



# Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması

*Araştırma Makalesi/Research Article*

 Cengiz PAŞAOĞLU<sup>1</sup>,  Emel CEVHEROĞLU<sup>2</sup>

<sup>1</sup>Kişisel Verileri Koruma Kurumu, Ankara, Türkiye

<sup>2</sup>Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi, Ankara, Türkiye

[cengizpasaoglu@kvkk.gov.tr](mailto:cengizpasaoglu@kvkk.gov.tr), [emel.cevheroglu@gazi.edu.tr](mailto:emel.cevheroglu@gazi.edu.tr)

(Geliş/Received:30.04.2019; Kabul/Accepted:24.04.2020)

DOI: 10.17671/gazibtd.559235

**Özet**— Bilgi toplumunun oluşum aşamalarından günümüze kadar veri, verilerin elektronik ortamlar dahil işlenmesi, saklanması ve paylaşılması gibi birçok yeni gelişme yaşanmış ve hayatımıza çok sayıda yeni kavram girmiştir. Günümüzde insana ait, kişiyi direkt veya dolaylı yollardan tanımlayabilecek her türlü bilgi olarak görülen kişisel veri kavramı çok önem kazanmış ve söz konusu verilerin korunması teknolojik gelişmeler karşısında yadsınamaz hale gelmiştir. Kişisel veri olarak bir kişinin adı, adresi, kimlik numarası, pasaport numarası, sağlık bilgisi gibi veriler sayılabilir. Bazen kişiyi tanımlamak için tek bir veri yeterli olabilirken bazen de birden fazla verinin birleştirilmesiyle bir kişiye ulaşmak mümkün olabilmektedir. Bu yüzden artık bireyler açısından kişisel mahremiyetini sağlamak ve bilgilerini güvenli olarak koruyabilmek için verilerin güvenli olarak saklanabileceği ortamlar önemli hale gelmiştir. Veri saklama ortamları denildiğinde ise aklımıza daha çok, son yıllarda giderek gelişmekte olan ve popülerliği her geçen gün daha da artan “Bulut Bilişim” gelmektedir. Bulut bilişim, verilerin saklanması konusunda bizlere birçok kolaylık sağlarken aynı zamanda mahremiyet ve kişisel verilerin korunması açısından ise birçok risk de taşımaktadır. Bu çalışmada, bulut bilişim sistemlerinin avantajları, kişisel verilerin korunması açısından içerisinde barındırdığı riskler, söz konusu risklere karşı alınabilecek güvenlik önlemleriyle birlikte özellikle şifreleme yöntemlerine değinilmiş, bununla birlikte kişisel verilerin korunması alanında yapılan hukuki düzenlemelerin bulut bilişim sistemleri açısından değerlendirmesi ve kişisel haklar üzerinde de durulmuştur.

**Anahtar Kelimeler**— bulut bilişim, kişisel verilerin korunması, kişisel veri, kişisel verilerin güvenliği, kişisel verilerin saklanması, kişisel verilerin şifrelenerek bulutta tutulması

## Protection of Personal Data in the Cloud Computing Systems using Cryptology Methods

**Abstract**— From the formation stages of the Information Society to the present day, there have been many new developments such as data, data processing, storage and sharing them in electronic environment and besides many new concepts have entered our lives. Nowadays, the concept of personal data, which can be defined as any kind of information that can define directly or indirectly to a real person, has gained importance and the protection of such data has been undeniable in the face of technological developments. Personal data can include a person's name, address, identification number, passport number and disease information etc. Sometimes a single data can be sufficient to identify a person, but sometimes more than one data needs to be combined. Therefore, environments where privacy is ensured and personal data is securely stored become very important for the individuals. When data storage is mentioned, Cloud Computing, with the improving popularity in recent years, comes to our mind. While cloud computing provides us with a lot of convenience in data retention, it also has many risks when it comes to privacy and personal data protection issues. In this article, the advantages of cloud computing systems, the risks involved in storing personal data, the security measures, particularly cryptology methods that can be taken against these risks as well as the legal regulations in this field considering cloud computing systems and personal rights are emphasized.

**Keywords**— cloud computing systems, protection of personal data, personal data, security of personal data, storage of personal data, keeping personal data in the cloud by encryption

## 1. GİRİŞ (INTRODUCTION)

Teknolojinin gelişmesi ve günümüzde çokça bahsedilen dijital çağa geçmiş olmanın sonucu olarak veri mahremiyeti konusu daha da önemli hale gelmiştir. İnternetin yaygınlaşması ve interneti hayatımızın her alanında kullanıyor olmamızdan dolayı farkında olarak veya olmayarak birçok kişisel verimizi sanal ortamlarda paylaşmaktayız. Bilgi toplumundan bu yana veri ekonomik bir faktör haline gelmiş ve alınıp satılabilir olmuştur. Bu durum kişisel verilerin korunması konusunun önemini artırmış ve insanların bu hususta daha dikkatli olmalarını zorunlu kılmıştır. Artık insanlar verileri toplanırken, işlenirken, paylaşılırken veya depolanırken bu konuda güvende olduklarını bilmek istiyorlar. Özellikle işlenen kişisel veri miktarının dijital çağ kapsamında hayatımıza giren büyük veri, yapay zeka ve nesnelerin interneti gibi kavramlar sonucu çok fazla olması ve bunların güvenli olarak saklanması ihtiyacıyla birlikte birçok veri depolama ortamı, aygıtı ve sistemi geliştirilmiştir. Veri depolamada önceden kullanılan fiziksel cihazlar bellek yetersizlikleri, maliyetlerinin yüksek olmaları ve her an erişilebilir olamamaları gibi kısıtlamaları yüzünden yerini sanal ortamlarda gerçekleştirilen depolama sistemlerine bırakmıştır. Bu sorunlara çözüm olması adına verilerin sanal sunucular üzerinde depolanması fikri sonucu bulut bilişim kavramı hayatımıza girmiştir. Bulut bilişim, sunucularında tutulan verilere internet erişimi sayesinde her an ulaşabilmemizi sağlayan, sistemin sunduğu hizmetlerden istediğimiz ölçüde yararlanmamıza fırsat sağlayan internet tabanlı bir teknoloji servisedir. Bulut bilişime Google Drive, iCloud, Dropbox, SkyDrive, Yandex.Disk gibi örnekler verilebilir. 1950 ve 1960'lı yıllarda ortaya atılan varsayımlardan geliştiği öne sürülen Bulut Bilişim'in tam olarak kaynağı bilinmemektedir. İlk gerçek bulut bilişim hizmeti olarak Amazon S3 geliştirilmiştir. S3 kapsamındaki en önemli işlemlerden birisi "kullandıkça öde modeli" olan fiyatlandırma modelidir. Bu model halen kullanılmakta olan bulut bilişim sistemlerinin fiyatlandırmaları için de kullanılmaktadır.

Bulut bilişim düşük maliyeti, yüksek performansı, fiziksel materyal gerektirmemesi, esnek olması gibi özellikleri ile bizlere birçok avantaj sağlamaktadır; ancak bu avantajların yanında internet erişimi gerektirmesi, hızının erişim kalitesine bağlı olması, güvenlik açıklıkları açısından barındırdığı risk ve tehditler gibi dezavantajları da bulunmaktadır.

Bu çalışmada ilk olarak veri kavramı ile birlikte kişisel veri açıklanmış, elde edilen verilerden kişiler hakkında nasıl bilgi sahibi olunabileceği ve bu verilerin nasıl saklanması gerektiği üzerinde durulmuştur. Sonrasında ise veri depolama sistemleri açısından bilgi teknolojilerinde en önemli gelişmelerinden biri olan bulut bilişim sistemlerinin geçmişten günümüze gelişimi, kullanım alanları, avantaj ve dezavantajları incelenmiştir. Daha sonra ise her alanda olduğu gibi bulut bilişim sistemlerinde de bulunan riskler, bunları önlemek için yapılması gerekenler, bulut bilişim sistemlerinde alınması

gereken güvenlik önlemleri ve özellikle şifreleme yöntemleri gibi konular üzerinde durulmuştur. Son bölümde de kişisel verilerin korunması kapsamında yapılan yasal düzenlemelerin dünya ve ülkemiz açısından tarihçesine değinilmiş, bulut ortamlarının konumunun yasal durumu ile bulut bilişim sistemlerinde kişisel verilerin güvenliği konusunda hizmet sağlayıcıların hukuksal sorumlulukları ve veri güvenliğinin sağlanması konuları anlatılmıştır.

## 2. KİŞİSEL VERİ VE KİŞİSEL VERİLERİN MUHAFAZASI (PERSONAL DATA AND STORAGE OF PERSONAL DATA)

### 2.1. Kişisel Veri Nedir? (What is Personal Data?)

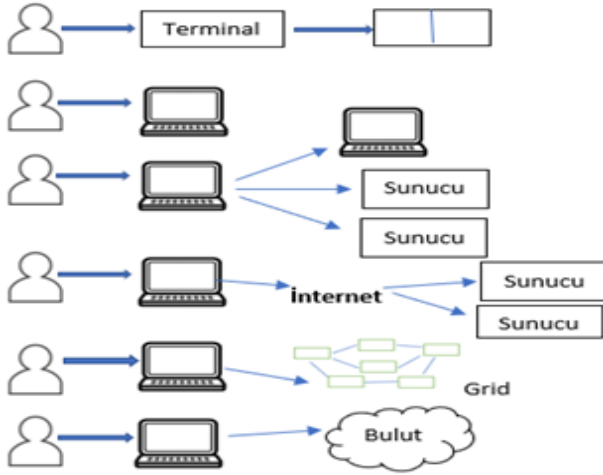
Kişisel veri, bir kişiyi doğrudan veya dolaylı yollardan tanımlayan veya başka verilerle eşleştirildiğinde tanımlayabilecek potansiyelde olan yani veri üzerinden kişinin bulunmasına olanak veren verilerdir [1]. Veri dijital çağda büyük önem taşımaktadır. Alınıp, satılabilen bir araç olarak görülen veri özellikle pazarlama şirketlerinin ve büyük şirketlerin müşteri verileri üzerinden kendilerini geliştirmeleri, müşteri beklentilerine cevap verebilecek nitelikte planlamalar yapması açısından yani müşteri ilişkileri yönetimi (CRM) çalışmalarında çok önemli hale gelmiştir. Kişisel verilerin işlenmesi konusunda çok dikkatli olmak gerekmektedir. Çünkü kişisel veriler ülkemiz de dâhil olmak üzere birçok düzenlemede özel hayatın gizliliği kapsamında anayasal güvence altına alınmış önemli verilerdir ve mahremiyete zarar verebilecek riskler barındırırlar. Kişisel verilerin işlenmesi sırasında mevcut yasal düzenlemelere göre hareket edilmeli, genel kurallara dikkat edilip uyulmalı, gerekli olan güvenlik önlemleri alınmalı ve kişiler verilerinin işlenmesi hususunda mutlaka bilgilendirilmeli, başka bir hukuki dayanak olmadan veri işlenmek isteniyorsa ancak kişilerin açık rızaları alınarak söz konusu veriler işlenmelidir.

