BULUT SİSTEMLERDE KİŞİSEL VERİLERİN KATEGORİZASYONU VE UYGUN ŞİFRELEME YÖNTEMLERİNİN ARAŞTIRILMASI

Ziya Can KALKAVAN
221402106

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2023

BULUT SİSTEMLERDE KİŞİSEL VERİLERİN KATEGORİZASYONU VE UYGUN ŞİFRELEME YÖNTEMLERİNİN ARAŞTIRILMASI

Ziya Can KALKAVAN
221402106
ORCID: 0000-0002-0735-1327

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksel Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder ŞAHİNASLAN

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Eylül, 2023



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Eğitim hayatıma ara verdiğim uzun yıllardan sonra tekrar başlamanın ve yüksek lisans tezimi tamamlamanın mutluluğunu yaşıyorum. Bu süreçte bana olan desteklerinden ailem ve arkadaşlarıma, araştırma sürecinde deneyim ve yardımlarını esirgemeyen Dr. Ender ŞAHİNASLAN'a, tezin değerlendirilmesinde öneri ve katkılarını gördüğüm jüri üyesi hocalarıma ve değerli danışman hocam Dr. Öğr. Üyesi Önder ŞAHİNASLAN'a katkılarından dolayı teşekkürlerimi sunarım.

Ziya Can KALKAVAN

Eylül, 2023

ÖZET

BULUT SİSTEMLERDE KİŞİSEL VERİLERİN KATEGORİZASYONU VE UYGUN ŞİFRELEME YÖNTEMLERİNİN ARAŞTIRILMASI

Ziya Can Kalkavan
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı
Danışman: Dr. Öğr. Üyesi Önder Şahinaslan
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2023

Bulut bilişim uygulamaları modern teknolojinin bizlere kattığı birçok avantajla birlikte kişisel veri güvenliğine dayalı endişeleri yanında getirmektedir. Avrupa için GDPR, ülkemizde ise KVKK ile kontrol altına alınmaya çalışan veri mahremiyeti için teknik altyapı yetersizliklerinin aşılması hedeflenmektedir. Bu çalışmada bulut ortamda bulunan kişisel verilerin korunmasına yönelik uluslararası standartların uygulama alanlarını değerlendirilmiş olup, bu standartlara uyum ile ilgili çalışmalar incelenerek hatalı kullanımların önüne geçilebilecek, hızlıca güncellenebilir bir altyapı oluşturulmaktadır. Çalışma detayında maskeleme ve şifreleme yöntemleri incelenmiş olup kontrol altına alınması gereken verinin boyutu ve niteliği nedeniyle yapılan testler sonucunda Blowfish şifreleme yöntemi tercih edilmiştir. Şifreleme süreçlerini KVKK'ya uygun bir şekilde işleyip yönetebilmek için ara katman web servis uygulama hazırlanıp, örnek bir bulut CRM uygulaması üzerinde çalışma yapılmıştır. CRM sisteminde uygulanacak olası kullanım senaryoları belirtilerek hazırlanan uygulamanın veriyi yerel sunucularda saklama sürecindeki konumu ve kullanılabilirliği değerlendirilmektedir.

Anahtar Sözcükler: Bulut Uygulamalar, KVKK, GDPR, Kişisel Veri, Şifreleme, Maskeleme, Anonimleştirme

ABSTRACT

CATEGORIZATION OF PERSONAL DATA IN CLOUD SYSTEMS AND RESEARCH ON SUITABLE ENCRYPTION METHODS

Ziya Can Kalkavan
Master Thesis
Department of Computer Engineering
Computer Engineering Master's Programme with Thesis
Thesis Advisor: Asst. Prof. Önder Şahinaslan
Maltepe University Graduate School, 2023

Cloud applications, along with many advantages brought by modern technology world, also raise concerns about personal data privacy and security. GDPR for Europe and KVKK for Turkey aim to eliminate the technical infrastructure deficiencies for data privacy that are attempted to be controlled. In this study, the application areas of international standards for the protection of personal data were evaluated. Studies on compliance with these standards have been examined and an infrastructure that can be easily updated has been tried to be created. Masking and encryption methods were examined in the details of this study. Blowfish Encryption was preferred due to attribute and the size of the data that needs to be controlled. A gateway web service application was developed to store and manage encryption processes in compliance with KVKK and its implementation was carried out on a sample CRM system. Possible usage scenarios were evaluated on the CRM system and the position of the application during the data storage process on local servers was assessed.

Keywords: Cloud Applications, KVKK, GDPR, Personal Information, Encryption

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZET v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ xi
ŞEKİLLER LİSTESİ xii
KISALTMALAR xiv
1. GİRİŞ 1
1.1 Problem 2
1.2 Amaç 5
1.3 Önem 5
1.4 Varsayımlar 5
1.5 Sınırlıklar 6
1.6 Tanımlar 6
2. GENEL BİLGİLER 8
2.1 Literatür Araştırması 9
2.2 Kişisel Verilerin Şifrelenmesi 15
2.2.1 DES 17
2.2.2 3DES 18
2.2.3 AES 19

2.2.4 RC algoritmaları 19
2.2.5 Blowfish 20
2.3 Kişisel Verilerin Maskelenmesi 21
2.3.1 K-Anonimlik modeli 21
2.3.2 L-Çeşitlilik modeli 23
2.3.3 T-Yakınlık modeli 25
2.4 Mevzuat Değerlendirme 26
2.4.1 Kişisel verilerin korunması kanunu 27
2.4.2 Genel veri koruma kısıtları (GDPR) 29
2.4.3 HIPAA 30
2.5 Bulut Sistemlerde Veri Mahremiyeti 31
3. YÖNTEM 33
3.1 Bulut Sistem Sağlayıcıları 33
3.2 Bulut Sistem Aktörleri 36
3.2.1 Bulut sistem kullanıcısı 37
3.2.2 Bulut sistem sağlayıcısı 38
3.2.3 Bulut sistem denetleyicisi 39
3.2.4 Bulut sistem danışmanlığı 39
3.2.5 Bulut sistem barındırıcı 39
3.3 Bulut Sistemlerde Veri Güvenlik Sertifikaları 39
3.3.1 ISO 27001 42
3.3.2 SOC 2 43

3.3.3 PCI DSS 44
3.3.4 CSA STAR 46
4. UYGULAMA 48
4.1 Yerel Ortam Web Servis 48
4.1.1 Web servis mimarisi 49
4.1.2 Web servis fonksiyonları 51
4.1.3 Şifreleme algoritmasının belirlenmesi ve verilerin şifrelenmesi 55
4.1.4 Verilerin kayıt altına alınması 57
4.1.5 Verilerin çözümlenmesi ve yorumlanması 57
4.2 Verilerin Kategorizasyonu 58
4.3 Bulut Geliştirme Ortamı 60
4.3.1 Veri transferi 61
4.3.2 Veri erişimi 64
4.4 Şifreleme Yönteminin Belirlenmesi 65
4.5 Önerilen Kullanım Senaryoları 67
4.5.1 Otomatik doğum günü tebriği maili gönderimi 67
4.5.2 Kampanya e-posta gönderimi 68
4.5.3 Servis durumu bilgilendirmesi 68
5. BULGULAR VE TARTIŞMA 69
5.1 Bulgular 69
5.2 Tartışma 70
6. SONUÇ ve ÖNERİLER 72
KAYNAKLAR 74

