©2020 Published in 8th International Symposium on Innovative Technologies in Engineering and Science 23-25 October 2020 (ISITES2020 Bursa - Turkey)
https://doi.org/10.33793/acperpro.03.01.81

Şifreleme Yöntemleri ve Hesap Güvenliği Üzerine Bir Araştırma
A Research on Encryption Methods and Account Security

*[1]Rıdvan Yayla, [2]Hakan Üçgün and [3]Sefa Tunçer
*[1]Bilgi İşlem Daire Başkanlığı – Bursa Teknik Üniversitesi, Türkiye
[2]Bilgi İşlem Daire Başkanlığı – Eskişehir Teknik Üniversitesi, Türkiye
[3]Bilgisayar Mühendisliği Bölümü – Bilecik Şeyh Edebali Üniversitesi, Türkiye

Öz

Günümüzde, küresel pandemiye yönelik önlemlerin arttırılması ile birlikte sanal dünya yaygın olarak kullanılmaktadır. Bu nedenle, giderek artan temel ihtiyaçları karşılamak amacıyla kullanıcı hesabı temelinde oluşturulan üyelik sistemleri önemli bir role sahiptir. Verilerin güvenli bir şekilde gönderilmesi, son kullanıcının verdiği bilgilerin alınabilmesi için günümüz sistemlerinde en önemli gereksinimler, bilgilerin sorunsuz bir şekilde taşınması ve gizliliktir. Kullanıcı hesaplarının geliştirilmesi ile birlikte bilgi güvenliği için oluşturulan şifrelerin karmaşık ve güvenli olması gerekmektedir. Bir hesabın güvenliği, siber saldırıları engellemeye yönelik şifre karmaşıklığı ile birlikte sms sistemleri, kimlik doğrulama, güvenlik sorusu, robot kontrolü gibi ilave önlemlerle güçlendirilmektedir. Simetrik ve asimetrik şifreleme algoritmaları, veri gizliliği ve bütünlüğü için kullanımı kolay ve uygun yöntemlerden oluşmaktadır. Bu çalışmada, her alanda kullanımı yaygınlaşan kullanıcı hesaplarının güvenliği için günümüzde kullanılan şifreleme yöntemlerinin geçerliliği analiz edilmiş ve şifre karmaşıklığının hesap güvenliğindeki rolü araştırılmıştır.

Anahtar Kelimeler: Kullanıcı hesabı, şifreleme, bilgi güvenliği, gizlilik

Abstract

Nowadays, the virtual world is widely used by increasing of the precautions for the global pandemic. Therefore, the membership systems that are created on the basis of the user accounts have an important role in order to meet the increasing requirements. The most important requirements of the current systems are privacy and delivering of the datas as seamlessly for sending of the datas as security and receiving of the end users datas. The security of an account is enhanced by additional measures such as sms systems, authentication, security question, and robot control along with password complexity to prevent cyber attacks. Symmetric and asymmetric encryption algorithms are composed of easy and convenient methods for data privacy and integrity. In this study, the validity of the used encryption methods in today for the security of user accounts, which are becoming widespread in every field, is analyzed and the role of password complexity in account security is investigated.

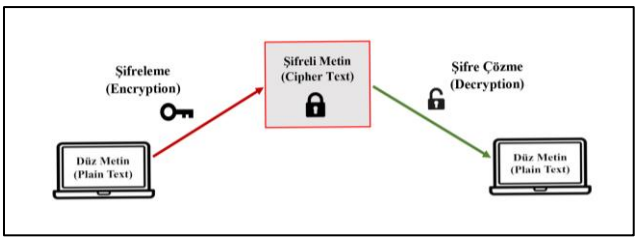
Key words: User account, encryption, data security, privacy

1. Giriş

Bilgisayar bilimlerinde, *cruptos* (gizli) ve *logos*(bilim) kelimelerinden oluşan kriptoloji biliminin temeli, bilginin güvenli bir şekilde iletilmesini sağlayan şifreleme yöntemlerinden oluşmaktadır. Bilginin gizlilik içinde ve eksiksiz bir biçimde son kullanıcıya ulaştırılması, kriptoloji bilimindeki

*Corresponding author: Address: Information Technology Department, Bursa Technical University, 16310, Bursa TURKEY. E-mail address: ridvan.yayla@btu.edu.tr, Phone: +902248081026

bilgi güvenliği ilkesinin en temel unsurlarındandır. Temel olarak bir metindeki şifreleme işlemi, düz metin (*plain text*), şifreleme işlemi (*encryption*) ve şifreli metin (*chipher text*) olarak üç aşamadan oluşmaktadır. Tersinir olarak, şifreli bir metnin yeniden düz metne çevrilmesi işlemi için de şifre çözme (*decryption*) işlemi uygulanmaktadır [1]. Ancak günümüz sistemlerinde temel şifreleme işlemlerinin bilgi gizliliği için yetersizliği, şifreleme algoritmalarının geliştirilmesini ve bu sayede bilginin son kullanıcıya daha güvenlikli bir şekilde ulaştırılmasını sağlamıştır.