### 2.2. Kişisel Verilerin Muhafazası (Storage of Personal Data)

Bulut bilişim sistemlerinin yaygınlaşmasından önce veriler dâhili depolama birimlerinde veya manyetik bant, disket sürücü, mini disk, taşınabilir bellek, CD/DVD gibi harici depolama birimlerinde tutulmaktaydılar. Söz konusu depolama birimleri teknolojinin gelişmesi ve değişen ihtiyaçlar yüzünden sürekli gelişim gösterdi. Bu gelişim süreçleri incelendiğinde veri depolama birimlerinde gigabayt başına düşen maliyetin azaldığı görülmektedir [2]. Bulut bilişimin yaygınlaşmasıyla bahsi geçen depolama birimlerinin kullanımı azaldı ve herhangi bir fiziksel materyale ihtiyaç duyulmadan verilere internet ortamı üzerinden kolayca ulaşılabilir duruma gelindi. Bulut bilişim ile hem maliyette düşüş yaşanarak avantaj elde edildi, hem de fiziksel materyale duyulan ihtiyaç gerekliliğinin önüne geçilmiş oldu.

### 3. BULUT BİLİŞİM SİSTEMLERİ (CLOUD COMPUTING SYSTEMS)

Bulut bilişim internet bağlantısıyla erişim sağlanabilen, uzak sunucu desteğiyle beraber verilerin saklanması, işlenmesini ve verilere her an erişim sağlanarak kullanılmasını sağlayan bir servistir. Bulut bilişim, hizmet sağlayıcılarının sunduğu altyapı desteği ile birçok kişi tarafından paylaşılarak kullanılmakta ve sunucunun sanallaştırma özelliği ile her kullanıcı kendine ait alanı bağımsız olarak kullanabilmektedir [3].



Şekil 1. Bilgi İşlem Geçmişi [4]  
(History of Information Processing)

Şekil 1’de ana bilgisayarlardan başlayarak bilişim alanında yaşanan gelişim süreci görülmektedir. Burada yer alan merkezi işlem kullanıcı ile terminaller arasında olan veri paylaşımından itibaren kullanılan terminal yapısının yerini önceleri bilgisayarlar, daha sonra bilgisayarlar üzerinde kullanılan internet ağ yapısı alırken günümüzde ise bu sistem daha da gelişmiş ve söz konusu işlemler artık bulut bilişim sistemleri üzerinden yapılabilmektedir hale gelmiştir [4].

Bulut Bilişim’in kaynağı tam olarak bilinmemekle birlikte araştırmacıların bazıları bulut bilişimi 1960’larda John McCarthy’nin bilgi işleminin bir kamu hizmeti şeklinde düzenlenebileceği görüşüne, bazıları ise 1950’lerde Herb Grosch’un terminaller kullanılarak dünyanın 15 büyük veri merkezinden çalışan bir sistem kullanacağı görüşüne dayandırmaktadırlar [5].

#### 3.1. Bulut Bilişim Sistemlerinin Avantajları (Advantages of Cloud Computing Systems)

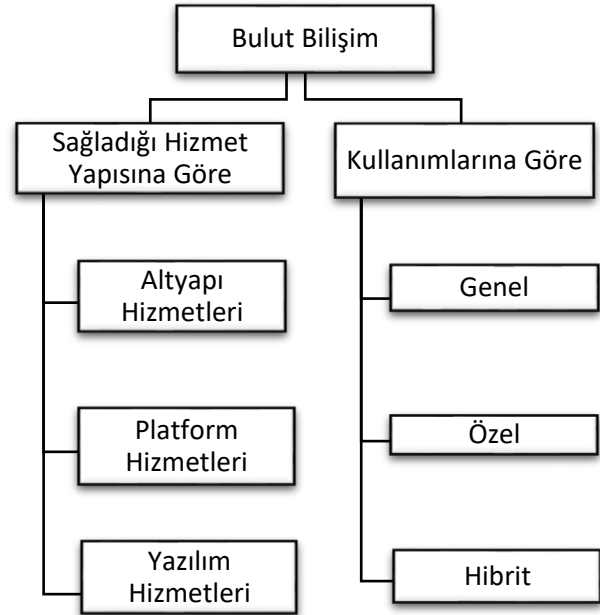
Bulut bilişim bizlere en başta düşük maliyet olmak üzere birçok avantaj sağlamaktadır. Bulut bilişim sayesinde sistem odaları veya veri merkezleri gibi maliyeti yüksek hizmetler yerine düşük maliyetli sanal sunucu desteği sağlanarak ucuz ve kolay yoldan veri depolama yapılabilmektedir. Bulut bilişimde “kullandığın kadar öde” sloganıyla hareket edilerek fazla maliyet durumunun ve iş yoğunluğuna göre oluşan trafiğin önüne geçilmiş

olur. Esneklik özelliği sayesinde işlerimizin yoğun olduğu dönemlerde genişleyen sunucu desteği, normal durumlarda tekrar küçülerek dönemsel yoğunluğa çözüm getirir. Özellikle küçük ve orta ölçekli şirketler için maliyetin düşük olmasından dolayı bulut bilişim hizmetleri çok fazla tercih edilmektedir. Bir diğer avantaj ise internetin olduğu her ortamda verilerin her an ulaşabilir durumda olmasıdır [6,43].

#### 3.2. Bulut Bilişim Sistemlerinin Dezavantajları (Disadvantages of Cloud Computing Systems)

Bulut bilişimin avantajlarının yanında dezavantajları da vardır. Bunlardan ilki internet erişiminin olmadığı yerlerde kullanılamıyor olmasıdır. İnternet erişiminin iyi olduğu durumlarda kolayca kullanılabilirken, internet erişiminin olmadığı durumlarda bulut bilişim üzerinden verilere erişilemez. Bulut bilişim sistemlerinde veri alışveriş hızı internet hızına bağlıdır, düşük hızla sahip bir internet erişiminin olması durumunda bulut bilişimde verilere erişim sağlanması zor olacaktır. Aslında bulut bilişime erişim hâlihazırda internet hızına bağlıdır. Bulut bilişimin bir diğer dezavantajı ise kurumun veya kişinin hizmet aldığı firmaya bağımlı hale gelmesi ve beraberinde gelen veri ihlali riskidir. Bulut bilişimde tutulan verilerin tam olarak hangi ülke ya da hangi hizmet sağlayıcısında tutulduğunun bilinmemesi veya söz konusu hizmet sağlayıcılarının güvenlik prosedürleri hakkında net bilgiye sahip olunamaması kişileri veri ihlali konusunda kuşkuya düşürmektedir [6].

#### 3.3. Bulut Bilişimin Sınıflandırılması (Classification of Cloud Computing)



Şekil 2. Bulut Bilişim Sınıflandırılma Şeması [7]  
(Classification Scheme of Cloud Computing)

Şekil 2’de kullanım alanları ve hizmet yapısına göre bulut bilişim sınıflandırması gösterilmiştir.

### 3.3.1. Sağladığı Hizmetlere Göre (According to the Services)

Bulut bilişim sistemleri sağladığı hizmete göre üç ana başlıkta sınıflandırılmıştır. Bu hizmetler aşağıda detaylı olarak ele alınmıştır.

#### a) Altyapı Hizmetleri (Infrastructure Services)

Bu hizmet kapsamında kullanıcılara, yazılımların bulundurulabileceği ve çalıştırılabileceği işleme, depolama ve temel hesaplama kaynakları gibi donanım desteği sağlanır [8].

Bazı şirketler hizmetlerini, web sitelerinde tutmak için sunucu satın alırlar. Alınan sunucular fiyat açısından maliyetli olabileceği gibi bu sunucularla ilgilenmek ve bakım onarım gibi hizmetleri gerçekleştirmek için ek bir insan gücüne de ihtiyaç olacaktır. Ancak bulutlardan alınacak altyapı hizmetleriyle bu sorun ortadan kaldırılabılır [9].

Kullanıcılar donanım satın almak yerine talep üzerine altyapı hizmeti olarak ödeme yaparlar. Hizmet sağlayıcı altyapının düzenli işleyişinden sorumluyken kullanıcı o altyapı üzerine kurulan yazılım, platform ve verilerden sorumludur. Geleneksel barındırma (hosting) hizmetinden farklı olarak altyapı hizmetinde, fiziksel sunucunun aylık veya yıllık kiralanması yerine sanal makineler kiralanarak ihtiyaca uygun olarak kullanılmaktadır. Kullanıcıların sanallaştırma, sunucular, depolama, ağ yapısı yönetimi ve kontrolü gibi görevleri bulunmamaktadır, ancak altyapı desteği üzerine kurulan işletim sisteminin, verilerin veya kullanılan ara yazılımların sorumluluğu kullanıcıya aittir. Amazon EC2 (Elastic Cloud Computing) ve S3 (Simple Storage Service) bu hizmete örnek olarak verilebilir [10].

#### b) Platform Hizmetleri (Platform Services)

Platform hizmetleri kullanıcılara programlama ve bu programları yürütme imkânı sağlar. Kullanıcı desteklenen programlama dilleri, yazılım kütüphaneleri ve araçlar kullanarak kendi uygulamalarını geliştirebilmekte ve bunu kolaylıkla bulut altyapısına dağıtabilmektedir. Altyapı hizmetinde olduğu gibi burada da kullanıcının bulut altyapısını yönetmek veya kontrol etmek gibi bir sorumluluğu bulunmamaktadır, ancak kullanıcı bulut altyapısına dağıtılmış olan uygulamalar üzerinde kontrol gerçekleştirebilir. Google App Engine en çok bilinen platform hizmeti örneklerinden biridir. Google App Engine, aynı sistem üzerinde uygulamalar oluşturmaya olanak sağlayan bir platformdur. Microsoft Azure, Force.com da benzer şekilde platform hizmeti sunmaktadır [10].