ÖZGEÇMİŞ 82

TABLOLAR LİSTESİ

Tablo 1. Maskeme ve Şifreleme Yöntemlerinin Karşılaştırması 3

Tablo 2. Geleneksel Sistemden Bulut Sisteme Geçiş 10

Tablo 3. Popüler Algoritmaların Karşılaştırması 16

Tablo 4. RC algoritmasının versiyonları 20

Tablo 5. Orijinal Veri 22

Tablo 6. Tablo 5'in Anonimleştirilmiş Hali 22

Tablo 7. Orijinal Maaş/Hastalık tablosu 23

Tablo 8. Tablo 7'nin l-çeşitlilik modeli ile maskelenmiş hali 24

Tablo 9. Tablo 7'nin yakınlık modeli uygulanmış hali 25

Tablo 10. Kişisel Verilerin Korunmasıyla İlgili Uluslararası Genel Düzenlemeler 27

Tablo 11. Hizmet Sağlayıcı Karşılaştırması 34

Tablo 12. Sağlayıcıların Kalite Puanlamaları 35

Tablo 13. Bulut Kullanıcısı ve Hizmet Sağlayıcı ilişkisi 38

Tablo 14. Servis Sağlayıcılarının Güvenlik Sertifikasyonları ve Akreditasyonları 42

Tablo 15. SOC 2 Sertifikasyon İçeriği 44

Tablo 16. PCI DSS Gereksinimleri 45

Tablo 17. Test Sistemlerinin Detayları 56

Tablo 18. CRM Kayıtlarının Yerel Sisteme Aktarılma Süresi 63

Tablo 19. Yerel Ortam Test Sunucuları 66

Tablo 20. Farklı şifreleme algoritmalarının aktarım süreleri 67

ŞEKİLLER LİSTESİ

Şekil 1. Şifreleme ve çözme süreci 2

Şekil 2. Bulut sisteme erişiminde mevcut durum 8

Şekil 3. Çalışma kapsamında kullanılacak mimari 9

Şekil 4. Adejo ve arkadaşları tarafından önerilen yöntem mimarisi 12

Şekil 5. Veri Güvenliğinde Karşılaşılan Zorluklar 14

Şekil 6. Simetrik şifreleme sistemi 17

Şekil 7. 3DES şifreleme/şifre çözme uygulaması diyagramı 18

Şekil 8. AES Algoritması Çalışma Prensibi 19

Şekil 9. Blowfish Algoritması 21

Şekil 10. Kişisel bilgi olarak kabul edilen bilgiler 28

Şekil 11. Güvenlik ve Gizlilik Ayrımı 31

Şekil 12. NIST bulut mimari aktörleri ve katmanları 36

Şekil 13. Bulut Sistemlerde Aktörler Arasındaki ilişki 37

Şekil 14. Güvenlik İçin Risk Yönetim Süreci 41

Şekil 15. ISO 27001 Uyum Adımları 43

Şekil 16. CSA STAR Standartları 47

Şekil 17. Veri Yerelleştirme İçin Genel Mimari 48

Şekil 18. Yerel Veritabanında Saklanan Örnek Bir Veri 49

Şekil 19. Web Servis Fonksiyonları 51

Şekil 20. Web Servis Fonksiyon Görümünü 52

Şekil 21. Tanımlı güvenlik algoritmaları 52

Şekil 22. Şifreleme Fonksiyonu 53

Şekil 23. Şifre Çözme Fonksiyonu 54

Şekil 25. Anahtar Üretme Fonksiyonu 54

Şekil 26. Farklı Şifreleme Algoritmalarının 102 Byte'lık veriyi işleme süresi 56

Şekil 27. Ön tanımlı ve sonradan tanımlanan kategoriler 58

Şekil 28. Alan tanımları tablosu üzerinde kategori sorgulaması 59

Şekil 29. Dinamik Olarak Sorgulanan Örnek Bilgiler 62

Şekil 30. Değişken paket boyutlarına göre aktarım süresi 63

Şekil 31. Salesforce Lightning Component ile Hassas Veri Görüntüleme 64

Şekil 32. Hassas Veriyi Görüntüleme Performansı Raporu (ms) 65

KISALTMALAR

KVKK	Kişisel Verileri Koruma Kurumu	Personal Data Protection Authority
GDPR	Genel Veri Koruma Kısıtlamaları	General Data Protection Regulations
PII	Kişisel Olarak Tanımlanabilen Bilgi	Personally Identifiable Information
HIPAA	Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası	Health Insurance Portability and Accountability Act
COPPA	Kaliforniya Tüketici Gizliliği Yasası	California Consumer Privacy Act
CCPA	Çocukların Çevrimiçi Gizliliğini Koruma Yasası	Children's Online Privacy Protection Act
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü	National Institute of Standards and Technology
PHI	Korunan Sağlık Bilgileri	Protected Health Information
CRM	Müşteri İlişkisi Yönetimi	Customer Relationship Management
DES	Veri Şifreleme Standardı	Data Encrypton Standard
3DES	Üçlü Veri Şifreleme Standardı	Triple Data Encryption Standard
AES	Gelişmiş Şifreleme Standardı	Advanced Encryption Standard
RC	Rivest Şifrelemesi	Rivest's cipher
NBS	Ulusal Standartlar Bürosu	The National Bureau of Standards

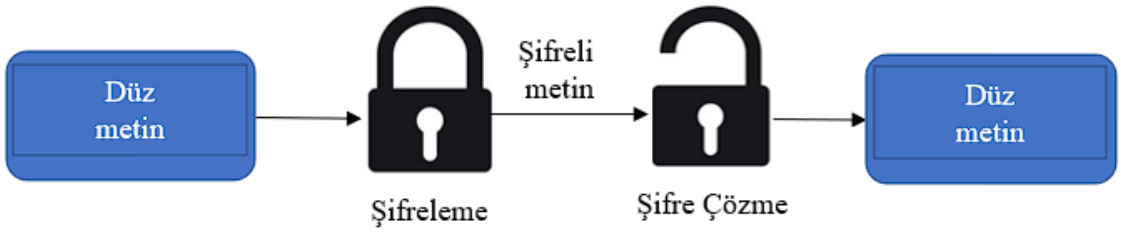
FIPS	Federal Bilgi İşleme Standartları	Federal Information Processing Standards
EDE	Şifreleme-Şifre Çözme-Şifreleme	Encryption-Decryption-Encryption
OECD	Ekonomik İşbirliği ve Kalkınma Örgütü	Organisation for Economic Co-operation and Development
TCKN	Türkiye Cumhuriyeti Kimlik Numarası	Identity Number
VKN	Vergi Kimlik Numarası	VAT Number
IBAN	Uluslararası Banka Hesap Numarası	International Bank Account Number
IP	Internet Protokolü	Internet Protocol
DLP	Veri Kaybı Önleme	Data Loss Prevention
CASB	Bulut Erişimi Güvenlik Aracısı	Cloud Access Security Broker
SaaS	Yazılım Hizmeti	Software as a Service
PaaS	Platform Hizmeti	Platform as a Service
IaaS	Altyapı Hizmeti	Infrastructure as a Service
EC	Avrupa Komisyonu	European Commission
ISO	Uluslararası Standardizasyon Örgütü	International Organization for Standardization
SOC	Hizmet Organizasyon Kontrolü	Service Organization Control
PCI DSS	Ödeme Kartı Endüstrisi Veri Güvenliği Standardı	Payment Card Industry Data Security Standard

CSA	Uyumluluk, Güvenlik, Sorumluluk	Compliance, Safety, Accountability
API	Uygulama Programlama Arayüzü	Application Programming Interface
ID	Kimlik Bilgisi	Identification
SMS	Kısa Mesaj Hizmeti	Short Message Service
AB	Avrupa Birliği	European Union
BM	Birleşmiş Milletler	United Nations
ENUM	Numaralı listeler	Enumerations