Şekil 1. Temel şifreleme yöntemi

Günümüzde üyelik sistemlerinin yaygın kullanılmasıyla birlikte kullanıcı hesaplarının güvenliği önemli hale gelmiştir. Geliştirilen şifreleme algoritmaları sayesinde hesap güvenliği birden fazla güvenlik yöntemi ile daha güvenlikli hale getirilmektedir. Son yıllarda tüm dünyada ortaya çıkan Covid-19 pandemi vaka sayılarının artması, insanların mecburi olarak evlerinde vakit geçirmesine ve sanal dünyaya olan bağımlılıklarının artmasına neden olmuştur. Bu dönemde e-ticaret, e-devlet, sosyal medya, çevrimiçi oyun vb. platformların kullanımı artmış ve kullanıcı hesaplarının güvenliği, dikkat edilmesi gereken bir unsur haline gelmiştir. Çalışma kapsamında, bir kullanıcı hesabının güvenliği için başta şifre karmaşıklığı olmak üzere alınan önlemler incelenmiş, şifreleme algoritmalarının hesap güvenliğindeki rolü araştırılmıştır.

2. Metodoloji

Şifreleme yöntemleri tarihsel süreç içinde farklı amaçlarla kullanılmıştır. Eski Mısır hiyerogliflerinden, eski Yunan savaş istihbaratında kullanılmasına kadar farklı zamanlarda pek çok şifreleme kullanılmıştır. Bilinen modern kriptoloji tarihinin en ilkel örneği, Sezar şifrelemedir. Bu yöntemde, yazıdaki harflerin yerleri belli kurallara göre değiştirilerek bir şifre elde edilir. Daha yakın tarihlerde bilinen diğer bir yöntem ise enigma şifre makinesidir [2]. Bir rotor parçası yardımıyla yapılan makine, 2. Dünya savaşı sırasında Nazi Almanyası tarafından gizli mesajların şifrelenmesi amacıyla kullanılmış ve şifrelerin kırılması sonucu savaşın seyri değişmiştir.

1970'li yıllarda Feistel, Data Encryption Standard'ın (DES) temelini oluşturulan Lucifer algoritmasını geliştirmiştir [3]. 1976'da Diffie ve Hellman Elliptic Curve Diffie-Hellman (ECDH) veya Elliptic Curve Digital Signature Algorithm (ECDSA) olarak isimlendirilen açık anahtar sistemini geliştirmişlerdir [4]. Rives, Shamir ve Adleman 1978'de asal çarpanlara ayırma zorluğuna dayanan ve ismini kendi soyadlarından alan RSA algoritmasını geliştirmişlerdir [5]. 1992'de Lai ve Massey Uluslararası Veri Şifreleme Algoritmasını (IDEA- International Data Encryption Algorithm) geliştirerek, uluslarası bir şifre standardının oluşmasını sağlamışlardır [5]. 1997 yılında ise, ABD'nin National Institute of Standards and Technology kurumu Data Encryption Standard'ın (DES) yerini alacak bir simetrik algoritma yarışması düzenmiş ve

yarışmayı Daemen ve Rijmen'in Rijndael algoritması kazanmıştır. Bu algoritma günümüzde Advanced Encryption Standard (AES) ismiyle standartlaştırılmıştır [5]. Geliştirilen bu şifreleme yöntemleri temelinde, farklı algoritma yöntemleri de geliştirilmiştir. Çakmak ve Adalı, çok karmaşık olmayan, kullanımı kolay, simetrik doğrusal olmayan bir şifreleme yöntemi geliştirmişlerdir [6]. Yılmaz ve Ballı bulanık mantık marifetiyle, BAHS, TOPSIS ve PROMETHEE çok kriterli karar verme yöntemlerini kullanarak, şifreleme algoritmaları arasında hızlı, performanslı ya da güvenli seçenekleri olarak üç farklı profil sunmuş, bu algoritmaları süre, hafıza ve güvenlik açısından değerlendiren bir program tasarlamıştır [7]. Özbilgin vd., temel Vigenere şifreleme yöntemini kullanarak, bir mesaj metnini Least Significant Bit (LSB) yöntemi ile bir görüntü içindeki piksellerin mavi bileşenine, 3 farklı algoritma kullanarak gizlemeyi başarmıştır [8]. Günümüzde şifreleme tekniklerinin amaçları, gizlilik, kimlik denetimi, bütünlük, reddedilmezdik ve erişim kontrolü olarak açıklanmaktadır [9]. Bu ilkeler doğrultusunda şifreli veriler, bir bütünlük içerisinde karşı kişiye olduğu gibi aktarılır. Şifreli olarak iletilen bilgiyi alıcı ve gönderici inkâr edemez ve bilgi gizlilik içinde kalarak, üçüncül kişilerin eline geçemez. Bu amaçların gerçekleştirildiği şifreleme yöntemi, güvenli şifreleme olarak nitelendirilir.