#### c) Yazılım Hizmetleri (Software Services)

Bu hizmet kapsamında kullanıcıların yazılımları veya uygulamaları bulutta servis olarak bulundurulur ve kullanıcılar bu yazılım hizmetlerine abonelik açtıklarında tarayıcılar aracılığıyla ulaşırlar. Kullanıcıların verilerinin ayrılmasında kimlik doğrulama ve yetkilendirme güvenlik politikaları kullanılır. Birçok CRM (müşteri ilişkileri yönetimi), ERP (kurumsal kaynak planlama) sistemleri gibi bulut yazılım hizmeti örnekleri bulunmaktadır. Salesforce.com, Force.com’u temel olarak oluşturulmuş yazılım hizmetlerinin en bilinen örneklerinden olan bir CRM sistemidir [10]. Başka bir örnek olarak Microsoft Office 365 servisi verilebilir. Yazılım hizmeti bir yazılımın temel mimari yapısını oluşturmak olarak görülmemelidir. Mevcut yazılımın yanında daha fazla yazılım sunmanın yolunu oluşturan bir iş modeli olarak yorumlanmalıdır [9].

### 3.3.2. Kullanım Şekline Göre (According to the way of use)

Bulut bilişim sistemleri kullanım şekline göre de üç ana başlıkta sınıflandırılmıştır. Bu hizmetler aşağıda ele alınmıştır.

#### a) Genel Bulut (Public Cloud)

Genel bulutta kullanıcı sınırlaması yoktur. Bünyesinde bulunan hizmetler sanallaştırılmış bir ortamda toplanmıştır ve internet üzerinden erişilebilirler. Genel bulut servislerine servis olarak yazılım (SaaS), bulut tabanlı web barındırma (IaaS) ve yazılım geliştirme ortamları (PaaS) örnek olarak verilebilir. Kullanıcı sadece paylaşılmış kaynaklar üzerinde kendi alanını kullanabilir. Bulut sağlayıcısı veri merkezlerini çok farklı yerlere kurabilir. Bu durumda kullanıcının verisinin fiziksel olarak nerede tutulduğunu bilme hususu ortadan kalkmaktadır. Kullanıcılar bu husus yüzünden kendi özel bulutlarına (private cloud) sahip olma eğilimindedirler [11].

#### b) Özel Bulut (Private Cloud)

Belirli bir kurum veya kuruluş için oluşturulmuş olan bu bulutta hizmet sağlayıcı kurumun kendisi olabilir veya üçüncü bir bulut hizmet sağlayıcısından da hizmet satın alınabilir.

#### c) Hibrit Bulut (Hybrid Cloud)

İki veya daha fazla bulut çeşidinin birleştirilmiş yapısıdır. Hibrit bulutun avantajı olarak önemli veriler özel bulutta tutulurken, aynı anda daha az kritik veriler genel bulutta tutulabilmektedir. Bu avantajının yanında özel ve genel bulutlar bir arada kullanıldığında yönetim sorumluluğu iki bulut sağlayıcı arasında bölünür. Bu durum yüzünden güven sorunu veya karşılıklı çakışma sorunları oluşabilir. Senkronizasyon, verilerin güvenliği gibi konularda da dikkat edilmesi gereken bir bulut çeşididir [11].

#### 4. BULUT BİLİŞİM SİSTEMLERİNDE VERİ MAHREMİYETİ (DATA PRIVACY IN CLOUD COMPUTING SYSTEMS)

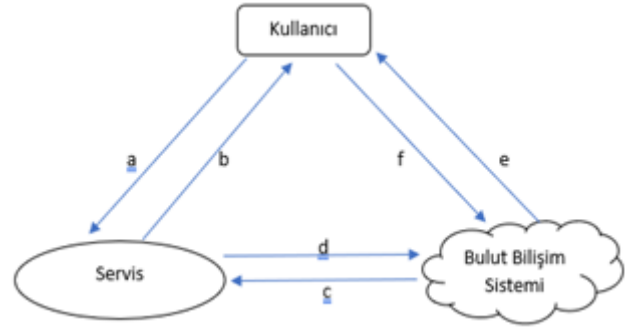
Bilgi sistemlerinde risk yönetimi konusunda birçok standart belirlenmiştir. Bunlara örnek olarak kuruluşların kullandıkları, ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı, bu standardı destekler düzeyde tasarlanmış olan ISO/IEC 27005 Bilgi Güvenliği Risk Yönetim Standardı ve risk yönetim süreçlerini bütünleştirmek amacıyla geliştirilmiş ISO 31000:2018 Risk Yönetimi Standardı sayılabilir. Bunlara ek olarak Türk Standartları Enstitüsü tarafından bilişim alanında bazı standartlar ve rehberler oluşturulmuştur. Bulut bilişim ile alakalı olarak TSE bünyesinde faaliyet gösteren Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubu tarafından Bulut Bilişim Güvenlik ve Kullanım Standardı Taslağı 2014 yılında oluşturulmuştur. Söz konusu taslakta kuruluşların iş süreçlerinde koruması gereken değerli varlıklar listesi yani varlık envanteri belirlenmiştir. Anılan varlık envanterinde risklerden etkilenebilecek en büyük kısmı, veri varlıkları oluşturmaktadır. Bu veri varlıkları içerisinde kişisel veriler büyük risk altında olarak belirtilmiştir [11].

Diğer taraftan Bulut Güvenliği Birliği (The Cloud Security Alliance, CSA), bir rehber yayınlamıştır. Bu rehber Bulut Kontrolleri Matrisi (CCM) olarak da adlandırılmaktadır. Söz konusu rehber, başlıca bulut bilişim risklerini değerlendirmeyi ve bu risklere karşı güvenlik önlemleri konusunda kişileri/kuruluşları bilgilendirmeyi amaçlayan 13 alandan 98 farklı bulut güvenlik kontrolünü içermektedir. Tüm bu belirlenen 98 farklı bulut güvenlik kontrolleri ISO 27001-27005 gibi standartlarla da eşleştirilmiştir [12].

##### 4.1. Bulut Bilişimde Mahremiyet Riskleri (Privacy Risks in Cloud Computing)

Bulut bilişim sistemleri birçok güvenlik ve mahremiyet risklerini de barındırmaktadır. Bulut bilişim kullanıcıları, bulut bilişim kullanan şirketler, bulut hizmet sağlayıcısı, bulut platformları geliştiren programcılar, bu platform üzerinden yazılım geliştiren yazılımcılar söz konusu risklerden etkilenebilecek olan kitlelerdir. Bahse konu riskler yüzünden kişisel verilerin üçüncü kişilerin ellerine geçmesi ve bunların kötüye kullanılması, ayrıca bu durumun oluşmasıyla ve ortaya çıkmasıyla birlikte itibar ve prestij kayıpları gibi istenmeyen durumlar da yaşanabilir.

Bulut bilişim kullanımı sonucu oluşabilecek sorunlar; yazılımsal ve donanımsal olabileceği gibi dışarıdan gelebilecek saldırılar yüzünden de olabilir. Bulut bilişimde muhtemel saldırı yüzeyleri Şekil 3'te görüldüğü gibidir.



Şekil 3. Bulut Bilişimde Saldırı Yüzeyleri  
(Attack Surfaces in Cloud Computing)

Şekil 3'te yer alan saldırı yüzeylerinde bulunan kullanıcı, servis ve bulut arasındaki yüzeyleri sınıflandıracak olursak a; genel olarak bir istemci programının, sunucuya sağladığı ortak ortam olarak yorumlanmaktadır. SSL sertifikası sahteciliği, tarayıcı önbelleklerine yönelik yapılan saldırılar, posta istemcilerine kimlik avı saldırıları olarak bilinen oltalama (phishing) saldırıları gibi HTML tabanlı bir hizmet için tarayıcı tabanlı saldırılar genel olarak bu yüzey grubundadır [13]. b; Kullanıcı yüzeyine yönelik olan saldırı çeşitleridir. Bu durum sunucu-istemci arabirim oluşturma olarak da yorumlanabilir. Arabellek taşması (buffer overflow) veya veritabanı üzerinde açık olan bir tablo üzerine yapılan SQL Injection işlemleri, bu yüzeyde gerçekleştirilen saldırılardır [14]. c; Bu yüzeyde ise kaynağa yönelik gerçekleştirilen kaba kuvvet saldırıları, bulut sağlayıcılarına yönelik daha fazla kaynak sağlamak veya sonlandırmak için DOS (Denial-of-Service) saldırılarıyla tetikleme saldırıları verilebilir [13,44]. d; Bulut sağlayıcısının gerçekleştirebileceği her türlü saldırı olarak değerlendirilebilir. Diğer yüzeylere göre belki de en önemli saldırı yüzeyidir. Gizlilik ve mahremiyetle ilgili saldırılar, zararlı girişimler bu yüzeydeki saldırı çeşitleridir [14]. e; Bulut kontrollerinde oluşan saldırılardır. Normalde aralarında mutlaka bir hizmet olduğundan dolayı bu yüzeyi tanımlamak zordur. f; Bu yüzeyde bir kullanıcının bulut üzerinden başka kullanıcı kayıtlarına erişim sağlayarak o kullanıcının bulutla sağlanmış olan hizmetleri üzerinde işlemler yapmak gibi kimlik avı benzeri girişimleri içerir [13].

##### 4.2. Şifreleme Yöntemleri (Encryption Methods)

Bulut bilişim sistemleri kullanırken, yüklemiş olduğumuz kişisel verilerin gizliliği ve üçüncü kişiler tarafından anılan verileri ele geçirme ya da verilere hukuka aykırı olarak erişim hususları düşünüldüğünde, bu tür durumları önlemek adına alınması gereken önlemlerin başında şifreleme işlemleri gelmektedir. Kişisel Verileri Koruma Kurulu tarafından hazırlanan "Kişisel Veri Güvenliği Rehberinde de vurgulandığı üzere bulut sistemlerinde kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle verilerin şifrelenmesi, bulut ortamlarına şifrelenerek atılması, mümkün olduğu durumlarda özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekecektir [15]. Bu kapsamda kullanılacak yöntemler aşağıda açıklanmıştır.

#### 4.2.1. Homomorfik (Eş biçimli) Şifreleme (Homomorphic Encryption)

Bulutta saklanan veriler üzerinde ek işlemler yapılmak istendiğinde şifrelerin bulut sağlayıcı tarafından çözülmesi sonrasında işlemin gerçekleştirilip, verilerin tekrar şifreleme işlemleri yapılarak kullanıcıya gönderilmesi veya bulutta depolanması gibi işlemler gerekmektedir. Bu durum ek bir hesaplama maliyeti gerektirmekte ve kullanıcıların gizli anahtar bilgilerini bulut sağlayıcılar ile paylaşmalarının gerekliliğini doğurmaktadır. Gizli anahtarların paylaşılma durumu ise verilerin gizliliğini etkilemekte ve veri ihlali olasılığını artırmaktadır.