1. GİRİŞ

Avrupa birliği ülkelerinde GDPR olarak adlandırılan kanun her ne kadar 2016 yılında yayınlanmış olarak gözükse de temelleri 1995 yılına dayanmaktadır (GDPR, 2016). Bulut tabanlı uygulamalar varsayılan olarak GDPR'a göre kurgulandığından GDPR'a tabi ülkelerde çevrimiçi bulut tabanlı uygulamaların kullanımı bu kısıtlar göz önünde bulundurularak kurgulanmıştır. Ülkemizde bu uygulamaları kullanan firmaların sayısı hızla artarken bu uygulamaların üzerinde sakladıkları verilerin KVKK'ya uygun bir şekilde kullanılmaması mevzuata aykırı bir kullanım durumunu ortaya çıkartmaktadır (Yılmaz, Arıkan, Su ve Yurekten, 2020). Mevzuatın hukuk birimleri tarafından yeterli teknik altyapıya sahip olmadan yorumlanması ve yanlış kullanım modellerinin uygulanması veri güvenliğini ve gizliliğini tehlikeye atmaktadır. Benzer durumda, saklanan verinin sınıflandırılması konusunda da belirlenen yanlış kullanımlar kişisel verinin gizliliğini ihlal etmektedir. Gizlilik ihlali sonucunda doğrudan erişime açık veri tamamen mevzuata aykırı bir durum oluşturur. Basit bir ifade ile yaklaşacak olursak gizlilik konusunda yetkilendirme bu süreçte büyük önem taşımaktadır. Örneğin fiziksel olarak erişilebilen matbu belgelerin saklandığı arşivler, dolaplar işletmelerde çalışan kişilerin yetki seviyelerince özel anahtar veya kartlarla erişilirken uygulamalar üzerinde saklanan verilerinde benzer yetki seviyeleri ile erişilebilir olması gerekmektedir (Savaş, Zaim ve Aydın, 2020). Verinin mahremiyetini düşündüğümüzde bu çalışma içerisinde belirtilecek şifreleme yöntemleri ele geçirilen verilerin gizliliğini koruyup üçüncü kişilerin hukuka aykırı bir şekilde erişmesinin önüne geçer (Paşaoğlu ve Cevheroğlu, 2020). Bu anlamda hukuka ve veri güvenliğine uygun yöntemlerin belirlenmesine ihtiyaç vardır. Çalışılacak konunun içeriği dönemsel olarak hızla yenilenebileceğinden yeniliklere açık bir zemin oluşturmaktadır (Yılmaz, Arıkan, Su ve Yurekten, 2020). Kritik iş süreçlerinde uzaktan sunulacak hizmetin huzurda verilen hizmet kadar hızlı ve güvenli sunulma zorunluluğu vardır (Şahinaslan vd., 2023). Dolayısıyla kişisel verilerin bulut ortamında saklanmasında ve kullanımından kaynaklı güvenlik, uyum ve hukuksal anlamda çeşitli problemler yaşanmaktadır. Bulut tabanlı altyapılar hali hazırda bu işi yaptıkları için veri güvenliğini sağlamak adına küçük işletmelere göre önemli tecrübeye sahiptir. Bu sebeple birçok büyük ölçekli firmalar dahi uygulama altyapılarını bulut

sistemlere taşıyor. Taşıma süreci öncesinde bu işletmeler taşıyacakları bulut sistemin güvenlik altyapılarını detaylı olarak irdeleyip sistemin sunduğu güvenlik düzeyinin en az işletmenin sahip olduğu güvenlik düzeyi kadar olduğundan emin olmaları gerekmektedir (Petkovic, 2010). Şekil 1'de temel anlamda şifreleme sürecinin akışına yer verişmiştir.



Şekil 1. Şifreleme ve çözme süreci

Şifreleme temel olarak simetrik ve asimetrik olmak üzere iki tipte karşımıza çıkmaktadır. Simetrik şifrelemede kullanılan anahtar şifre çözme sürecinde de kullanılmaktadır. Asimetrik şifrelemede ise genel ve gizli anahtar kelime kullanılmaktadır (Arshad, Umair, Munawar, Naveed ve Naeem, 2020). Yapılan çalışmalarda anahtarların genel kullanımı yerine gizli olarak dağıtılması güvenlik performansını artırdığı gözlemlenmektedir. Bu tez çalışmasında yapılan çalışmada kullanılacak şifreleme yöntemlerinde anahtarlar gizli olarak konumlandırılıp dinamik bir şekilde üretilecektir.

1.1 Problem

Dijitalleşme hızının oldukça yüksek olduğunu günümüzde verilerin önemi giderek artmaktadır. Birçok alanda dijital dönüşüm ilerlerken özellikle sağlık alanında daha hızlı ilerlemektedir. Kişilerin sağlık verileri, tedavi süreçlerindeki araştırmalar gibi geniş bir alanda üretilen bilgilerin saklanması ilerleyen teknolojinin getirdiği yeni zorluklarla karşı karşıya kalmaktadır. Saklama ve güvenlik hizmetlerinin sağlanması, bu hizmetlerin ölçeklendirilebilmesi için bulut tabanlı hizmetler avantajlı bir şekilde öne çıkmaktadır.

Literatür taramasında ulaşılan çalışmaların genel çerçevesi kontrol edildiğinde veri gizliliği ile ilgili çalışmaların çoğunluğunun sağlık sektörüne yönelik olduğu gözükmektedir. Bu çalışmaların detayında tıbbi verilerin yüksek gizlilik gerektirdiği ve bunun sağlanması için HIPAA kısıtlamalarının dikkate alınması gerektiğinden bahsedilmektedir (Kahrobaei, Najarian, Shpilrain ve Wood, 2019). Sağlık alanında

yapılacak gizlilik çalışmalarının uygun altyapıda kurgulanarak farklı sektörlerde uygulanabilirliği değerlendirilmelidir.

Klinik ve sağlık kuruluşlarınca bir günde oldukça büyük veri üretilmektedir. Üretilen bu veriler doğrudan kişilerle ilişkili olduğundan sızması veya yetkisiz kişilerce erişilmesi durumunda finansal, sosyal ve sağlık açısından hasar verici sonuçlar doğurabilir. Bölgesel ve uluslararası olarak birçok kısıtlama olmasına rağmen bunlar arasından HIPAA ve GDPR ön plana çıkmaktadır (Shuaib, Alam, Alam ve Nasir, 2021). GDPR'ın sadece Avrupa Birliği ülkelerine yönelik olması Avrupa'da yer alan Amerika kökenli işletmeler için büyük para cezalarına neden olabiliyor. Bu durumu önlemek için 2018 yılında California GDPR kısıtlamalarını yansıtan kendisine ait gizlilik yasasını çıkarttı. Bu hukuk düzenleri karşılaştırıldığında bu çalışmaların tam olarak kapsadığı verinin detayına yeteri kadar dikkat edilmediği görülmektedir. Kişisel veri ve kişisel bilginin farklarının bu yasalara göre belirlenip farklılıkların ortadan kaldırılması için çalışmalar yapılması gerekmektedir (Voss ve Houser, 2019). Yapılan literatür araştırmasında ulaşılan çalışmaların ortak noktasının dünya genelinde bir model oluşturup kısıtlamaların bu model çerçevesinde uygulanmasını sağlamaktır. Verinin anonimleştirilmesi mahremiyeti açısından oldukça bir öneme ve uygulamada zorluğa sahiptir. Anonimleştirme, veri üzerinden gerçek kişiye ulaşılmayı engellemeyi hedefler. Literatürde anonimleştirmede kullanılan ve kişisel verinin açık bir şekilde paylaşılmasını engelleyen başlıcaları k-anonimlik, l-çeşitlilik ve t-yakınlık olmak üzere birkaç yöntem bulunmaktadır (Canbay, Sağıroğlu ve Vural, 2022). Tablo 1'de yapılan karşılaştırmaya göre maskelenen verinin uygulamalar üzerinde gerçek veri olarak kullanılması mümkün olmamaktadır. Bu sebeple veriyi kontrollü olarak erişilebilir bir hale getirmek için güvenli yöntem şifreleme ile saklama yöntemidir.