2.1. Şifreleme Yöntemleri

Günümüzde kullanılan şifreleme algoritmaları, simetrik ve asimetrik şifreleme olarak iki ana başlıkta toplanmaktadır [10]. Ayrıca bu iki şifreleme algoritmalarının birlikte kullanılması ile hibrid şifreleme algoritmaları da geliştirilmiştir.

2.1.1. Simetrik Şifreleme Yöntemleri

Şifrelemenin temeli, şifreleme algoritmalarındaki anahtar kavramına dayanmaktadır. Simetrik şifrelemede, şifreleme ve şifre çözme işlemleri için bir adet gizli anahtar kullanılmaktadır. Bu şifreleme türünde, şifreli metin ile birlikte bir adet gizli anahtar gönderilir ve gönderilen aynı anahtar aracılığı ile şifre çözülür.

Tablo 1. Bazı simetrik şifreleme algoritmaları [11]

Algoritma	*Geliştirici*	*Tarih*	*Anahtar Uzunluğu*
Lucifer	*IBM*	*1970*	*128 bit*
DES (Veri Şifreleme Standardı)	*IBM*	*1977*	*56 bit (parity işlemi ile 64 bit)*
IDEA (Uluslararası Veri Şifreleme Algoritması)	*Lai-Massey, ETH Zurich (İsviçre)*	*1992*	*128 bit*
RC2 (Rivest's Cipher veya Ron's Code2)	*Rivest, RSA Veri Güvenliği (ABD)*	*1992*	*2048 bite kadar*
Blowfish	*Bruce Schneier, Counterpane Systems (ABD)*	*1993*	*448 bite kadar*
RC5 (Rivest's Cipher veya Ron's Code5)	*Rivest, RSA Veri Güvenliği (ABD)*	*1995*	*2048 bite kadar*
AES	*Joan Daemen ve Vincent Rijmen*	*2000*	*128 bit*

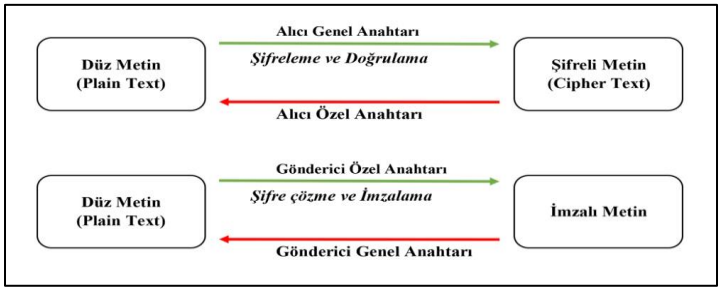
Simetrik şifreleme algoritmaları, blok şifreleme ve dizi şifreleme algoritmaları olarak iki bölümde incelenir [10]. Genellikle bütünlük ilkesinin gerçekleştirilmek istendiği durumlarda kullanılan blok

şifreleme, veriyi bloklar halinde işler. Bu işlem bazen bağımsız bazen de birbirine bağımlı olarak gerçekleştirilir.

Dizi şifrelemede ise veri bir bit dizisi olarak ele alınır ve kayan anahtar denilen bir dizi üretilir. Zamana bağlı olarak kayan anahtar ürettiği için bu algoritmaya "hafızalı şifreleme" denilmektedir. Simetrik şifrelemede, aynı şifreleme anahtarı kullanıldığından şifreleme ve şifre çözme işlemleri çok hızlı bir şekilde yapılmaktadır [12]. Bilimsel literatürde çeşitli simetrik şifreleme algoritmaları geliştirilmiş olup, bu algoritmalardan bazılarına ait temel bilgiler Tablo 1'de gösterilmiştir [11].

2.1.2. Asimetrik Şifreleme Yöntemleri

Asimetrik şifreleme yöntemleri şifreleme ve şifre çözme işlemleri için farklı anahtarların kullanıldığı "açık anahtarlı şifreleme" olarak adlandırılan yöntemlerdir. Asimetrik şifrelemede kullanılan anahtarlar, açık (genel) anahtar (*public key*) ve özel anahtar (*private key*) olarak isimlendirilmektedir. Genel anahtar, şifreleme ve kullanıcı doğrulama işlemleri için kullanılırken, özel anahtarlar şifre çözme ve imzalama işlemleri için kullanılmaktadır.