Söz konusu durumu önlemek adına veriler homomorfik şifreleme kullanılarak şifrelenebilir. Homomorfik şifreleme ile verilerin şifreleri çözülmeden işlemler yapılabilmektedir. Homomorfik şifrelemede istemci verileri şifreleyerek sunucuya gönderir, sunucu kendisine gelen şifrelenmiş veriler üzerinde gerekli f fonksiyonu işlemlerini yapar ve hesaplanan şifreli sonucu istemciye gönderir. İstemcide hesaplama sonucu gizli anahtar kullanılarak deşifre edilir ve böylece verilerin gizliliği ve güvenliği sağlanmış olur [16].

Homomorfik şifreleme, karşı tarafa gönderilmek istenilen metinler üzerinde yapılan cebirsel işlemler ile şifreleme işlemleri sonucunda oluşan yeni şifreli sonucun şifresi çözüldüğünde oluşan sonuç ile aynı cebirsel işlemlerin açık metinlerde yapılmasıyla elde edilen sonucun, aynı olmasını sağlayan bir şifreleme tekniğidir [16]. Yani  $Enc(b)$  ve  $Enc(c)$ 'den  $Enc(f(b,c))$ 'yi hesaplayabiliyorsak yapılan şifreleme homomorfik şifrelemedir. Buradaki f bir fonksiyon belirtir ve toplama ve çarpma işlemleri gibi matematiksel işlemleri içerir [17]. Homomorfik şifrelemenin formülü esas olarak eşitlik (1) ve eşitlik (2)'de görüldüğü gibidir.

$$\forall b, c \in Q \text{ iken } b+c=Dec_K(Enc_K(b)+Enc_K(c)) \quad (1)$$

$$\forall b, c \in Q \text{ iken } b*c=Dec_K(Enc_K(b)*Enc_K(c)) \quad (2)$$

Eşitlik (1) ve eşitlik (2)'de yer alan  $Enc$  şifreleme işlemini,  $Dec$  şifrenin çözülmesi işlemini ve  $K$  ise kullanılan gizli anahtar ifade etmektedir.

Günümüzde homomorfik şifreleme ile toplama ve çarpma işleminin yanında çıkarma, XOR veya sayıların üssünü alma işlemleri gibi işlemler de yapılabilmektedir. Diğer işlemlerin de yapılabilmesi için bu tarz şifreleme algoritmalarının geliştirilmesi gerekmektedir [18]. Homomorfik şifreleme genel hatlarıyla toplama işlemine göre homomorfik özellik gösterenler ve çarpma işlemine göre homomorfik özellik gösterenler olarak ikiye ayrılmaktadır. Toplama ya da çarpma özelliklerinden herhangi birini taşıyan algoritmalar kısmi homomorfik şifreleme, her iki özelliğin de bir arada bulunduğu algoritma ise tam homomorfik şifreleme olarak değerlendirilmektedir. Paillier ve Goldwasser-Micali

şifreleme sistemleri toplama özelliğine göre değerlendirilen sistemler sınıfında yer alırken RSA (Rivest-Shamir-Adleman) ve El Gamal şifreleme sistemleri çarpma özelliğine göre değerlendirilen sistemler sınıfındadır.

##### a) Paillier

1999 yılında Pascal Paillier tarafından bulunarak onun adının verildiği olasılığa dayanan bir açık anahtar algoritmasıdır. Homomorfik şifrelemenin toplama özelliğine göre olan algoritma sınıfında yer alır. İlk olarak iki büyük asal sayı seçilir. Bu seçilen asal sayılar p ve q ismiyle ifade edilecek olursa seçilen bu sayıların eşitlik (3)'de yer alan formülü sağlaması gerekmektedir [19].

$$EBOB(pq, (p-1)(q-1))=1 \quad (3)$$

Eşitlik (3)'de yer alan formülde de görüldüğü gibi seçilen sayıların çarpımıyla, birer sayı eksiklerinin çarpımlarının en büyük ortak böleninin 1 olması gerekmektedir. Sonrasında  $p*q$  sonucu n değerine,  $EKOK(p-1,q-1)$  değeri de  $\lambda$  değerine eşitlenir. Rastgele bir g değeri  $g \in Z_{n^2}^*$  eşitliğine göre seçilir. L fonksiyonu  $L(u)=u-1/n$  şeklinde tanımlanmak üzere,  $\mu=(L(g^\lambda \text{ mod } n^2))^{-1} \text{ (mod } n)$  değeri hesaplanarak kontrol edilir. Sonuç olarak bu işlemlerden şifreleme için (n,g) açık anahtarı; şifreleme işlemini çözmek için ise  $(\lambda,\mu)$  gizli anahtarı elde edilir. Şifreleme işleminde m şifrelenecek mesaj olarak kabul edildiğinde, rastgele bir r değeri seçilir ve şifreli mesaj eşitlik (4)'de verildiği gibi c değerine eşitlenir [19].

$$c=g^{m.r^n} \text{ (mod } n^2) \quad (4)$$

Şifrelenmiş olan c metninin tekrar eski şifrelenmeden önceki haline yani m değerine çevirmek için eşitlik (5)'de yer alan formül kullanılır.

$$m=L(c^\mu \text{ (mod } n^2)) * \mu \text{ (mod } n) \quad (5)$$

Homomorfik şifrelemenin özellikleri aynı şekilde Paillier algoritması için de geçerlidir. Söz konusu algoritma kullanılarak da verilerin güvenliği sağlanabilir.

##### b) Goldwasser-Micali

1982 yılında Shafi Goldwasser ve Silvio Micali tarafından geliştirilen asimetrik bir anahtar şifreleme algoritmasıdır. Goldwasser-Micali Algoritması da Paillier Algoritması gibi Homomorfik Şifreleme'nin toplama özelliğine göre olan algoritmalarındadır. Kesin olarak güvence altına alınan ilk olası açık anahtar şifreleme algoritması olan Goldwasser-Micali Algoritması verimli bir algoritma olarak yorumlanmamaktadır. Bunun sebebi baştaki düz metin şifrelendiğinde neredeyse yüz kat daha büyük bir metin haline gelmesindedir. Goldwasser ve Micali semantik güvenlik kavramını öne sürmüşlerdir. Paillier Algoritması gibi anahtar üretme, şifreleme ve şifre çözme adımlarından oluşmaktadır. Bu algoritma bir x değerinin

kare mod N olup olmadığına karar vermenin zorluğu üzerine çalışan bir algoritmadır. Eşitlik (6), eşitlik (7), eşitlik (8) ve eşitlik (9)'da yer alan formüller x'e uygulandığında doğru bir sonuç elde ediliyorsa x mod N. ye göre kuadrattır denilir. Eşitlikler de yer alan (p,q) N'in çarpanlarıdır [19].

$$x_p = x \pmod{p} \quad (6)$$

$$x_q = x \pmod{q} \quad (7)$$

$$x_p^{(p-1)/2} = 1 \pmod{p} \quad (8)$$

$$x_q^{(q-1)/2} = 1 \pmod{q} \quad (9)$$

Sonrasında anahtar üretimi için gerekli işlemler uygulanır. Bu işlemler RSA şifreleme sistemindeki gibidir. Alınan p ve q değerleri ile eşitlik (10)'daki işlemler uygulanır [19].

$$a_p^{(p-1)/2} = -1 \pmod{p}, \quad a_q^{(q-1)/2} = -1 \pmod{q} \quad (10)$$

Buradan elde edilen (a,N) değeri açık anahtarı oluştururken, (p,q) çarpanları ise gizli anahtarı oluşturur. Şifreleme işleminde bir A kişisi B kişisine şifreli halde mesajı yollamak istediğinde  $(m_1, m_2, \dots, m_n)$  şeklinde bir m bit dizisi olarak düşünülen mesajda her bir  $m_i$  biti mod N yada  $\gcd(b_i, N)$  grubunda bir değer üretir ve eşitlik (11)'de yer alan formülde elde edilen şifreli  $c_i$  verileri karşı tarafa gönderilir [19].

$$c_i = b_i^{2*} a^{m_i} \pmod{N} \quad (11)$$

A kişisinden B kişisine gönderilen bu şifreli mesaj sonrasında B kişisinin gerçekleştireceği işlem adımları sayesinde tekrar m mesajının anlaşılması yönünde olacaktır. Eline ulaşan her bir i değeri için asal çarpanları(p,q) kullanarak  $c_i$ 'nin kuadratik olup olmadığını bulmaya çalışır. Kuadratik ise  $m_i=0$ , değilse  $m_i=1$ 'dir. B kişisi böylelikle m mesajını elde eder.

#### c) RSA Algoritması (RSA Algorithm)

Mesajların şifreli formatları üzerinde işlemlerin gerçekleştirilmesi düşüncesi Rivest, Adleman ve Derouzos tarafından belirtilmiştir. Baş harflerinin birleşiminden oluşturulan RSA algoritması homomorfik şifrelemenin ilk yöntemlerinden biridir. Çarpma işlemine göre kısmi-homomorfik özellik gösterir. RSA'da şifreleme işleminde de şifreleme işleminin çözülmesinde de modüler aritmetik işleminden yararlanır. RSA'nın şifreleme işlemi eşitlik (12)'de, şifre çözme işlemi ise eşitlik (13)'de verildiği gibidir [17,19].

$$\text{Enc}(m) = m^e \pmod{n} = E \quad (12)$$

$$\text{Dec}(E) = E^d \pmod{n} \quad (13)$$

Eşitliklerde yer alan Enc şifreleme işlemi, Dec şifrenin çözülmesi işlemi, m şifrelenmesi istenilen mesajı, n

modülü, e açık anahtarı, d gizli anahtarı ifade etmektedir. E ise şifreleme işleminin sonucunda karşı tarafa iletilen şifrelenmiş haldeki veriyi ifade etmektedir. Şifre çözme işleminde ise bu E üzerinden işlemler gerçekleştirilir. Homomorfik şifreleme yöntemi açısından düşünüldüğünde RSA formülü eşitlik (14)'de ifade edilmektedir [16,18].

$$\text{Enc}(m_1) * \text{Enc}(m_2) = m_1^e * m_2^e \pmod{n} = (m_1 * m_2)^e \pmod{n} = \text{Enc}(m_1 * m_2) \quad (14)$$