Tablo 1. Maskeme ve Şifreleme Yöntemlerinin Karşılaştırması

Durum	**Maskeleme**	**Şifreleme**
Geri dönüştürülebilir mi?	Hayır. Orjinal veriye geri dönülemez.	Evet. Yetkili erişim sonucunda oluşturulan şifreli verinin geri dönüşü mümkündür.

Brute-Force yöntemlerle saldırıya açık mı?	Hayır. Maskelenen veride çalınabilecek nitelikte gerçek kişi bilgisi bulunmadığından yetkisiz erişim ile çalınabilecek bir bilgiye erişilemez.	Evet. Yeterli süre ile deneme yapılması durumunda kullanılan şifreleme yöntemine bağlı olarak değişken sürelerde çözülmeye uygundur.
Şifreleme anahtarına bağlı bir güvenlik var mı?	Hayır. Maskeleme işleminde anahtara bağlı bir güvenlik yapısı bulunmadığından anahtar üzerinden erişim riski bulunmamaktadır.	Evet. Kullanılan şifreleme algoritmasına bağlı olarak kullanılan anahtarlama yapısı güvenlik oranını farklı oranlarda artırıp azaltacaktır.

Şifreleme ile veri saklama yöntemi dünya çapında kabul görmüş şifreleme algoritmalarını kullanmak veri güvenliğini artıracaktır. Bu süreçte ele alınacak yöntemler değerlendirilirken performans sorunu ortaya çıkmaktadır. Performans sorunun ortadan kaldırılmasından ziyade en az zaman kaybı ile verinin mahremiyetini sağlamak ana problemin çözümüne olumlu yönde katkı sağlayacaktır. Veri şifrelemede çevrimiçi şifreleme yöntemleri ile sürecin daha hızlı ilerlediği savunulmaktadır. Ayrıca çevrimiçi şifreleme yöntemlerinde şifreleme anahtarlarının kullanıcı üzerinden değil, dışarıdan paylaşılması ile güvenlik daha da artırılmaktadır (Rajani ve Vijay, 2017). Çevrimiçi şifreleme, internet ortamında bulunan verilerin transferi sırasında kullanıldığından olası saldırı ve sızmalara karşı önemli bir güvenlik önlemi olarak kullanılmaktadır. Saldırı ve sızma konusu dışında sistemlere aktif olarak erişebilen ancak güvenlik seviyesince yetkisiz kişilerin bilinçli veya bilinçsiz olarak bu verilere erişmesi engellenmelidir. Çevrimiçi şifreleme modeli ile güvenlik, gizlilik, veri bütünlüğü, uyumluluk ve küresel ortamda erişim avantajları ön plana çıkmaktadır. Günümüzde kullanılan bulut uygulamalarında ortaya çıkan sorunların büyük bir çoğunluğu literatür taramasında görüldüğü gibi veri mahremiyeti hakkında önlemler alınmamasından kaynaklanmaktadır ve bu gibi durumlar yüksek meblağlarda para cezaları uygulanabilmektedir (Barta, Ludvai ve Puskás, 2020). Bu tez çalışmasında bulut uygulamalarında veri mahremiyetinin korunması ele alınarak problemin çözümüne yönelik bir yöntem hazırlanacaktır.

1.2 Amaç

Bu çalışma, günümüzde aktif bir şekilde kullanılmakta olan bulut uygulamalarda saklanan verilerin gerçek anlamda güvenli ve veri güvenliği standartlarına (KVKK, GDPR, HIPAA, vs.) uygun bir şekilde kullanılmasına yönelik bir altyapı oluşturulması amaçlanmaktadır. Ülkemizden kurumsal seviyede erişilebilen bulut sistemlerde, veri gizliliğinin ihlal edilmesini engellemek ve KVKK kısıtlarına göre yönetilebilir bir akış oluşturulması hedeflenmiştir. Veri niteliğine göre şifreleme yöntemi ile gizlilik sağlayan bulut tabanlı güvenli bir çözüm yöntemi üzerinde çalışılacaktır.

Bu çalışmada yapılacak uygulama ile işletmelere bulut uygulama seçiminde yol gösterici bir rehber olacaktır. Böylece kullanılacak bulut sistemlerin, mevcut iş süreçlerine uyarlanmasında dikkat edilmesi gereken aşamaların detayları belirlenmiş olacaktır.

1.3 Önem

Bu çalışma; işletmelerin sahip oldukları verileri bulut uygulamalarda güvenli ve kısıtlama mevzuatlarına uygun bir şekilde kullanmaları için yetkililere kılavuzluk edecek niteliktedir. Aynı zamanda kapsamı bakımından işletmelerin bulut ortamda kullandıkları uygulamalarda veri sınıflandırma ve saklama süreçlerinin iyileştirilmesine katkı sunacaktır.

Bulut ortamında yer alan verilerin mahremiyetinin sağlanması güvenlik ve yasal uyum bakımından oldukça kritiktir. Veri mahremiyetinin sağlanamaması durumunda işletmelere ciddi yaptırımlar ve hukuki sorumluluklar yüklenmektedir. Telafisi mümkün olmayan pek çok sonuçla karşılaşılabilmektedir. Bu çalışmada geliştirilecek altyapı önerisi ile yaşanabilecek bu problemlerin önlenmesi bakımından önemlidir.

1.4 Varsayımlar

Çalışmada literatür araştırmaları yanında sektördeki en iyi uygulamalardan elde edilecek çıktıların doğru ve güvenilir olduğu kabul edilecektir. Çalışmada kullanılacak örnek verilerin herhangi bir veri sınıflandırmasına tabi tutulmadan bulut ortamında açık bir şekilde saklandığı varsayılacaktır. Yapılan literatür araştırmalarında açıl bir şekilde görüldüğü üzere dosya tipindeki verilerin gizliliği üzerinde durulmuştur. Bu çalışmaya konu olacak

veriler herhangi bir dosya verisi olmayıp (resim, ses, video, metin vb.) veritabanında ham hali ile kişisel veri olarak saklandığı kabul edilecektir.

1.5 Sınırlıklar

Bu çalışmada geliştirme ve uyarlamaya açık bulut sistemler üzerinden detaylandırma yapılacaktır. Doğrudan müşteri ile işletme arasında temas gerektiren süreçlere ait veriler ile sınırlandırılacaktır. Bu çalışma kullanılan şifreleme yöntemleri ve teknolojik uygulamalarla sınırlıdır.

1.6 Tanımlar

Bu çalışmada kullanılacak terimlerin ayrıntılı açıklamalarına aşağıda yer verilmiştir.

KVKK: Temel hak ve özgürlükleri korumak için uyulması gereken usul ve esasların yer aldığı Kişisel Verilerin Korunması Kanunu (KVKK, 2016) olarak ifade eder. Yurtiçinde bulunan kişisel verilerin saklanması, korunması ve müşteri rızası ile işlenmesini kanunen korumayı amaçlayan bir yasadır. Genel hedefi bu verilerin hukuk ilkelerine uygun olarak güvenli bir şekilde işlenip, bireylere ait olabilecek bütün verileri koruma altına almak ve bu sayede özel hayatın gizliliğini güvence altına almaktır. Türkiye içerisinde yer alan veri saklayan ve işleyen bütün kuruluşlar bu yükümlülüğe uymak zorundadırlar.