Şekil 2. Asimetrik şifreleme yöntemi

Alıcının genel anahtarı ile şifrelenen veri, sadece alıcının özel anahtarı ile açılabilir. Gönderici, alıcının genel anahtarı ile şifreleyerek veriyi gönderir. Şifrelenerek gönderilmiş veri, sadece özel anahtara sahip alıcı tarafından okunabilir [12]. Göndericinin özel anahtarı ile imzalanan veri, alıcı ve herkes tarafından, göndericinin genel anahtarı ile doğrulanabilir. Gönderici taraf, kendi özel anahtarını kullanarak veriyi imzalar. Bu imzalı veri, sadece özel anahtara sahip gönderici tarafından gönderilebilir. Asimetrik şifreleme yöntemi Şekil 2'te gösterilmiştir. Bilim dünyasında farklı asimetrik şifreleme algoritmaları geliştirilmiştir. Çeşitli asimetrik şifreleme algoritmalarına ait bilgiler Tablo 2'de gösterilmiştir.

2.1.2. Şifreleme Yöntemlerinin Karşılaştırılması

Şifreleme yöntemlerinin kullanımları göre bazı zayıf ve kuvvetli yönleri vardır. Anahtar uzunlukları ve aynı anahtarların kullanımlarına göre performans değişikliği gösterebilmektedir. Günümüzde şifreleme yöntemlerinin amaçlarına göre, tüm beklentileri karşılayan asimetrik şifreleme yöntemleri, anahtar uzunluklarından dolayı bazı problemleri de beraberinde getirir. Tablo 3'de şifreleme yöntemlerinin çeşitli avantaj ve dezavantajları verilmiştir [13].

Tablo 3. Şifreleme algoritmalarının karşılaştırılması

Yöntem	*Avantajlar*	*Dezavantajlar*
Simetrik Şifreleme	• *Algoritma hızlıdır.* • *Donanım ile birlikte kullanılabilir* • *Güvenlidir*	• *Güvenli anahtar dağıtımı zordur.* • *Kimlik doğruma ve bütünlük ilkesini tamamen gerçekleştiremez.*
Asimetrik Şifreleme	• *Bütünlük, kimlik doğrulama ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.* • *Kullanıcılar anahtarı belirleyebilir.*	• *Algoritma anahtar uzunluklarından dolayı yavaştır.* • *Farklı anahtar uzunluklarından kaynaklanan problemler oluşur.*

3. Hesap Güvenliği

Bir üyelik sistemine ait kullanıcı hesabının tam güvenliği, belirli faktörlere bağlı olarak değişmektedir. Ham verinin son kullanıcıdan alınarak, depolanması veya kaydedilmiş verinin son kullanıcıya aktarılması gibi süreçlerde, korunması gereken veriler, birçok yorumlayıcı işlemden geçmektedir. Başta şifre karmaşıklığı olmak üzere, sistem ve ağ güvenliği, yazılım güvenliği ve veri tabanı güvenliği bir kullanıcı hesabının güvende kalmasını sağlayan temel faktörlerdir.

Tablo 2. Bazı asimetrik şifreleme algoritmaları [10]

Algoritma	*Geliştirici*	*Tarih*
Diffie-Hellman	*Whitfield Diffie , Martin Hellman*	*1976*
RSA	*Ron Rivest (R), Adi Shamir (S) ve Leonard Adleman (A)*	*1978*
ElGamal	*Taher Elgamal*	*1984*
Elliptic Curve Cryptography	*Neal Koblitz ve Victor S. Miller*	*1985*
Paillier	*Pascal Paillier*	*1999*

3.1. Sistem ve Ağ Güvenliği

Bir üyelik sistemine ait sunucu hizmetlerinde güvenlik duvarı ve yetkilendirme hizmetleri, kullanıcı hesaplarının güvenliğini önemli ölçüde etkilemektedir. Kullanıcı hesaplarının yönetimine ait ana yetkilerin ağ üzerinde açık bırakılması, birden fazla kişiye tüm yetki izinlerinin verilmesi hesap güvenliğini tehlikeye düşüren faktörlerdir. Üyelik sistemi bilgilerinin tutulduğu sunucuların (firewall) güvenlik duvarı hizmetlerinin sürekli olarak aktif bırakılması, gereksiz servislerin kapatılması da bilgilerin korunmasını sağlayan etmenlerdendir. SSH portunun değiştirilmesi ve port değiştirme imkânının bulunmadığı durumlarda SSH anahtar-çifti ile kriptolu SSH anahtarı çiftinin karşılaştırılması ile yetkisiz girişler engellenebilmektedir [14].
Ayrıca yetkisiz girişlerin engellenmesi için sistem yöneticisinin vereceği izin kadar deneme imkânı veren Fail2ban gibi servislerin kurulumu sunucunun daha güvende kalmasını sağlayacaktır. DDoS ve Brute Force gibi siber saldırılar aracılığıyla yapılmaya çalışılan yetkisiz girişler, giriş kontrolünü yapan Fail2ban servisi sayesinde otomatik olarak banlanarak, bu IP'lerden yapılan ataklar engellenebilmektedir [15]. İlave bir önlem olarak, fiziksel sunucular üzerinde sanallaştırma yapılarak, tüm fiziki sistemin zarar görmesi engellenmeli ve sanal sunucu yedeklerinin alınması