Eşitlik 14'de yer alan formül üzerinden örneğin  $m_1=2$ ,  $m_2=3$ ,  $e=7$ ,  $d=3$ ,  $n=33$  alındığında  $m_1$  verisinin şifrelenmiş metni  $\text{Enc}(m_1) = m_1^e \pmod{n} = 2^7 \pmod{33} = 29$  olarak bulunur,  $m_1$ 'in şifrelenmiş haline  $e_1$  diyelim. Böylece  $e_1=29$  olarak bulunur. Aynı işlemi  $m_2$  içinde yapalım ve  $m_2$ 'nin de şifrelenmiş haline  $e_2$  ismini verelim.  $\text{Enc}(m_2) = m_2^e \pmod{n} = 3^7 \pmod{33} = 9$  olarak bulunur. Ve bu sonuç  $e_2$ 'ye eşitlenir. Bu elde edilen şifreli metinlerin çarpımı  $e_1 * e_2 = 29 * 9 = 261$ 'dir. Karşı tarafa şifreli halde gönderilen bu çarpım değerinin şifresi çözülmek istenildiğinde eşitlik (13)'de yer alan formül uygulanır.  $\text{Dec}(e_1 * e_2) = (e_1 * e_2)^d \pmod{n} = (261)^3 \pmod{33} = 6$ 'dır. İki değer çarpımı işlemi karşı tarafa iletmek isteyen kullanıcı veriler üzerinde bu şekilde şifreleme yöntemleri yaparak elde ettiği işlem sonucunu karşı tarafa ilettiğinde, alıcı kişi kullanılacak gizli anahtar yardımıyla şifre çözme işlemi gerçekleştirir ve elde edilen sonucun mesajı gönderen kişinin işlem sonucunu aynı olduğunu görürüz. Bu şekilde iletilmek istenen mesaj gerekli şifreleme işlemleri yapılarak, üçüncü kişilerin erişimine kapalı olarak alıcı tarafa iletilmiş olur ve böylece verilerimizin gizliliği ve mahremiyeti sağlanmış olur [16,18].

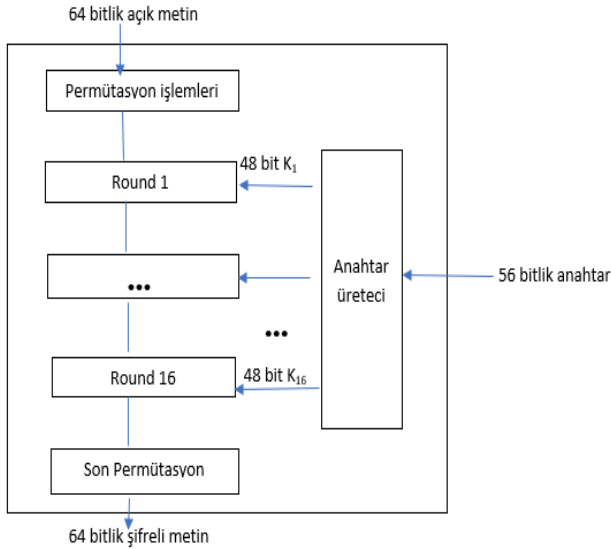
#### d) El Gamal Algoritması (El Gamal Algorithm)

1985 yılında Taher Elgamal tarafından bulunan açık anahtar şifrelemeli bir algoritmadır. Dairesel gruplar üzerindeki ayrık logaritma zorluğuna dayanan bir algoritmadır. Q derecesinde g üretici kullanılarak bir G grubu oluşturulur, Gönderici bu gruptan bir x değeri seçer ve  $m = g^x$  değerini hesaplar. X gizli anahtar olarak tutulurken; G, q, g, m açık anahtar olarak belirtilir. Şifreleme aşamasına gelindiğinde yayımlanan G grubundan rastgele seçilen r değeriyle birlikte  $c_1 = g^r$  ve  $s = m^r$  eşitlikleri yardımıyla gönderilmek istenen n mesajı n' dönüştürülerek  $c_2 = n^r * s$  eşitliğinden  $c_2$  değeri elde edilir. Gönderilmek istenen şifreli metin  $(c_1, c_2) = (g^r, n^r * m^r)$  olarak gönderilir. Mesajı alan kişi şifreli metni açmak için sahip olunan x değeriyle  $(c_2 / c_1^x)$  bölüm işlemi gerçekleştirir [19].

#### 4.2.2. DES Algoritması (DES Algorithm)

Blok şifrelemenin bir örneği olan DES algoritması temel olarak bir metni bloklara bölerek her parça için şifreleme yapmaktadır. Anahtar uzunluğu esas olarak 64 bittir ancak 8 bit şifreleme algoritması tarafından kullanılmaz, dolayısıyla 56 bitlik anahtar uzunluğu bulunmaktadır. Girdi olarak ise 64 bitlik mesaj DES algoritmasına girer

ve sonuç olarak 64 bitlik şifreli metin üretilir. DES aslında NIST (National Institute of Standards and Technology) tarafından yayınlanan simetrik anahtarlı blok şifresidir ve DES aynı zamanda Feistel şifrelemenin bir uygulamasıdır. 16 sefer Feistel yapısı kullanılır. Genel olarak kullanılan DES algoritması şifreleme yapısı Şekil 4’de verildiği gibidir [20].



Şekil 4. DES Algoritması Şifreleme Yapısı [20]  
(Encryption Structure of DES Algorithm)

#### 4.2.3. BLOWFISH Algoritması (BLOWFISH Algorithm)

Blowfish algoritması da DES algoritması gibi simetrik bir anahtar şifreleme algoritmasıdır. DES gibi 64 bit blokları şifreler ancak Blowfish’de kullanılan anahtarın uzunluğu 32-448 bittir. Bruce Schneier tarafından geliştirilmiş olan Blowfish algoritması DES algoritmasına bir alternatif oluşturması amacıyla geliştirilmiştir. DES algoritmasında olduğu gibi Blowfish’de de Feistel yapısı kullanılır [21].

#### 4.2.4. AES Algoritması (AES Algorithm)

Gelişmiş şifreleme standardı olarak bilinen AES 2001 yılında NIST tarafından yayınlanmıştır. Anahtar uzunluğu 128, 192 ve 256 bit olabilmektedir. Anahtar uzunluğuna göre algoritma ismi değişmektedir. Anahtar uzunluğu 128 bit uzunluğunda olduğunda AES-128, 192 bit uzunluğunda olduğunda AES-192, 256 bit uzunluğunda olduğunda ise AES-256 olarak isimlendirilmektedir. Şifrelemedeki tur sayısı, anahtar uzunluğuna bağlı olarak; 128 bit uzunluğundaki anahtar için 10 tur, 192 bit uzunluğundaki anahtar için 12 tur, 256 bit uzunluğundaki anahtar için ise 14 turdur. Genel olarak algoritmanın çalışma mantığı 4x4 matris üzerine yayılmış durumdaki metinlerin kaydırma işlemleri uygulanmasıdır. Matris 4 satır ve 4 sütun yani toplamda 16 bölmeden oluşmaktadır. Bu matrislere durum ismi verilmektedir. Durumun her bölmesine 1 baytlık veri düşmekte ve her satırda 4 sütun olduğu düşünüldüğünde toplam olarak bir satırda 32 bitlik bir kelime meydana gelmektedir [22].

## 5. KİŞİSEL VERİLERİN KORUNMASI KAPSAMINDA HUKUKİ DÜZENLEMELER VE BULUT HİZMET SAĞLAYICILARIN GÜVENLİK SORUMLULUKLARI (LEGAL REGULATIONS UNDER THE PROTECTION OF PERSONAL DATA AND SECURITY RESPONSIBILITIES OF CLOUD SERVICE PROVIDERS)

### 5.1. Kişisel Veri Koruma Tarihçesi (Personal Data Protection History)

Uluslararası düzeyde kişisel verilerin korunması ilk olarak 1948 tarihli İnsan Hakları Evrensel Beyannamesi ve 1950 yılında imzalanan Avrupa İnsan Hakları Sözleşmesi (AİHS) ile başlamıştır. Söz konusu sözleşmenin kabul edilmesinin ardından özel hayatın gizliliğine verilen önem artmıştır.[23] Sonrasında 23 Eylül 1980 tarihinde OECD Sözleşmesi kabul edilmiş olmakla birlikte anılan sözleşmedeki temel ilkeler bağlayıcı olarak kabul edilmemektedir. Daha sonra Avrupa Konseyi tarafından 1981 tarihinde kişisel verilerin korunması konusundaki ilk geniş kapsamlı sözleşme olan 108 sayılı “Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi” imzalanmış ve söz konusu sözleşmeyi imzalayan ülkeler tarafından iç hukuka aktarılması yükümlülüğü getirilmiştir. Sözleşmenin amacı uyrukları ne olursa olsun her insanın mahremiyet hakkına saygı gösterilmesini ve kişisel verilerin otomatik olarak işlenmesinde mahremiyete saygı gösterilmesini sağlamaktır. Bu sözleşme içerisinde kişisel veri, otomatik veri işleme, denetleyici (kontrolör) gibi terimlerin tanımları yapılmış, sözleşmenin amaç ve kapsamı belirtilerek bu alan için bir temel oluşturulmuştur [24]. 14 Aralık 1990 tarihine gelindiğinde ise Birleşmiş Milletler Genel Kurulu üye devletlerin kişisel verilerin korunması konusunda asgari bir standart ortaya koyabilmeleri için “Bilgisayara Geçirilmiş Kişisel Veri Dosyalarının Denetlenmesine İlişkin Rehber İlkeleri” kabul etmiştir [25].

Kişisel verilerin korunması konusundaki en büyük gelişme ise 1995 yılında Avrupa Birliği (AB) tarafından hazırlanan ve 1998 yılında yürürlüğe giren 95/46/AT sayılı “Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif” (AB Veri Koruma Direktifi) olmuştur. Söz konusu direktif ile kişisel verilerin korunması konusunda AB’ye üye tüm ülkelerde geçerli olacak temel esaslar belirlenmiş, AB veri koruma standartlarına sahip olmayan ülkelere veri aktarımı yasaklanmıştır [25]. Söz konusu direktifin yürürlük tarihinden itibaren AB ülkeleri direktifteki kişisel veri koruma standartlarını iç hukuklarına aktarmaya başlamışlardır. Direktifin 29. maddesinde kurulmuş olan bir çalışma grubu (Article 29 Data Protection Working Party) bulunmaktadır. Bahse konu çalışma grubu veri koruma konusunda genel geçer yasa ve yükümlülüklerin analizini yaparak tavsiye kararları ve raporlar yayınlamaktadır. Bu çalışma grubunun yayınladığı raporlar, Avrupa Ekonomik Alanı’ndaki veri sorumlularının, müşterisi bulunan servis sağlayıcıların ve müşterilerin veri koruma konusundaki sınırlandırmaları



bilmeleri, gerekli teknik ve idari tedbirleri almaları adına büyük önem taşımaktadır [26].