GDPR: Avrupa Birliği ülkeleri tarafından gerçek kişilerin verilerini korumak üzere düzenlenmiş mevzuat olup Genel Veri Koruma Mevzuatını (GDPR, 2016) ifade eder. Avrupa Birliği içerisinde yer alan veya Avrupa Birliği vatandaşlarının verilerini barındırıp işleyen bütün işletmeleri kapsamaktadır. Verilerin saklanması ve işlenmesi için verinin asıl sahibi olan vatandaşlardan açık ve net bir şekilde rıza alınması gerekliliğini ortaya koymaktadır ve bu rıza metni içerisinde şeffaf bir şekilde verinin hangi yollarla işlenip, nasıl kullanılacağı ile ilgili detay barındırmak zorundadır.

Şifreleme: Verinin okunduğunda anlamlandırılamayacak bir şekilde güvenli olarak matematiksel işlemler sonucunda değiştirilmesi işlemidir. İletişim anında veriye ulaşılması durumunda şifrelenen verinin insan gözü tarafından anlamlandırılması oldukça zordur.

Anonimleştirme: Kişilerin gizliliğini ihlal etmemek amacıyla ulaşılabilen verilerin içeriğinin maskelenmesini veya tekil anahtar ile işaretlenerek saklanması işlemini ifade eder (Majeed ve Lee, 2021). Veri işleme süreci başladığında anonimleşmiş verilerin gizliliği açık haline göre oldukça yüksektir. İşlenecek veri içerisinde bulunan doğrudan veya dolaylı olarak bir bireye ulaşılmayı sağlayan bilgilerin rastgele farklı bilgiler kullanılarak değiştirilmesi ile gerçek kişiye ulaşılabilmesi engellenmeye çalışılmaktadır.

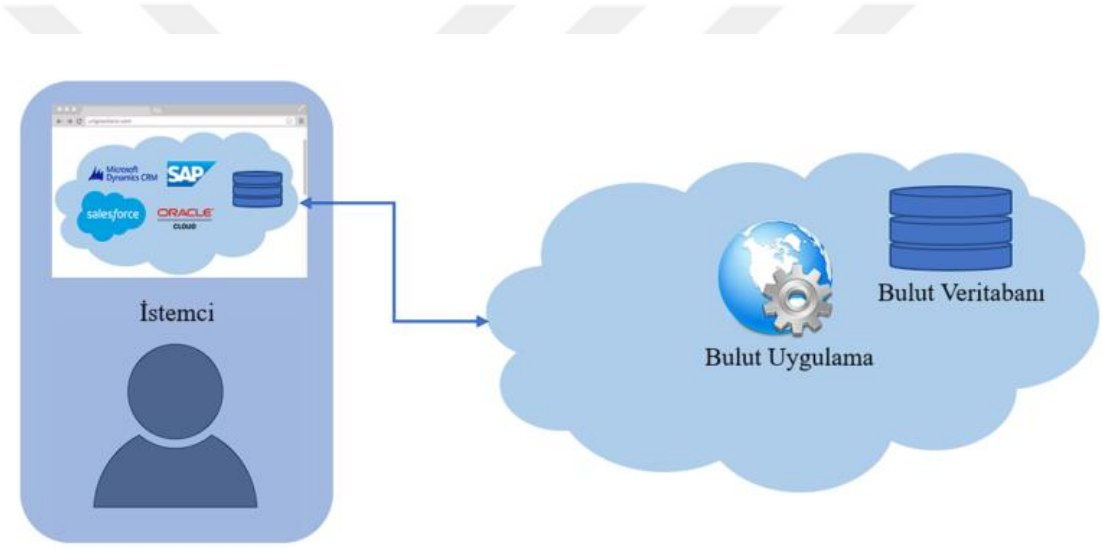
Kişisel Veri: Sahip olunan bilgiler ile gerçek kişiyi tanımlamaya yetecek niteliğe sahip veriyi ifade eder. Doğrudan veya dolaylı olarak gerçek kişiye ulaştırabilir olması yeterlidir. İlk bakışta düşünüldüğü gibi sadece isim, vatandaşlık numarası veya telefon numarası gibi temel bilgiler değil, sağlık bilgileri, coğrafi bilgiler, biyometrik bilgiler ve ip adresi gibi farklı niteliklere sahip tanımlayıcı diğer bilgiler gibi geniş bir alan olarak belirtilebilir. Bu kapsamda toplanan veriler anket, pazarlama ve analiz gibi oldukça geniş alanlarda kullanılabilir. GDPR ve KVKK tarafından yapılan tanımlarda benzer şekilde ifade edilmektedir.

Enum: Programlama dilinde özel bir sınıf olarak kullanılır. Bir grup sabit değerler kümesini temsil eder. Sadece okunabilir, değiştirilemez.

Veri Göçü: Pratikte aktif olarak kullanılan adı Data Migration'dır. Yeni bir sürecin, uygulamanın, sistemin canlı kullanıma açılması ile eski yapıda bulunan verilerin toplu olarak yeni sisteme aktarılması aşaması veri göçü olarak tanımlanır. Sahip olunan veriler işletmenin kurumsal hafızasını oluşturduğundan, bu veriler olmadan yeni yapının kullanılması işletmeyi faaliyetlerini durduracak veri kaybı durumuna sokabilir. Genel olarak, veri merkezi eşitlemesi, uygulama güncellemeleri, bulut sistem geçişleri, şirket yönetimlerinin birleşmesi veya veri merkezi taşınması gibi süreçlerde uygulanır. Taşınacak verinin büyüklüğü, kesinti anında oluşabilecek kriz durumuna göre önceden detaylı planlama yapmayı gerektirir.

