgileri içeren veri setleri V(H,YH,HO) şeklinde ifade edilebilir. Hassas bilgiler doğrudan veri sahiplerini tanımlarken, yarı hassas olan bilgiler ise dolaylı yönden veri sahiplerinin tanımlanmasını mümkün kılmaktadır. Hassas olmayan ve yarı hassas olan bilgiler üzerinde işlemler yapılarak veriden fayda sağlamaya yönelik madencilik veya istatistiki işlemler yapılmaktadır.

Mahremiyet açısından yapılan sınıflandırmadan sonra risklerin tanımlanarak azaltılmasına yönelik çalışmaların yapılması gerekmektedir. Bu kapsamda öncelikle veri setleri içerisinden hassas (H) olan bilgiler çıkarılarak V(YH, HO) formatına getirilmelidir. Bu aşamadan sonra dikkat edilmesi gereken diğer önemli husus yarı hassas (YH) olan verilerin dikkatlice incelenmesi ve ihtiyaca göre anonimleştirme yapılması gerekmektedir. Veri faydasının korunabilmesi amacıyla ihtiyaçlara göre tolere edilebilecek veri kayıp seviyesi belirlenerek anonimleştirme yapılmalıdır. Anonimleştirilmiş yarı hassas verileri YH* olarak ifade ettiğimizde Y(YH*,HO) formatına getirilen veriler paylaşıldığında mahremiyet ihlalleri en aza inecektir.

Akıllı şebekelerde enerji kullanım verileri incelendiğinde, insanların hangi saatlerde çalıştığı, uyku saatleri, günlük hayata dair planlamaları ile ilgili tahminler yürütebilecek bilgiye sahip olunabilmektedir. Elde edilen verilere bakıldığında kişisel bilgilerin dışında, mahalleler, devlet kurumları, şirketler, önemli kişiler, politikacılar vb tüketicilere ait bilgilerden yapılacak çıkarımlarla mahremiyet saldırıları yapılabilecektir. Yapılacak çıkarımlar bilgilerin saldırganların eline geçmesine ve saldırılarını bu bilgilere göre planlariskler içerir. Dolayısıyla akıllı cihazlardan alınan bu tür bilgiler ticari ve stratejik nitelikte önemli veriler olabilir. Buradan da anlaşılabileceği gibi enerji kullanım verileri basit bir faturalandırma ve elektrik faturalarını azaltmaya yönelik olmayabilir. Kritik, kişisel ve özel bilgilerin kestirilmesini sağlayabilecek veriler olabilir. Bu durumda bu verilerin taşınmasında güvenliğin yanısıra mahremiyetin de önemi öne çıkmaktadır. Örneğin bir konutta elektrik tüketiminin izlenmesi sonucu elde edilen veriler müşterinin davranışını etkileyebilir. Bu verilerin sızdırılması ve olmaması gerekenlerce bilinmesi, müşterinin mahremiyetini doğrudan etkileyebilecektir. [24]

Bu verilerin dağıtım şirketleri açısından da önemi bulunmaktadır. Arz-talep yönetimi, elektrik enerjisinin verimli biçimde dağıtımı, optimum yük akış analizi vb durumlarda bu verilerin kritik bir önemi bulunmaktadır. Şirketlerin daha karlı ve daha az maliyetle enerjiyi arz etmesinde faydalı olabilecek bilgiler olduğu aşikârdır.

Akıllı şebekelerde veri mahremiyetine yönelik tehditleri dört seviyede incelemek mümkündür. [25]