Daha sonra geçen süre zarfında AB ülkelerindeki veri koruma kanunlarındaki farklılıkların yarattığı sıkıntılar sebebiyle AB kapsamında yeknesak bir kanuna duyulan ihtiyaç ve teknolojiye yaşanan hızlı gelişmeler ile kişisel verilerin korunması hususunda daha katı önlemlerin alınması gerekliliği sonucunda Avrupa Parlamentosu'nda 25 Mayıs 2016 tarihinde bu alandaki son yirmi yılın en büyük düzenlemesi olarak görülen Genel Veri Koruma Tüzüğü (GDPR) kabul edilmiş ve 25 Mayıs 2018 tarihinde 95/46/AT sayılı AB Veri Koruma Direktifi yürürlükten kalkarak GDPR yürürlüğe girmiştir [25].

Ülkemizde ise, Türkiye'nin gerek Avrupa Konseyi 108 sayılı sözleşmeyi ilk imzalayan ülkelerden biri olması ve iç hukuka aktarma gerekliliği, gerekse Avrupa Birliği müzakereleri kapsamındaki çalışmalarda ve ilerleme raporlarında Kişisel Verilerin Korunması alanında temel ve çerçeve bir kanuna olan ihtiyacın sürekli vurgulanması neticesinde kişisel verilerin korunması kanunu yapım çalışmaları 1989 yılında bir komisyon kurularak başlamıştır. Komisyon çeşitli tasarılar hazırlamış ancak çalışmalarını sonuçlandıramadan dağılmıştır. Ardından 2004 yılında yeni bir komisyon oluşturularak tasarı hazırlık çalışmalarına devam edilmiş, hazırlanan tasarı 2006 yılında Başbakanlığa oradan da 2008 yılında Türkiye Büyük Millet Meclisi'ne (TBMM) sevk edilmiştir. Ancak araya seçimlerin girmesi nedeniyle tasarı yasalaşamamış ve hükümsüz sayılarak Başbakanlığa iade edilmiştir. Daha sonra 2012 ve 2014 yıllarında Adalet Bakanlığı bünyesinde yeni bir çalışma grubu kurulmuş, önceki tasarı yapılan öneri ve eleştiriler bünyesinde yeniden ele alınmış ve TBMM'ye sunulmuşsa da araya seçimler girmesi sebebiyle hükümsüz sayılmış ve yasalaşamamıştır. Sonrasında tekrar kanun yapım süreçleri çalıştırılmış ve yeni bir tasarı hazırlanmış, söz konusu tasarı 9 Şubat 2016 tarihinde TBMM Adalet Komisyonu'nda, 24 Mart 2016 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir [25]. Bununla birlikte "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetin Sağlanması Hakkında Yönetmelik ile sağlık alanındaki kişisel verilerin ve Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te de elektronik haberleşme sektörü kapsamında işlenen kişisel veriler üzerine tanımlamalar yapılmıştır [27].

Diğer taraftan, ABD Başkanı Donald Trump tarafından imzalanan ve ABD'de 2018 yılında yürürlüğe giren "The Cloud Act" isimli yasa kapsamında ABD dışında tutulan verilere erişmek isteyen her seviye yetkili diğer yasal yardım anlaşmalarını gözetmeksizin şirketleri veri paylaşımı yapmaları konusunda zorunlu tutabilecektir. Bu yasa ABD vatandaşlarını görüş ayrılığına düşürmüştür. Bir grup vatandaşın suçluların bilgilerinin kolay yoldan elde edilebileceği için kolluk kuvvetlerinin işlerini

kolaylaştırarak, suçluların kısa sürede yakalanacağını düşünerek yasaya olumlu bakarken; diğer grup kişisel verilere ulaşarak gizlilik ve mahremiyet konusunda sorun yaşanacağını düşünerek yasayı eleştirmişlerdir [28].

Kişisel verilerin korunması konusunda belirli alanlar için farklı yasal düzenlemeler oluşturulsa da sosyolojik açıdan bakıldığında kişisel verilerin hukuka uygun olmayan şekillerde işlenmesi, paylaşılması gibi veri üzerinden gerçekleştirilen her türlü işlem İnsan Hakları Evrensel Beyanname'sinde temel haklar kapsamında bulunmakta, Türkiye Cumhuriyeti Anayasası, Türk Ceza Kanunu ve Kişisel Verilerin Korunması Kanunu ilgili maddelerince bu konuda belirli yaptırımlar uygulanabilmektedir.

## 5.2. Bulut Ortamının Konumu ve Yasal Durumu (Location and Legal Status of Cloud Environment)

Bulut bilişim sistemleri birbirinden farklı ülkelerde bulunan kullanıcıların yine farklı ülkedeki bir sunucuya erişim sağlayarak gerçekleştirdiği bir hizmettir. Sunucuların bulunduğu ülkedeki yasalar ile kullanıcıların bulunduğu ülkelerin yasaları birbirinden farklı olacağı için bu durum arada bir anlaşmazlık yaratabilir. Bu anlaşmazlığı gidermek için ve olası her türlü güvenlik sorununda çözüm bulunabilmesi için hizmet sağlayıcıların birçok sorumluluğu bulunmaktadır. Öncelikle yapılan bu sözleşmelerde her türlü durum ve güvenlik ihlali riskine karşı yapılacaklar, iki tarafın rol ve sorumlulukları açıkça belirtilmelidir ve yasa farklılıkları konusunda ise uluslararası geçerliği olan yasalar ve sözleşmeler kullanılmalıdır [30]. Bununla birlikte verilerin önemi de göz önünde bulundurulmalı yeterli seviyede güvenlik önlemleri alınmalıdır.

Ülkemizde 7 Nisan 2016 tarihinde yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun tanımlar kısmında veri sorumlusu ve veri işleyeni tanımları mevcuttur. Bu kapsamda veri sorumlusu kişisel verilerin işleme amaç ve vasıtalarını belirleyen, veri kayıt sisteminin kurulması ve yönetilmesinden sorumlu olan gerçek ya da tüzel kişi iken veri işleyen veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek ve tüzel kişiler olarak tanımlanmaktadır [31].

Bu açıdan bakıldığında bir şirket ya da kuruluş işlemiş olduğu kişisel verileri barındırmak ve gerektiğinde üzerinde işlem yapabilmek için bulut hizmet sağlayıcı ile anlaşılabilir, bu durumda bulut hizmet sağlayıcı sadece barındırma hizmeti verdiği, kendi adına herhangi bir kişisel veri işlemediği ve veri sorumlusunun talimatları doğrultusunda hareket ettiği için veri işleyen olacaktır [29]. Bununla birlikte söz konusu kişisel veriler veri sorumlusuna ait olmayan başka bir yerde barındırılacağı için konu veri aktarımı kapsamında da değerlendirilmelidir.

Bu minvalde söz konusu Kişisel Verilerin Korunması Kanununun 8 inci maddesi yurt içi veri aktarımının 9

uncu maddesi ise yurt dışı veri aktarımının şartlarını belirlemektedir. Bu kapsamda kanunun 8 inci maddesi ile yurt içinde hizmet alınan bulut hizmet sağlayıcısına veri aktarımı gerçekleşecek ve ilgili kişilerin açık rızası yoksa Kanunun 5 inci maddesinin ikinci fıkrası (Kanunlarda açıkça öngörülmesi, -Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması, -Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması, -Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması, -İlgili kişinin kendisi tarafından alenileştirilmiş olması, -Bir hakkın tesisi, kullanılması veya korunması için veri işlenmesinin zorunlu olması, -İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması) [31] ile yeterli önlemler alınmak şartıyla 6. maddesi üçüncü fıkrasında (sağlık ve cinsel hayat dışındaki kişisel verilerin kanunlarda öngörülen hallerde, sağlık ve cinsel hayata ilişkin kişisel verilerin ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgili kişinin açık rızası aranmaksızın işlenebileceği) [31] yer alan şartlardan birinin varlığı gerekecektir. Bu şartlardan herhangi biri mevcut ise ancak bulut hizmeti kullanılabilir.

Diğer taraftan bir önceki paragrafta anlatılan hususlar çerçevesinde bulut hizmet sağlayıcıların sunucuları ülkemiz sınırları içerisinde değilse bu durum anılan kanunun 9 uncu maddesi kapsamında belirlenen yurt dışına veri aktarımına girecektir. Söz konusu 9 uncu maddede ise, kişisel verilerin, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamayacağı; ancak anılan hükmün ikinci fıkrası uyarınca Kanunun 5 inci maddesinin ikinci fıkrası ile özel nitelikli kişisel veriler bakımından 6 ncı maddesinin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; ya yeterli korumanın bulunması ya da yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması kaydıyla kişisel verilerin ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılacağı düzenlenmiştir [31]. Öte yandan, özel nitelikli kişisel verilerin yurt dışına aktarımında "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ile ilgili Kurul'un 31.01.2018 tarihli ve 2018/10 sayılı kararının dikkate alınması şarttır. Bununla birlikte Kanunun 9 uncu maddesinin üçüncü fıkrası hükmü uyarınca yeterli korumanın bulunduğu ülkeler ise henüz Kurul tarafından belirlenmemiştir. Bu kapsamda yurt dışında yerleşik bulut hizmetinden faydalanabilmek için ilgili kişilerin açık rızası alınmıyorsa, açık rıza harici yukarıda belirtilen hukuka

uygunluk sebeplerinden yararlanılacaksa mutlaka Kurulun izninin alınması, Kurulun izni olmadan bulut hizmetinin kullanılmaması gerekecektir. Aksi takdirde hukuka aykırı veri aktarımı olabileceği için cezai yaptırımlarla karşılaşmak büyük oranda olasıdır.