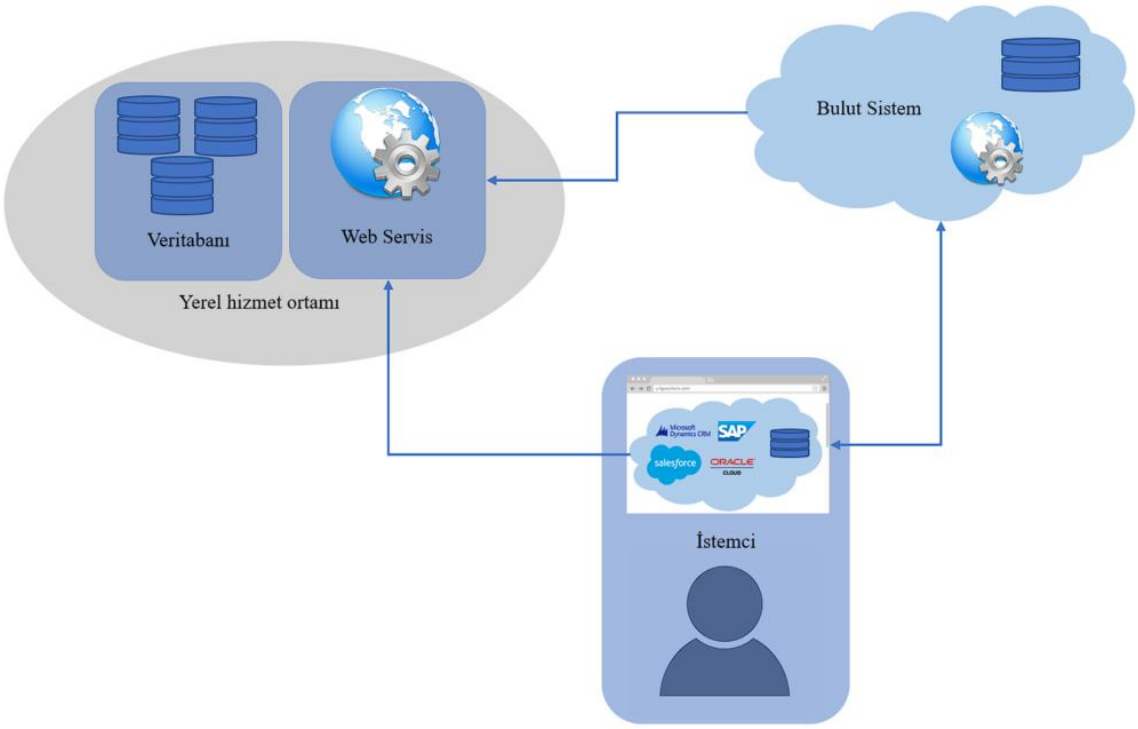
2. GENEL BİLGİLER

Bulut sistemlerde görüntülenecek veriler sistemlerin arkasında yer alan veri tabanlarında sistemin güvenlik prosedürlerine uygun olarak saklanmaktadır. Veri merkezleri genellikle dağıtık mimari ile yönetilerek farklı ülkelerde konumlandırma yöntemiyle dağıtılır. Bulut uygulama kendi içerisinde uygulama altyapısı ve işletmeye ait verilerin tutulduğu bulut veritabanına sahiptir. Şekil 2'de belirtildiği gibi istemci olarak belirtilen kullanıcı internet tarayıcısını kullanarak işletmesinin sahip olduğu bulut uygulamaya erişim sağlayabilmektedir.



Şekil 2. Bulut sisteme erişiminde mevcut durum

Bu çalışmada bulut sistem üzerinde görüntülenecek verinin web servisler ile Türkiye sınırlarında bulunan veri merkezlerinde saklanıp ön yüz ile güvenli bir şekilde haberleştirilmesi sağlanacaktır. Şekil 3'te önerilen mimari ile ilgili görsele yer verilmiştir.



Şekil 3. Çalışma kapsamında kullanılacak mimari

Şekil 3'te belirtilen şema üzerinde tasarlandığı gibi istemci kendisine ait bir tarayıcı kullanarak bulut uygulamaya erişim yapmaya devam edebilecek, bulut uygulama üzerinde işletmesinin sahip olduğu süreçlere yönelik işlemleri yapabilecek ancak burada hedeflenen süreçte verinin belirteç bilgisi bulut sistem üzerinden gelirken, kullanıcının göreceği kişisel veriler yerel ortamda saklanan bir sunucudan anlık olarak atılan istek ile sorgulanıp gösterilecektir.

Veri haberleşmesinde verinin güvenliğini sağlamak için şifreleme yöntemi belirleme ve maskeleme işleminin bulut sistemde uyarlanarak kullanıcıya görüntülenecek verinin kontrollü olarak ulaştırılması sağlanmıştır. Bu süreçte kullanılacak algoritmalara göre çeşitli ölçümler yapılarak istek-cevap performansları farklı sunucularda testler yapılarak gösterilmiştir.

2.1 Literatür Araştırması

Literatürde verinin gizliliği ile ilgili yapılan çalışmaların büyük bir çoğunluğu sağlık sektörüne yönelik olup bu sektörde elde edilen dosyalar üzerinde gizleme süreçlerinin uygulanmasına yönelik çalışmalardır. Sağlık sektöründe üretilen bu bilgilerin gün geçtikçe artması bu verileri kullanarak medikal, sosyal ve bilimsel anlamda yapılan

çalışmaların önünü açmaktadır. Çalışmalarda kullanılan verilerin mahremiyeti göz önünde bulundurulduğunda araştırmacılar için yeni bir konu daha gün yüzüne çıkmaktadır. Burada araştırmacılar tarafından verinin mahremiyetini sağlamak adına birçok anonimleştirme şeması ortaya koyarken günün sonunda k-anonimleştirme, l-çeşitlilik ve t-yakınlık şemaları oldukça popüler bir şekilde öne çıkmaktadır (Wang, Jia, ve Ke, 2017).

Literatürde yapılan araştırmalarda çok açık bir şekilde maskeleme yöntemlerinin analiz, anlamlandırma süreçlerinde kullanıldığı gözlemlenmiştir. Böylece veri üzerinden yapılabilecek yorumlama çalışmalarının çıktıları veri değişimlerinde doğrudan bozulmaya uğramayacaktır. Veri güvenliği ve gizliliği ön planda tutularak yapılacak işlem devam edebilecektir. Günümüzde bulut bilişim altyapılarının güçlenmesi, internet hızlarının artması ile büyük-küçük birçok işletme tarafından uygulamalar bulut sisteme taşınıyor veya işletmelerin verileri bulut sistemler üzerinde taşınıyor (Sharma, Himanshu, ve Khatri, 2019).

Geleneksel sistemlerden bulut sistemlere geçişte öncelikli değerlendirilmesi gereken konunun güvenlik sorunları olduğu savunulmaktadır (Shaqrah, 2016). Shaqrah'ın yaptığı çalışmada sonuç olarak bilgileri güvenli olarak saklanması en büyük öncelik sıralamasında olduğu belirtilmiştir. Bununla beraber saklanan verilerin güvende olmamasının en büyük nedeni olarak servis sağlayıcıların mimari ve altyapı özellikleri gösterilmiştir. Tablo 2'de bu çalışmada derlenen geleneksel sistemden bulut sisteme SaaS olarak geçişin detaylarına yer verilmiştir.

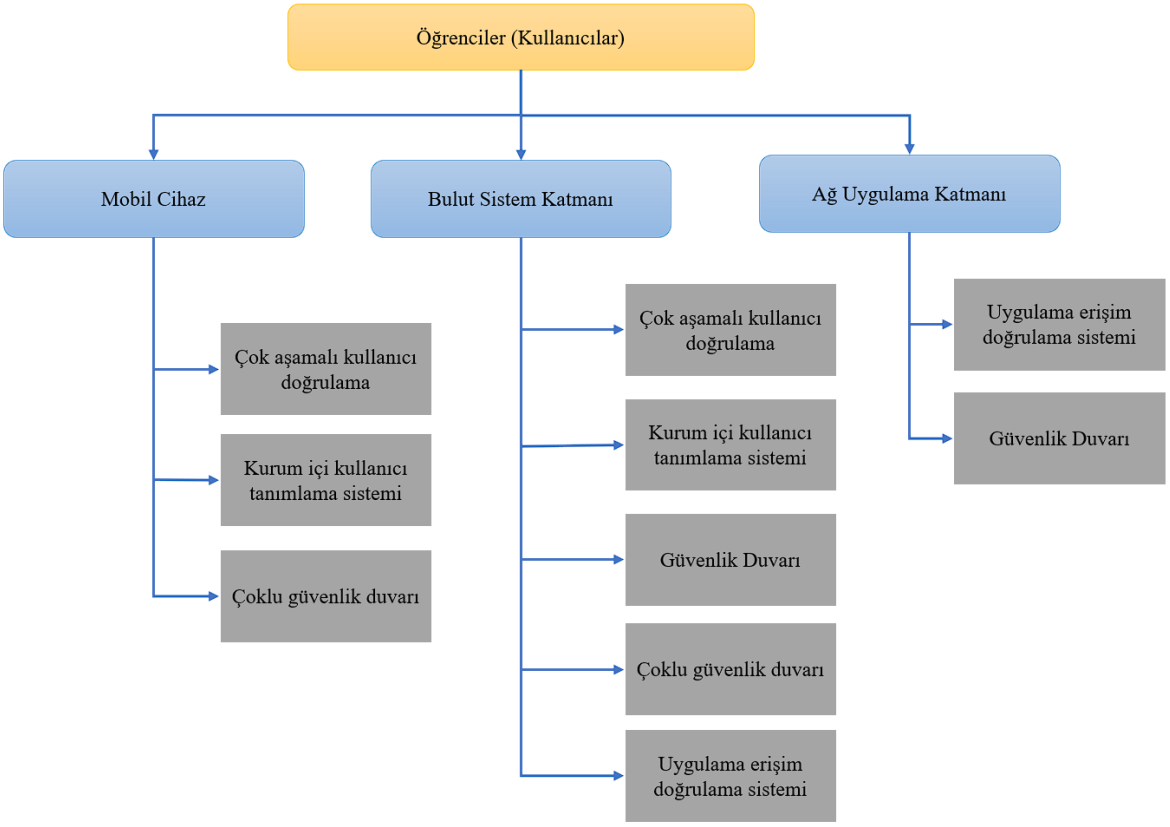
Tablo 2. Geleneksel Sistemden Bulut Sisteme Geçiş