a. Fiziksel seviyedeki saldırılar: Fiziksel seviye saldırılar verilerin aktarılması sırasında sinyal bozucular kullanarak yada akıllı sayaçlara fiziksel zarar vererek yapılan saldırılardır. Böylece haberleşme kanallarında işaretlerin bozulması yada protokollere saldırı yapılarak veri trafiğinin aşırı oranda artışı hedeflenir.
b. MAC seviyesindeki saldırılar: MAC seviyesinde saldırılarda ise MAC parametrelerin illegal biçimde değiştirilmesi sonucu verilerin sağlıklı biçimde şebeke ulaşmaması amaçlanmaktadır.
c. Taşıma ve Ağ Seviyesindeki saldırılar: Taşıma ve ağ seviyesindeki saldırılarda kaynağı sönümlendirerek uçtan uca veri akışını kesmek hedeflenir. Böylece veri trafiğini bir süreliğine legal trafiği kesmektedir.
d. Uygulama seviyesindeki saldırılar: Uygulama seviyesindeki saldırıların temel amacı uygulamaya yoğun periyotlu istek göndererek hedef CPU ve hafızayı kilitlemektir.

IV. SONUÇLAR

Elektrik şebekelerinin akıllı hale getirilmesi önümüzdeki on yıl içinde dünyada olduğu gibi ülkemizde de şebeke otoriteleri için kaçınılmaz bir zorunluluk olacaktır. Ancak şebekelerin akıllı hale gelmesi neticesinde veri mahremiyeti ve güvenliği hususları önemli bir zafiyet noktası olarak öngörülmektedir. Bu zafiyet noktaları şebekelerde gerek ticari gerekse stratejik olumsuzluklara yol açacaktır. Yukarıda belirtilen olumsuzluk ve zafiyetlere rağmen akıllı şebekelerin kullanılması zorunlu olacaktır. Bu nedenle şebekelerin akıllı hale getirilmesi durumunda olası zafiyetler ve tehditler belirlenerek önlemler alınmalıdır. Stratejilerin belirlenmesinde gerçek ve tüzel kişilere ait hassas ve genel bilgilerin tehditlere karşı korunması ile zafiyet risk oranının azaltılması dikkat edilecek hususlardan olmalıdır.

Örnek olarak, Güneydoğu Anadolu bölgesindeki elektrik dağıtım şirketlerinin en önemli sorunu kaçak elektrik kullanımıdır. Genellikle elektrik sayaçlarının eski teknoloji olması, sayaçlarda oynama yapılabilmesi veya güvenlik nedeniyle bazı mahallelerde elektrik sayaçlarının okunamaması problemleri oldukça fazladır. Elektriğin kaçak kullanımının önlenmesi için sayaçların uzaktan okunması ve üzerinde oynama yapılmaya olanak vermemesi önem kazanmaktadır. Bu bölgelerde akıllı sayaçların uzaktan okunmasına yönelik projeler geliştirilmekte ve mevcut sayaçlar yerine hem uzaktan okunabilen hemde üzerinde hatalı ölçüm yapılmasını sağlayacak müdahalelere imkan verilmeyecek akıllı sayaçların geliştirilmesi ve yaygınlaştırılması teşvik edilmektedir. Benzer şekilde 31 Mart 2015 sistem çökmesi gibi olayların tekrar yaşanmaması için iletim şebekesinin de akıllı hale getirilmesi zorunludur. İleriki çalışmalarda, akıllı şebekelerin yaygınlaşması önünde engel olarak düşünülebilecek güvenlik ve mahremiyet sorunun farklı bakış açılarıyla ele alınması gerekmektedir.

REFERENCES

[1] R. Lu, Privacy-enhancing aggreation techniques for smart grid communications, Springer, 2016

[2] 12. C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford, and P. Armstrong, "Power signature analysis," IEEE Power Energ. Mag., vol. 1, no. 2, pp. 56–63, 2003.

[3] M.F. Öttekin, Elektrik Altyapılarında Bilgi Güvenliği Riskleri ve Çözümler, Akıllı Şebekeler Sempozyumu, EMO, 2013

[4] Korolova, A., Protecting privacy while mining and sharing user data, Doktora Tezi, Stanford Üniversitesi, Bilgisayar Mühendisliği Bölümü, 2012.

[5] Verykios,S.V., Bertino, E.,Fovino, N.I., Provenza, P.L., Saygin, Y., Theodoridis, Y., "State-of-the-art in Privacy Preserving Data Mining", ACM SIGMOD Record, Cilt 33, Sayı 1, 50-57, 2004.