### 5.3. Verilerin Güvenliğinin Sağlanması (Providing Data Security)

Kişisel Verilerin Korunması Kanununun "Veri Güvenliğine İlişkin Yükümlülükler" başlıklı 12nci maddesinin birinci fıkrasında, veri sorumlusunun, kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorunda olduğu belirtilmektedir [15]. Bu itibarla, veri güvenliğini sağlayamayan veri sorumluları hakkında Kanunun 18. maddesinde belirlenen oranlarda idari para cezalarının uygulanacağı da belirtilmiştir [31].

Dolayısıyla veri güvenliği yükümlülüğü veri sorumluları açısından hem idari para cezasıyla karşı karşıya kalmamak hem de ticari itibarlarının zedelenmemesi için son derece önemlidir. Özellikle de güvenlik unsurunun çok net olarak veri sorumlusu tarafından kontrol edilmediği bulut bilişim sistemleri kullanıldığında veri güvenliği hususu çok daha dikkatli ve özenli ele alınmalıdır. Yani bulut hizmeti kullanılırken bulut ortamında tutulan verilerin güvenliğinin etkin bir şekilde sağlanması için bulut hizmet sağlayıcı tarafından gerekli tedbirlerin alınıp alınmadığının değerlendirilmesi, bu kapsamda gerekli denetimlerin mutlaka yapılması son derece önemlidir.

Bu kapsamda bulut bilişim hizmeti sunacak servis sağlayıcının değerlendirilmesi aşamasında; alınacak hizmetin kapsamı ve bilgi güvenliği gereksinimleri göz önünde bulundurularak hizmet alınmalıdır ve buna uygun sözleşmeler yapılmalıdır [15]. Söz konusu sözleşmede rol ve sorumluluklar net olarak belirtilmeli ve sözleşme özellikle yeterli güvenlik önlemlerinin alınması hususunda açık maddeler içermelidir. Çünkü yukarıda genel olarak anlatılan, gerek yurt içinden gerekse yurt dışından tüm hukuki şartların sağlanarak bulut hizmeti alındığı düşünüldüğünde, özellikle söz konusu hizmet kapsamında bulut hizmet sağlayıcı veri işleyen olabileceğinden Kurul ile direkt irtibat halinde olacak kişi veri sorumlusudur, bu husus göz önünde bulundurulduğunda yaşanabilecek bir veri güvenliği ihlalinde muhtemel cezalar ile karşılaşacak olan veri sorumlusu, bulut hizmet sağlayıcı ile yapacağı sözleşme kapsamında kendini bir nebze koruma altına alabilecektir.

Bununla birlikte bulut bilişim hizmeti kapsamında tutulan verilerin güvenliğini sağlamak için aşağıdaki önlemlerin

de mutlaka göz önünde bulundurulması gerektiği düşünülmektedir.

Öncelikle bulut bilişim sistemlerinin uygulama ve veri merkezlerinin hangi ülkede tutulması gerektiği hususu ele alınmalı, bu kapsamda ilgili yasalara uygun hareket edilmelidir. Ayrıca bulut bilişim ile çalışan tüm sistemler arasındaki veri trafiği, güvenli iletişim protokolleriyle gerçekleştirilmeli herhangi bir zafiyet içermemeli, şifreli protokoller kullanılmalıdır. Aynı bulut ortamını kullanan veri sorumlularına ait sistemler ağ seviyesinde birbirlerinden mantıksal ve mümkünse de fiziksel olarak ayrılmalı, her bir veri sorumlusunun yalnızca kendilerine ait veriye erişim imkânı sağlanmalıdır [32]. Bulut hizmeti kapsamında, şablon olarak kullanılabilir imajların imha edilmesine (silme/yok etme) bulut hizmet sağlayıcı tarafından imkân tanınmalıdır [15,33,37]. Bulut hizmeti kapsamında herhangi bir sanal makinenin hizmetinin sonlandırılması durumunda, sanal makinenin bulut bilişim sunucularında bulunan bellek bölgeleri ile disk bölgelerinin bulut hizmet sağlayıcı tarafından imha edilmesi sağlanmalıdır [34]. Kesintisiz hizmet verebilmek için ise bulut ortamı internet bağlantısının, yeterli seviyede DDoS korumasına sahip olmalıdır [35,44]. Güvenilir kimlik yönetimi kullanılmalı, özel nitelikli kişisel veriler de işleniyorsa kullanıcının en az iki katmanlı kimlik doğrulama yöntemi ile kimliği doğrulanmalıdır. İlk olarak kullanıcı, kullanıcı adını ve şifresini girdikten sonra güvenilir bir ikinci iletişim kanalından (e-posta, anlık mesaj servisleri, kısa mesaj servisleri vb.) tek seferlik şifre üretilerek bu sağlanabilir [36,37].

#### 5.4. Verilerin Korunmasında Şifreleme Yaklaşımı (Encryption Approach in Data Protection)

Verilerin korunması hususunda yukarıda belirtilen veri güvenliğine ilişkin önlemlerin alınması her ne kadar çok önemli ise de bulut hizmet sağlayıcılarının sunucularında tutulan verilerin güvenliğinin kötü niyetli olabilecek hizmet sağlayıcılara karşı da korunabilmesi için uygun şifreleme algoritmalarının kullanılması, bu kapsamda oluşturulacak şifre anahtarlarının başka güvenli yerlerde tutulması gerektiği, veri sorumlusu açısından bulut hizmet ilişkisi sona erdirildiğinde kişisel verileri imha etmek için söz konusu şifre anahtarlarının tüm kopyalarının yok edilmesinin uygun olacağı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberinde yayınlanmıştır [37].

Dolayısıyla Kişisel Verileri Koruma Kurulu rehberine göre, bulut hizmet sağlayıcıları kapsamında tutulacak kişisel verilerin korunması konusundaki temel güvenlik yaklaşımının yukarıdaki bölümlerde detaylı bir şekilde anlatılan şifreleme yöntemleri olduğu görülmektedir. Zira şifreleme algoritmaları kullanılmadan bulutta tutulan veriler, veri sorumlusunun direk kendi kontrolünde olmadığı için herhangi bir saldırı ya da güvenlik ihlali sonucu üçüncü kişiler tarafından ele geçirilirse sonuçları veri sorumlusu açısından iyi olmayacaktır. Bir taraftan idari para cezası yaptırımını ile karşı karşıya kalırken diğer

taraftan ve belki de daha önemli olabilecek muhtemel itibar kaybı da yaşayacaktır. Nitekim bu konuda benzer olayların yaşandığı, Kişisel Verileri Koruma Kurumunun internet sayfasında yayımlanan birtakım veri ihlal bildirimlerinde ve Kurul kararlarında açıkça görülmektedir. Bununla birlikte verilerin şifreli tutulması herhangi bir saldırı ya da verileri ele geçirme durumu yaşansa bile veriler kullanılamaz olacağından muhtemel yaptırımlara maruz kalınmasını önleyecektir ki Kurul da yayımlanmış olduğu rehberlerde bu yönde yönlendirme yapmaktadır.

Bu kapsamda şifreleme algoritmaları incelendiğinde ise özellikle homomorfik şifreleme öne çıkmaktadır. Homomorfik şifreleme, özellikle Büyük Veri, Makine Öğrenmesi gibi veri işleme yöntemleri ile veri kümeleri üzerinde analizler yapan çalışmalarda büyük önem taşımaktadır. Veri işlemlerde, homomorfik şifrelemenin performansını ölçmek adına birçok çalışma yapılmıştır [38-40].

Örneğin görsel sınıflandırıcıları dağıtılmış veriler üzerinden, yüksek performansta ve güvenli bir şekilde öğrenme yapabilmek için yeni bir mahremiyet koruma çerçevesi geliştirilmiş ve söz konusu homomorfik şifreleme sistemi görsel öğrenmede kullanılarak, 40 yüz tanıma özelliği sınıflandırılıp, %84 doğruluk değeri elde edilmiştir [41]. Ayrıca eğitilmiş sinir ağlarını, şifreli verilere uygulanabilecek sinir ağlarına dönüştürmek için 60.000'den oluşan bir veri kümesinde çalışma yapılmış, anılan veri setinin 50.000 verisi eğitim için, 10.000 verisi ise test için kullanılarak saatte 59.000 tahmin, %99 doğrulukla gerçekleştirilmiştir [40-42].

Yapılan çalışmalarda homomorfik şifreleme yaklaşımlarının, veriler üzerinde hızlı ve güvenli işlem performansı sağladığı açıkça görülmektedir [34,39].

Veri sorumlusunun direk kontrolünde olmayan bulut hizmet sağlayıcıları tarafında oluşabilecek sorunları da göz önünde bulundurarak veri güvenliği konusunda özellikle veri sızıntılarını önlemek, verileri hem kötü niyetli saldırganlara karşı koruyabilmek hem de herhangi bir ihlal durumunda verilerin kullanılamamasını sağlayabilmek için özellikle homomorfik şifreleme gibi şifreleme yaklaşımlarına başvurulması gerektiği değerlendirilmektedir.

## 6. SONUÇ (CONCLUSION)

Günümüzde bulut bilişim giderek yaygınlaşan ve kullanıcı sayısı açısından her geçen gün artış gösteren önemli bir teknoloji haline gelmiştir. Kullanım kolaylığı, düşük maliyetli olması ve esnek kullanıma yönelik bir sistem oluşu gibi avantajları kullanıcıların bulut bilişim hizmetlerini seçmesi hususunda en önemli tercih sebeplerindedir. Ancak kişisel verilerin korunması ve mahremiyeti söz konusu olduğunda kullanıcılar tedirginlik yaşamaktadırlar. Kişisel verilerin bulut bilişim sistemlerinde tutulması sonucu verilerin aslında hangi

ülkede, hangi servis sunucusunda tutulduğunun bilinmemesine yol açmaktadır. Bireylerin verileri üzerinde kontrollerini sağlayabilmeleri için verilerinin nasıl işlendiğini bilmek, güvenlik prosedürleri ve önlemleri hakkında bilgilendirilmeyi istemek, yurt içi ya da yurt dışına aktarım konusunda bilgilendirilerek gerekmesi halinde açık rıza vermemek ya da bu duruma itiraz etmek gibi çeşitli hakları bulunmaktadır. Veri sorumlularının ve bulut hizmet sağlayıcıların bu konuları titizlikle ele almaları ve bulut bilişim kapsamında tutulan kişisel veriler konusunda çok daha dikkatli olmaları gerekmektedir.