Model	**Geleneksel Sistemler**	**Bulut Sistemler**
Kazanç Modeli	• Ürün satın alınır • Teknik mimari hazırlanır	• Hizmet satın alınır • Mimari hazırdır
İş Modeli	• Ürün için ödeme yapılır • Üst seviye yönetim	• Kullanım için ödeme yapılır • Daha az yönetim ihtiyacı
Erişim Modeli	• Yerel ağ	• İnternet üzerinden

	• İşletme bilgisayarları	• Herhangi bir cihaz
Teknik Model	• Paylaşımsız, tek sunucu • Statik	• Çoklu sunucu, ölçeklendirilebilir • Elastik • Dinamik
Teslim Modeli	• Maliyetli ve uzun süren canlı geçişleri • Bakım maliyeti • Yer işgaliyesi	• Daha hızlı canlı geçişi • Daha hızlı yatırımdan geri dönüş kazanma

Bulut bilişim sistemlerinde veri saklama ihtiyacının üretilen verilerin artması ile doğru orantılı olarak arttığını belirten Tuğbagül Altan Akın bu alanda bulut tabanlı depolama çözümlerinin tercih edildiğini belirtmiştir. Tercih edilen bu çözümlerin gizlilik ve mahremiyet gibi konularda ortaya çıkarabileceği problemlere değinip bu konuda alınabilecek önemlerden bahsetmiştir. Sistemlerin güvenliklerinin, yine bu sistemlere bağlı çözümler ile sağlanması gerektiğini belirtirken, gizlilik için sunulan çözümlerin yeterli olmadığını belirtmektedir (Altan Akın, 2014). Çözüm önerisi olarak bulut sistemlere yüklenecek belgelerin çevrimdışı ortamda şifrelenip çevrimiçi ortama yüklenmesi gerektiğini savunmaktadır.

İnternet tabanlı eğitim sistemlerinin güvenliği üzerine çalışma yapan Adejo ve arkadaşları, bulut yapılarda verinin korunması ve güvenliği ile ilgili yaptıkları çalışmada günümüzde e-öğrenme sistemlerinin artık mobil öğrenme ve hatta bulut tabanlı öğrenme sistemleri haline döndüğünü belirtmektedir. Eğitim sektörünün teknoloji ile iç içe olması, bulut teknolojilerinden faydalanması gelişim anlamında yüksek oranda fayda sağlarken güvenlik ve korunma anlamında öğrenciler tarafından bir çekince uyandırmaktadır. Bu çekincelerin ortadan kaldırılması için bulut sistemlerde uygulanabilecek yetkilendirme, şifreleme, dağıtık depolama mimarisi yedekleme ve yedekten geri dönme gibi konulara değinilmiştir (Adejo, Ewuzie, Usoro ve Connolly, 2018). Şekil 4'te bu konuda belirtilen mimariye detaylarıyla yer verilmiştir.



Şekil 4. Adejo ve arkadaşları tarafından önerilen yöntem mimarisi

Güvenlik ve gizlilik üzerine Ömer Aydın tarafından yapılan çalışmada içerik olarak veri mahremiyeti detaylı bir şekilde tanımlanmış olup konunun öneminden bahsedilmiştir. Buna ek olarak bulut tabanlı sistemlerde paylaşılan içeriklerin artması ile mahremiyet konusuna dikkat çekilip, olası tehditlerin hukuk ve teknolojinin imkanları ile çözümüne yönelik tartışmaya yer verilmiştir. Bu tez çalışmasında yer verdiğimiz maskeleme ve şifreleme süreçlerine detaylı bir şekilde değinerek veriyi anonimleştirme ve diferansiyel mahremiyet konularını açıklamıştır. Sürecin detayında birey ve bireye ait belirtici bağlantıyı koparma yöntemin üzerinde durulmuş ancak bunun yeterli bir önlem olmadığı belirtilerek çeşitlilik yöntemini ele almışlardır. Son olarak yine bu tez çalışmasında değinilen maskeleme yöntemlerinin sonuncusu olan yakınlık modelini kullanarak veriye yapılan izinsiz erişim ile gizliliği sağlamaya çalışmıştır (Aydın, 2022).

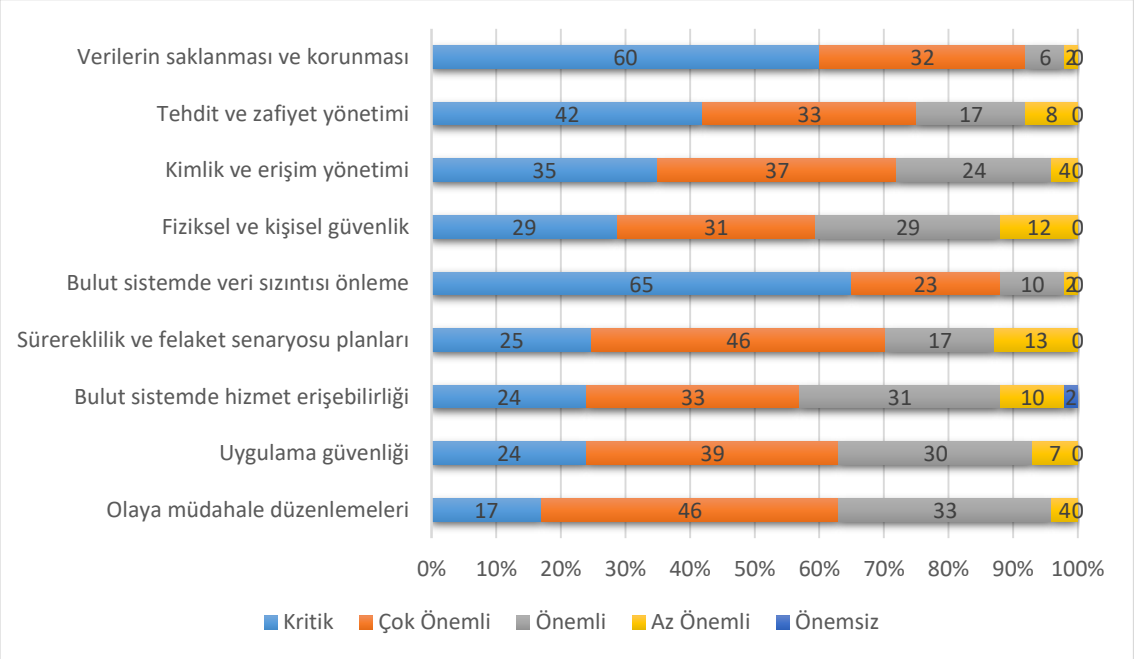
Bulut bilişim sistemlerinin popüler olmaya başladığı dönemlerde yapılan bir çalışmada, bu işletmelerin bir kısmı ise yaptıkları iş açısından kritik olan süreçleri gizlilik ve bulutta bulunan verinin güvenliği ile ilgili çekinceleri sebebiyle bulut ortama taşıma konusunda temkinli davrandığı konusuna değinilmektedir (Chen ve Zhao, 2012).