gerekir [16]. Yedekleme işlemleri sayesinde, en azından kısa süreliğine saldırıya uğramış yazılımlar, yeniden kullanıcıların hizmetine sunularak, saldırıdan en az hasar ile çıkılması hedeflenmelidir.

3.2. Yazılım Güvenliği

Kullanıcı hesaplarının güvenliği, giriş yapılan yazılımların güvenli kodlama standartlarına uygun bir şekilde kodlanması ile yakından ilişkilidir. Yazılım geliştirme aşamasında, yazılım geliştirme süreçleri dikkatli bir şekilde izlenmeli ve sürekli yazılım testleri yapılarak yazılım süreçleri tamamlanmalıdır. Kullanıcı hesaplarının bağlı olduğu yazılımlar ya da sayfaların zayıf yönleri tespit edilerek, yetkisiz girişlerin engellenmesi öncelikli olan bir önlemdir[17]. Son kullanıcıdan alınan bilgilerin güvenli bir şekilde veri tabanlarına kaydedilmesi için, siber saldırılara karşı ilave koruma kodları gerekebilir. Korumalı kodlama sayesinde bilgiler, veri tabanına sorunsuz bir şekilde kaydedilir ve aynı şekilde veri tabanındaki bilgiler kullanıcıların bilgisine sunulabilir. Kullanıcılardan istenilen bilgilerin mutlaka istemci arayüzünde ve sunucuda doğruluk denetimleri yapılmalıdır. Bu sayede yazılımın web uygulaması, javascript temelli XSS (Cross Site Scripting) saldırılarına karşı korunabilmektedir [18].

3.3. Veritabanı Güvenliği

Verilerin iyi planlanmış ve korunmuş yazılım süreçlerinden geçirilerek depolama alanına ulaştırılması, kullanıcı hesabı güvenliğinin bir diğer faktörüdür. Bir veritabanında uzun süre kalacak olan bilgilerin sürekli olarak korunması ve veritabanına ait yetkilerin güncel olarak kontrol edilmesi gerekir [19]. Özellikle veritabanı sistemlerine karşı gerçekleştirilen Dos atakları, sistemde büyük oranda kaynak kullanımına neden olan arama ve istek gönderme işlemleri ile sunucuya aşırı yük bindirilerek, sistemin kullanılamaz hale gelmesine neden olmaktadır. Veri tabanı işlemlerinde, SQL injection sorgu ataklarına karşı yazılım güvenliği ile birlikte sağlanabilen korumalı filtreleme kodları vasıtasıyla veri tabanı güvenliği sağlanmaktadır [20]. Ayrıca verilerin, veri tabanında birden fazla alanda önem sırasına göre farklı tablolarda tutulması da ayrı bir güvenlik önlemidir. AES, MD5 vb. şifreleme algoritmaları kullanılarak bir kullanıcı hesabına ait önemli bilgiler ayrıca şifrelenmelidir. Dinamik haldeki veri akışının ya da statik verilerin korunması için AES şifreleme algoritması ile veri tabanı güvenliği sağlanabilmektedir. Bunun yanı sıra, veri tabanındaki güvenliğin öncelik sırasına göre DES, Triple DES, DESX, 128-bit AES, 192-bit AES, 256-bit AES gibi farklı şifreleme algoritmaları da kullanılmaktadır. Veri tabanı güvenliği için bir şifreleme algoritması kullanmak, uzun bir zaman diliminde kullanıcı hesabının güvenliğini büyük ölçüde sağlayacaktır [21].