[6] Sweeney, L., "k-Anonymity: A model for protecting privacy," International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, Cilt 10, Sayı 5, 557–570, 2002.

[7] İnternet: Barbaro, M.,Zeller, T., "A Face Is Exposed for AOL Searcher No. 4417749", http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=0, 2006.

[8] İnternet: Üstün, G., "e-devlet Skandalı", http://www.milliyet.com.tr/Ekonomi/HaberDetay.egori=ekonomi&ArticleID=972537&Date=30.07.2008&b,2008.

[9] İnternet: Hurriyet Gazetesi, "70 milyon kişinin bilgilerini ele geçirdiler" http://www.hurriyet.com.tr/70-milyon-kisinin-bilgilerini-ele-gecirdiler-15424807, 2010.

[10] Gökçe, H., Abul, O., "Sensitive knowledge hiding application", Electrical, Electronics and Computer Engineering (ELECO), Bursa,Türkiye, 558-562, 2010.

[11] Gehrke, J., "Models and Methods for Privacy-Preserving Data Analysis and Publishing ", The 22nd International Conference on Data Engineering, Atlanta, ABD,105-106, 2006.

[12] Chaum, D.L., "Untraceable electronic mail, return addresses, and digital pseudonyms,", Communications of the ACM, Cilt 24, Sayı 2, 84-90, 1981.

[13] Jakobsson, M., Juels, A.,Rivest,R.L., "Making mix nets robust for electronic voting by randomized partial checking, ", In Proceedings of the 11th USENIX Security Symposium, San Franscisco,339-353, 5-9 Agustos 2002.

[14] Gayatri Nayak and Swagatika Devi (2011), "A Survey On Privacy Preserving Data Mining: Approaches And Techniques", International Journal of Engineering Science and Technology, Cilt 3, Sayı 3, 2127-2133, 2011.

[15] Lindell, Y., Pinkas, B., "Privacy Preserving Data Mining", 20th Annual International Cryptology Conference, California, USA, 36-53, 2000.

[16] Hand, D., Mannila, H., Smyth, P., "Principles of DataMining", MIT Press, 2001.

[17] Vaidya, J., Clifton, C., "Privacy-Preserving Data Mining: Why, How, and When"IEEE Security & Privacy,Cilt 2, Sayı 6, 19-27, 2004.

[18] Du, W., Atallah, M. J., "Secure Multi-Party Computation Problems and Their Applications: A Review And Open Problems", In Proceedings of New Security Paradigms Workshop, New Mexico, ABD, 11-20, 2001.
[19] Adam,N. R.,Worthmann, J. C.,"Security-control methods for statistical databases: a comparative study" ACM Computing Surveys (CSUR), Cilt 21, Sayı 4, 515–556, 1989.
[20] Yongcheng, L., Jiajin, L., Jian, W., "Survey of Anonymity Techniques for Privacy Preserving", 2009 International Symposium on Computing, Communication, and Control (ISCCC 2009), Singapur, 248-252, 2011.
[21] Du, W., Zhan, Z. "Using randomized response techniques for privacy-preserving data mining",International Conference on Knowledge Discovery and Data Mining,San Francisco,, ABD, 505-510, 2003.
[22] Zhang, N., Wang, S., Zhao, W. "A new scheme on privacy-preserving data classification", International Conference on Knowledge Discovery and Data Mining, Chicago, ABD,374–382, 2005.
[23] Zhang, L., Zhang, W., "Generalization-based privacy-preserving data collection" International Conference on Data Warehousing and Knowledge Discovery, Las Vegas, ABD,115–124, 2008.
[24] R. Herold and C Hertzog, Data privacy for the smart grid, CRC press, 2015
[25] A. Prcopiou and N. Komninos," Current and Future Threats framework in smart grid domain", proc of the 5th IEEE Conf on Cyber Technology in automation, control and intelligent systems, China, 2015