Verilerin bulut bilişim sistemlerine yapılacak saldırılarla üçüncü kişilerin eline geçmesini önlemek adına yukarıda belirtilen gerekli güvenlik önlemlerinin alınması ve özellikle verilerin şifreli olarak bulutta tutulması önerilmektedir. Şifreli olarak tutulan veriler güvenlik ve mahremiyet konusunda alınabilecek önlemlerin en başında gelmektedir. Bu konu Kişisel Verileri Koruma Kurulunun yayınlamış olduğu rehber de açıkça ele alınmıştır.

Bununla birlikte veri işleyen olarak değerlendirilebilecek bulut hizmet sağlayıcılarla uluslararası geçerliliği olan sözleşmeler imzalanmalı ve bu konudaki yasal düzenlemelere uyum sağlandığından emin olunmalıdır. Herhangi bir veri ihlali veya veri sızıntısı durumunda hizmet sağlayıcıların ve kullanıcının sorumlulukları titizlikle belirlenmeli ve yapılan sözleşmeler de bu sorumluluklar açıkça belirtilmelidir.

Bu çalışmada bulut bilişim sistemlerinde tutulan kişisel verilerin önemi, bu kapsamda oluşabilecek riskler ve bulut bilişim sistemleri kapsamındaki kişisel verilerin korunması konusunda veri güvenliği hususunda yapılması gerekenler ve özellikle verileri şifreleme yöntemleri ele alınmış, hukuki açıdan veri sorumlularının ve veri işleyen olarak değerlendirilen bulut hizmet sağlayıcıların yapmaları gerekenler ve bu konuda gerçekleştirilen yasal düzenlemeler incelenmiş, bulut bilişim sistemleri kapsamında tutulan kişisel verilerin korunması ve mahremiyetinin sağlanmasının önemine vurgu yapılmıştır.

Diğer taraftan dijital çağda olduğumuzdan hareketle, özellikle yapay zeka, büyük veri, nesnelere interneti gibi teknolojiler her geçen gün önem kazanmakta ve işlenen veri miktarı da artmaktadır. Bu minvalde artan veri miktarıyla birlikte şifreleme teknolojileri de önem kazanmaktadır. Dolayısıyla gelecekte bulut bilişim sistemlerinde veri ihlalleri/sızıntılarının önlenmesi kapsamında diğerlerine nazaran daha sıklıkla kullanılacağını düşündüğümüz homomorfik şifreleme yöntemlerinin detaylı bir şekilde araştırılıp ele alınması gerektiği değerlendirilmektedir.

## KAYNAKLAR (REFERENCES)

- [1] P. M. Schwartz, "Information Privacy in the Cloud", *University of Pennsylvania Law Review*, 161(1623), 1624-1662, 2013.
- [2] Internet: M., The Evolution Of Data Storage, <https://www.nimbushosting.co.uk/the-evolution-of-data-storage/>, 10.11.2018.
- [3] Communication from the Commission to the European Parliament the Council the European Economic and Social Committee and the Committee of the Regions, **Unleashing the Potential of Cloud Computing in Europe**, European Commission, Brüksel, 2012.
- [4] B. Furht, A. Escalante, **Handbook of Cloud Computing**, Springer Publishing Company, New York, A.B.D, 2010.
- [5] Internet: Bulut Bilişim Tarihçesi, <https://bulutcloudbilisim.wordpress.com/2012/06/27/bulut-bilisim-tarihcesi/>, 16.11.2018.
- [6] Internet: Bulut Bilişim Nedir?, [https://aws.amazon.com/tr/what-is-cloud-computing/?nc1=h\\_ls](https://aws.amazon.com/tr/what-is-cloud-computing/?nc1=h_ls), 23.11.2018.
- [7] Y. İnağ, E. Ceyhan, Ş. Sağıroğlu, "Bulut Bilişimin Kurumsal Zorlukları ve Çözüm Önerileri", **Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, ODTÜ, Ankara, Haziran, 2015.
- [8] P. M. Mell, T. Grance, **The NIST Definition of Cloud Computing**, National Institute of Standards & Technology, United States, 2011.
- [9] E. Mathisen, "Security Challenges and Solutions in Cloud Computing", **5th IEEE International Conference on Digital Ecosystems and Technologies**, Daejeon, 208-212, 2011.
- [10] H. Yang, M. Tate, "Where are we at with cloud computing?: A descriptive literature review", *Communications of the Association for Information Systems*, 31(2), 2-4, 2012.
- [11] H. Kılıç, **Kamuda Bulut Bilişim Kullanımına Yönelik Risk Analizi ve Yönetimi**, Uzmanlık Tezi, T.C Çevre ve Şehircilik Bakanlığı, 2017.
- [12] P. Mell, "What's Special about Cloud Security?", *IT Professional*, 14(4), 6-8, 2012.
- [13] A. Singh, M. Shrivastava, "Overview of Attacks on Cloud Computing", *International Journal of Engineering and Innovative Technology*, 1(4), 321-323, 2012.
- [14] O. Samuel, M. A. Shah, A. Hayat, "Cloud Computing: Attacks and Defenses", *International Journal of Scientific & Engineering Research*, 6(4), 745-751, 2015.
- [15] Kişisel Verileri Koruma Kurumu, **Kişisel Veri Güvenliği Rehberi Teknik ve İdari Tedbirler**, KVKK Yayınları, 8-25, Ankara, 2018.
- [16] E. Çalık, H. A. Erdem., M. A. Aydın: "Bulut Bilişim Güvenliği için Homomorfik Şifreleme", **19. İnternet Konferansı**, Yaşar Üniversitesi, İzmir, 249-253, 27-29 Kasım 2014.
- [17] M. Tebaa, S. E. Hajji, A. E. Ghazi, "Homomorphic encryption method applied to Cloud Computing", **2012 National Days of Network Security and Systems**, Marrakech, 86-89, 2012.

- [18] S. Ravindran, P. Kalpana, "Data Storage Security Using Partially Homomorphic Encryption in a Cloud", *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4), 603-606, 2013.
- [19] X. Yi, R. Russell, E. Bertino, **Homomorphic Encryption and Applications**, Springer, Melbörn, Avustralya, 2014.
- [20] S. Kumari, Reema. Princy, S Kumari, "Security in Cloud Computing using AES & DES", *International Journal on Recent and Innovation Trends in Computing and Communication*, 5(4), 194 – 200, 2017.
- [21] A. Rachna, A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", *International Journal of Engineering Research and Applications*, 3(4), 1922-1926, 2013.
- [22] M. P. Babitha, K. R. R. Babu Raman, "Secure cloud storage using AES encryption", **2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)**, Pune, 859-864, 2016.
- [23] I. Gursel, "Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 18(1), 33-112, 2016.
- [24] Internet: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, <https://rm.coe.int/1680078b37>, 26.11.2018.
- [25] C. Paşaoğlu, Y. Vural, "Dünyada ve Türkiye'de Kişisel Verilerin Korunması", **Siber Güvenlik ve Savunma Farkındalık Caydırıcılık**, Cilt 1 Editör: Sağiroğlu Ş., Alkan M., Grafiker, Ankara, s.282-309, 2019
- [26] Internet: Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=640601](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640601), 28.11.2018.
- [27] M. V. Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", *Istanbul Medipol University School of Law Journal*, 3(2), 101-167, 2016.
- [28] Internet: F. Babur, CLOUD yasası ile kullanıcı verilerine artık daha kolay ulaşılacak, <https://www.donanimhaber.com/CLOUD-yasasi-ile-kullanici-verilerine-artik-daha-kolay-ulasilacak--98663>, 16.01.2019.
- [29] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi**, KVKK Yayınları, 56-61, Ankara, 2018.
- [30] R. Buyya, J. Broberg, A. Goscinski, **Cloud Computing Principles and Paradigms**, John Wiley&Sons, New-Jersey, A.B.D., 2011.
- [31] 6698 sayılı Kişisel Verilerin Korunması Kanunu, **29677 sayılı Resmi Gazete**, 1-6, Ankara, 2016.
- [32] A. Ahmad, N. Nasser, M. Anan, "An Identification and Prevention of Theft of Service Attack on Cloud Computing", **International Conference on Selected Topics in Mobile & Wireless Networking**, Kahire, 1-6, 2016.
- [33] B. Grobauer, T. Walloschek, E. Stocker, "Understanding Cloud Computing Vulnerabilities", *IEEE Security & Privacy*, 9(2), 50-57, 2011.
- [34] I. K. Aksakallı, "Bulut Bilişimde Güvenlik Zaafiyetleri, Tehditler ve Bu Tehditlere Yönelik Güvenlik Önerilerinin İncelenmesi", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 5(1), 18-19, 2019.
- [35] R. Deshmukh, K. Devadkar, "Understanding DDoS Attack & Its Effect In Cloud Environment", *Procedia Computer Science*, 49, 202-210, 2015.
- [36] C. Huang, S. Ma, K. Chen, "Using onetime passwords to prevent password phishing attacks", *Journal of Network and Computer Applications*, 34, 1292-1301, 2011.
- [37] Kişisel Verileri Koruma Kurumu, **Kişisel Verilerin Silinmesi Yok Edilmesi ve Anonim Hale Getirilmesi Rehberi**, KVKK Yayınları, 1-13, Ankara, 2018.
- [38] Z. Tari, X. Yi, U.S. Premarathe, P. Bertok, I. Khalil, "Security and Privacy in Cloud Computing: Vision, Trends, and Challenges", *IEEE Cloud Computing*, 2(2), 30-38, 2015.
- [39] S. Sridhar, S. Smys, "A Survey on Cloud Security Issues and Challenges with Possible Measures", **International Conference on Inventive Research in Engineering and Technology**, Pattaya, 1-12, 2016.
- [40] R. Hallman, C. Graves, M. H. Diallo, "Homomorphic Encryption for Secure Computation on Big Data", **The 3rd International Conference on Internet of Things, Big Data and Security**, Portekiz, 340-347, 2018.
- [41] R. Yonetani, V. N. Boddeti, K. M. Kitani, Y. Sato, "Privacy-preserving visual learning using doubly permuted homomorphic encryption", **IEEE International Conference on Computer Vision (ICCV)**, Venedik, 2040-2050, 2017.
- [42] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, J. Wernsing, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy", **Proceedings of The 33rd International Conference on Machine Learning**, 201-210, New York, 2016.
- [43] A. İnan, M. Nergiz, Y. Saygın, "Öğrenci Verilerinin Korunması: Fatih Projesi Işığında Teknik Değerlendirme", *Bilişim Teknolojileri Dergisi*, 10(1), 67-77, 2017.
- [44] E. Masum, M. Samet, "Mobil Botnet ile DDOS Saldırısı", *Bilişim Teknolojileri Dergisi*, 11(2), 111-121, 2018.