3.4. Şifre Karmaşıklığı

Şifre karmaşıklığı, bir kullanıcı hesabı için kullanılan en temel veri güvenliği ilkelerinden biridir. Kullanıcıların hesap oluşturma işlemi esnasında şifrelerini yeniden girilmesi istenerek, gerçekte yanlış bir şifre girip, girmediği kontrol edilir. Ayrıca gerçek bir kişi olup, olmadığını test etmek için catpcha denilen robot kontrolü uygulamalarından yararlanılmaktadır. Bütün bu önlemler, kullanıcıların daha güvenli bir şekilde hesaplarını koruyabilmesi adına yapılan işlemlerdir. Şifrelerin yalnızca rakam ya da harflerden oluşması, en çok bilinen şifrelerin tercih edilmesi veya

kişisel bilgileri hatırlatıcı şifrelerin kullanılması şifrelerin kolay bir şekilde ele geçirilmesine neden olan başlıca hatalı uygulamalardır [22].
Günümüzde 8 karaktere kadar olan şifreler, bilinen yöntemler aracılığıyla dakikalar içinde kırılabilirken, 8 karakter ve daha fazla uzunluktaki şifreler ancak on yıllar içinde kırılabilmektedir. Bu nedenle en az 8 karakter olan hem harf, hem rakam hem de özel karakterlerden oluşan şifreler güçlü şifre olarak kabul edilmektedir [23]. Şifrelerin uzunlukları ve çözülme olasılıkları Tablo 4'de belirtilmiştir.

Tablo 4. Şifre karmaşıklığının karşılaştırılması [16]

Şifre Karmaşıklığı	***Şifre Uzunluğu & Olasılıklar***		
	4 karakter	***8 karakter***	***10 karakter***
Sadece rakamlar	$10^4 = 10000$	$10^8 = 100000000$	$10^{10} = 10000000000$
Sadece semboller	$19^4 = 130321$	$19^8 = 16983563041$	$19^{10} = 6131066257801$
Sadece küçük harf	$26^4 = 456976$	$26^8 = 208827064576$	$26^{10} = 141167095653376$
Küçük + Büyük harf	$52^4 = 7311616$	$52^8 = 53459728531456$	$52^{10} = 144555105949057024$
Rakam + Küçük + Büyük harf + sembol	$81^4 = 43046721$	$81^8 = 645753531245761$	$81^{10} = 12157665459056928801$

Örneğin; 8 karakterli bir şifre oluşturulurken, şifrenin oluşturulma yöntemi ile ilgili olasılıklar göz önüne alındığında, harf, rakam ve özel karakterlerden oluşan bir şifrenin kırılma olasılığı çok düşük olacaktır. Tablo 4'de de görüldüğü gibi, şifre uzunluğu daha fazla olduğunda ve şifreler harf, rakam ve özel karakterler ile daha karmaşık hale getirildiğinde şifrelerin kırılma olasılığı da azalmaktadır. Yazılımcılar, şifre karmaşıklığına özen gösterip kullanıcılara ait şifre alanlarına harf, ve özel karakterler ile girme zorunluluğu getirdiğinde, kullanıcı hesaplarının daha güvenli şekilde oluşturulmasını sağlayabilir [24]. Bu bağlamda yazılımcılar tarafından, şifrelerin sıralı harf ve rakamlardan oluşmaması ve özel karakter içermesi, günümüzde kullanılan çoğu hesap oluşturma işleminde kullanıcılara ayrıca hatırlatılmaktadır. Ayrıca, şifre karmaşıklığı ile birlikte hesap güvenliği için birden fazla güvenlik işlemi de sunulmaktadır [25]. Bu işlemler genellikle robot kontrolü, sms sistemleri, güvenlik soruları ve kimlik doğrulama gibi ilave önlemlerdir. Özellikle bankacılık sektöründe kullanılan tek kullanımlık sms şifre yöntemi, internet bankacılığı dolandırıcılığını %70'lere kadar indirmiştir. Fakat mobil banka şube uygulamalarının yaygınlaşması ile birlikte telefon güvenliği de ayrı bir önem kazanmıştır [26]. Bu nedenle akıllı telefonların sürekli şifre ile korunması, parmak izi ya da yüz tanıma gibi ilave önlemler ile koruma altına alınması bu sorunu en aza indirgeyecektir.

3.5. Hesap Güvenliği için Kullanıcı Temelinde Alınabilecek Önlemler

Hesap güvenliği, sistemci ve yazılımcı tarafından alınan önlemler ile güvenli hale getirildiği gibi aynı zamanda son kullanıcıların da alabileceği önlemler ile daha güvenli hale getirilebilmektedir. Kullanıcılar kendi güvenlik önlemlerini alabildiği takdirde, kullanıcı hesapları daha iyi korunabilecektir. Kullanıcı temelinde alınabilecek önlemler, aşağıdaki gibi sıralanabilir [27]:

- Kullanıcılar, hesaplarına ait şifreleri periyodik olarak değiştirmeli ve aynı şifreleri sürekli olarak kullanmamalıdır.

- Kullanılmayan (sosyal medya, mobil/internet şube banka, forumlar, e-ticaret vb.) hesaplar kapatılmalı ve üyelik sisteminde kişisel bilgilere ait bilgiler tamamen silinmelidir.
- Mobil ya da web tabanlı uygulamalarda üçüncü parti casus yazılımların kurulumu, hesap kurulumu esnasında veya sonrasında kaldırılmalıdır.
- Kimlik avı ve olta saldırılarına karşı özellikle mobil cihazlarda sosyal medya hesapları üzerinden yönlendirilen resmi ya da profesyonel görünümlü sayfalara tıklanmamalı ve kişisel bilgiler girilmemelidir.
- Özellikle sosyal medya hesapları üzerinden giriş izni isteyen sayfaların güvenliği kontrol edilmeli ve bilinmeyen bir uygulama ise, bu tip web sitelerine giriş izni engellenmelidir.
- Hesap güvenliği için bazı e-ticaret sayfalarında kredi kartı vb. banka hesap bilgileri sonraki işlemler için kullanım kolaylığı açısından kaydedilmek istenmektedir. Bu bilgiler ilgili sayfada oluşabilecek her türlü siber saldırıya karşı kaydedilmemeli ve gerekli olduğunda banka bilgileri manuel girilmelidir.
- Kullanıcı hesaplarında e-posta bilgisinin paylaşımı nedeniyle e-posta kutusuna gönderilen web bağlantılarının güvenliği kontrol edilmeli, ilgili kullanıcı hesabına ait bir web bağlantısının doğru bir yönlendirme olduğu kanısına varıldığı takdirde tıklanmalıdır. Aksi takdirde ilgili kullanıcı hesabında kullanılan tüm bilgileri art niyetli üçüncül şahısların eline geçebilmektedir.
- Şifrelerin ele geçirilmesini kolaylaştıran kişisel ad, özel tarihler, memleket vb. şifrelerin yerine karışık şifreler tercih etmemelidir. Örneğin kişisel hatırlama açısından "Sakarya54" gibi bir şifre yerine "$aK@ryA_45" gibi daha karmaşık şifreler tercih edilmelidir.

4. Sonuç ve Tartışma

Bu çalışmada, asimetrik ve simetrik şifreleme algoritmaları incelenmiş ve şifreleme yöntemlerinin kullanıcı hesabı güvenliğine ait etkileri araştırılmıştır. Bir kullanıcı hesabına ait bilgilerin, şifreleme algoritmaları ile şifrelendiğinde daha uzun ömürlü saklanabildiği ve yetkisiz girişlerin engellenerek siber saldırılara karşı korunabildiği gözlemlenmiştir. Ayrıca şifre karmaşıklığının hesap güvenliğindeki rolü incelenmiş ve kullanıcı hesaplarının sistemci ve kullanıcı tarafından nasıl korunabileceği gösterilmiştir. Şifre karmaşıklığının tek başına yeterli olmadığı durumlarda, hesap bilgileri robot kontrolü, kimlik doğrulama, tek kullanımlık sms doğrulama gibi ek yöntemlerle korunabilmektedir. 2000'li yılların başında özellikle akıllı telefonların hayatımıza girmesi ile birlikte başlayan kullanıcı hesabı temelindeki üyelik sistemleri, günümüzde Covid-19 pandemi vakalarının artışı ile birlikte en çok kullanılan mobil/internet uygulamaları olmuştur. Bu durum, güvenlik endişelerini de beraberinde getirmiş, hesap güvenliğinin artırılmasına yönelik önlemler, kaçınılmaz bir hale gelmiştir. Hesap güvenliği, şifre karmaşıklığı ve sistemci-kullanıcı bazlı alınan önlemlerle daha güvenli hale getirilmektedir. Hesap güvenliği, çalışmada bahsedilen önlemler ile koruma altına alınırken, insanlar sanal dünyayı daha etkin kullanmakta ve evlerinde kalarak kendi sağlıklarını da koruma altına almaktadır. Günümüzde tüm dünyayı etkileyen bu durum, eğitimden ticarete, seyahatten turizme kadar her alanda kendini göstermiş, kullanıcı hesabı temelindeki tüm üyelik sistemlerinin kullanılmasını zorunlu hale getirmiştir. Bu zorunluluktan doğan şifreleme ve hesap güvenliği, önümüzdeki yıllarda daha da önem kazanacak ve tüm insanların mecburi olarak dikkat etmesi gereken bir güvenlik faktörü haline gelecektir.

References

[1] Baykara M., Daş R., Tuna G., Yeni Bir Simetrik Şifreleme Algoritması ve Uygulanması, Turkish Journal of Science and Technology,2017; 12:1.

[2] Cihan S., Öztürk E., Kriptoloji ve Kriptoloma Teknikleri, 2015, https://www.slideshare.net/selimcihan/kriptoloji-kriptolama-teknikleri (03 July 2020)

[3] Aumasson J.P., Serious Cryptography- A Practical Introduction to Modern Encryption 1st Ed. San Francisco; 2018.

[4] Tuncal T. Bilgisayar Güvenliği Üzerine Bir Araştirma Ve Şifreleme-Deşifreleme Üzerine Uygulama, Maltepe Üniversitesi Fen Bilimleri Enstitüsü, Master Thesis,İstanbul, 2008.

[5] Güleryüz H. İ., Gri Seviye Görüntülerde Kriptografik Uygulamalar, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Master Thesis, Elazığ, 2014.

[6] Çakmak A., Adalı E., Mesajların Şifrelenmesinde Yeni Bir Yöntem ve Android Uygulaması. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi 2013; 6:1.

[7] Yılmaz M., Ballı S., Veri Şifreleme Algoritmalarinin Kullanimi İçin Akilli Bir Seçim Sistemi Geliştirilmesi. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi 2016; 2:2.

[8] Özbilgin F., Durmuş F., Karagöl S., Yazılı Metni Şifreleyip LSB Yöntemi ile Gizleme. Düzce Üniversitesi Bilim ve Teknoloji Dergisi 2018; 6:3.

[9] Can K.M., Şifreleme (Kriptografi) Nedir? Şifreleme Tarihi ve Geleceği, 2019, https://medium.com/clevelteam/%C5%9Fifreleme-kriptografi-nedir-%C5%9Fifreleme-tarihi-ve-gelece%C4%9Fi-22b4ffe0ea3d (7 July 2020)

[10] Beşkirli, A., Özdemir, D. , Beşkirli, M., Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme. European Journal of Science and Technology, 2019; (Special Issue).

[11] Şifreleme Yöntemleri, İTÜ Bilgi İşlem Daire Başkanlığı, 2013, https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri (28 July 2020)

[12] Şahin F., Modern Blok Şifreleme Algoritmaları, İstanbul Aydın Üniv. Dergisi, 2013;5:17.

[13] Paşaoğluı C., Güler H. Jafari M., Ağ Tabanlı Veri Sızıntısı Tespit ve Önlenmesi Üzerine Bir İnceleme , Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2019;3:2.

[14] Başaranoğlu E., Simetrik Şifreleme Ve Asimetrik Şifreleme Temelleri, 2015, https://www.siberportal.org/blue-team/cryptography/basics-of-symmetric-encryption-and-asymmetric-encryption/ (5 May 2020)

[15] Şeker Y., Fail2Ban Nedir ? Nasıl Kullanılır?. 2020, https://medium.com/@yakupseker/fail2ban-nedir-nas%C4%B1l-kullan%C4%B1l%C4%B1r-6c186444f7f2 (25 July 2020)

[16] Kodaz H., Botsalı F. M., Simetrik Ve Asimetrik Şifreleme Algoritmalarinin Karşılaştırılması, Selçuk-Teknik Dergisi 2010; 9:1.

[17] Arslan İ., Özbilgin İ.G., Sanallaştırma ve Güvenlik: Bir Sanallaştırma Platformu Yapısının İncelenmesi, International Conf. on Computer Science and Engineering (UBMK), 2017; p.221-226.

[18] Beyaz.Net İpucu- XSS Nedir?, https://www.beyaz.net/tr/ipucu/entry/850/xss-nedir (16 June 2020)

[19] Yakut E., Sunucu Güvenliğini Artırma Yöntemleri-Sunucu güvenliği nasıl artırılır?. 2017, https://www.yakuter.com/sunucu-guvenligini-artirma-yontemleri/ (27 May 2020)

[20] Ping C., A second-order SQL injection detection method, IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conf. (ITNEC), 2017,p. 1792–1796.

[21] Arslan İ., Özbilgin İ. G., Virtualization and security: Examination of a virtualization platform structure, Int. Conf. on Computer Science and Eng. (UBMK), 2017, p.221-226.

[22] Of M., Siber Güvenlik Üzerine Bir Araştırma, Bayburt Üniversitesi Fen Bilimleri Dergisi, 2019; 2:2.

[23] Huiping J., Strong password authentication protocols , 4th International Conf. on Distance Learning and Education, 2010,p. 50–52.

[24] Aydın E., Modern Şifreleme Teknikleri ve Güvenlik Teknolojisi, Marmara İletişim Dergisi,1995; 9:9.

[25] Pagar V. R., Pise R. G., Strengthening Password Security through Honeyword and HoneyEncryption Technique, Int. Conf. on Trends in Electronics and Informatics,2017; p. 827–831.

[26] Daist S.M. Shaji R.S. Jayan J.P., Asymetrıc Key Based Data Communıcatıon Under Mobile Cloud System, Global Conf. on Communication Technologies (GCCT),2015;p.559-564.

[27] Yazıcı B., Güçlü Şifre Oluşturmak İçin Öneriler. 2017, https://www.burcinyazici.com/guclu-sifre-olusturmak-icin-oneriler-2596.html/ (12 July 2020)