Henüz veri koruma kanunları ve uluslararası kısıtlamaların olmadığı bu dönemlerde işletmeler tarafından bunun gibi çekinceler yaşanması normal karşılanmaktadır. Günümüze gelindiğinde literatürde hala bu konuda çeşitli çalışmaların yapılmaya devam edildiği gözlenmektedir. Bu sebeple konu hala güncelliğini koruyup bu alanda yapılacak çalışmalara açık olduğu göz ardı edilemez şekilde ortadadır. Burada yola çıkarak yapılan literatür araştırmasında karşılaşılan başka bir sonuç ise, bulut bilişim sistemlerinin her geçen gün hızla geliştiği bu gelişmelerin yeni problemlere yol açacağı yönündedir. Bu sebeple veri maskeleme, yetkilendirme, şifreleme, bütünlük kontrolleri hali hazırda yapılabilmesine rağmen piyasada yer alan uygulamalar tarafından hala tamamen güvenli bir şekilde çözülemediği düşünülmektedir. Bu sebeple bunun gibi sorunların çözülebilmesi için gelecek teknolojiler ve modern yazılım mimarilerini ele alan daha fazla araştırma ve gerçekleştirme çalışması yapılmalıdır (Soni, Ambalkar ve Bansal, 2016).

Bulut sistemlerin benimsenerek kullanılmasının önündeki engellerden bir tanesi işlenen kişisel verilerin sızması ve mahremiyet kavramının ortadan kalkmasıdır (Mowbray ve Pearson, 2009). Mowbray ve arkadaşının yaptığı çalışmada bulut sistem kullanım senaryoları incelenmiş, burada riski azaltmaya yönelik alınacak önlemler altında buluta gönderilecek hassas veri miktarının azaltılması önerilmiştir. Ancak bu yöntemin uygulanabilirliği iş süreçleri ile doğrudan etkili olduğundan kullanımı için doğru ve eksiksiz bir iş süreci analizi yapılması gerekmektedir.

Literatür incelemesinde yapılan çalışmaların birçoğunun yazılımsal seviyede güvenlik durumu değerlendirdiği görülmektedir ancak Sun ve arkadaşlarının yaptığı çalışmada donanım seviyesinde de güvenlik önlemlerinden bahsedilmiş ve bu konu ile ilgili alınabilecek önlemlerin yapılan çalışmalarca karşılaştırması yapılmıştır (Sun, Zhang, Xiong ve Zhu, 2014). İşletmelerin tamamen güvenli bir bulut sistem yapısı kurulmadan tüm yapılarıyla bulut sistemlere geçmeyeceğini belirtmişler. Güven ortamının oluşabilmesi için yapılan çalışmaların yeterli seviyede olmadığı, önerilen yöntemlerin güvenlik anlamında boşlulara sahip olduğu öne sürülmüştür. Araştırmacılar tarafından bu konunun önünün açık olduğu ortadadır ve güvenilir bir ortam oluşturulması için daha fazla çalışma yapılması gerekmektedir.

Rao ve arkadaşının yaptığı bulut ortamlarda veri güvenliğinin zorluklarını konu alan çalışmada çözüm önerisi olarak verilerin bulut ortamda kimlik tabanlı doğrulama ile RSA şifreleme yöntemi kullanılması sunulmuştur (Rao ve Selvamani, 2015). Ancak burada da diğer çalışmalarda olduğu gibi uyarlanacak güvenlik önlemlerinin henüz yeterli seviyede olmadığı, bu konu üzerinde daha gelişmiş şifreleme tekniklerinin kullanılması gerektiğine değinilmiştir. Yaptıkları çalışmada veri güvenliği ile ilgili zorluklara Şekil 5'te detaylı bir şekilde yer verilmiştir.



Şekil 5. Veri Güvenliğinde Karşılaşılan Zorluklar

Yapılan araştırmalarda veri sızıntısını önleme ve verilerin korunaklı bir şekilde saklanması veri güvenliği zorlukları arasında temek etkiyi oluşturan konular olarak gözükmektedir.

2000'li yılların sonunda dijital içerik üretme sıklığının arttığını, bununla ilgili insanların platformlara kendi ürettikleri içerikleri yüklemelerini ve bu verilerin gizliliğini konu alan Pearson ve arkadaşlarının çalışmasında, yüksek kalite dijital kameralar ve güncel yazılım sürümüne sahip cep telefonları ile çekilen fotoğraflarda konum bilgisinin yer almasının ve bu bilgi ile harita üzerinde ev, seyahat rotası gibi mahrem kabul edilebilecek bilgilerin görüntülenebilmesinden bahsedilmiş ve bu bilgilerin bulut ortama yüklenirken değiştirilmesi için yöntem önerisinde bulunulmuştur (Pearson, Shen ve Mowbray, 2009).

Burada belirtilen yöntem ile bulut sisteme yüklenen içeriğin dosya öznitelik bilgileri değiştirilerek doğru olmayan bilgilerle gerçek verinin gizliliğini koruması hedeflenmiştir.

Dosya yapıları üzerinden yapılan çalışmalarda ele geçirilen veya yetkisiz bir şekilde erişilen verinin uygun bir modelle şifrelenmesi sonucunda kolaylıkla açığa çıkamayacağı vurgulanmaktadır (Sharma, Himanshu ve Khatri, 2019). Bunlara ek olarak şifreleme süreçlerinde güvenliğin artırılması için çok katmanlı şifreleme süreçlerinin uygulanması gerektiği belirtilmektedir. Ancak dikkat edilmesi gereken konulardan bir tanesi, gelişen teknolojinin bulut bilişim sistemlerini sadece son kullanıcılarla değil "Nesnelerin İnterneti" konseptindeki cihazlarla iletişim kuruyor olması nedeniyle şifreleme süreçlerinin daha basit şekilde yapılarak cihazlar üzerinde oluşabilecek yükü en aza indirmeye çalışılması gerekmektedir.

Literatür araştırmalarının detayına inildiğinde gerek bulut tabanlı gerekse yerel ortamlarda yapılan araştırmaların neredeyse tamamı verilerin dosya seviyesinde şifrelenmesi üzerinde durmuştur. Metin, resim, video ve ses gibi formatlarda bulunan dosyaların şifrelenmesi ve bulut sistemlerde güvenli bir şekilde barındırılması üzerine araştırmalar yapılmış olup genel olarak varılan sonuçta saklanan bu verilerin güvenli bir şifreleme süreci ile barındırılmaması durumunda yetkisiz erişim ve veri çalışması gibi durumlarda ciddi problemlere yol açacağı belirtilmiştir. Elde edilen bilgiler ışığında küçük boyutlu metin bazlı veri gizliliğini artırma ihtiyacı bu tez çalışmasına konu olan durumun gerekliliği bir kez daha ortaya çıkmıştır.

Bu tez çalışmasının sağladığı en büyük katkının bulut sistemlerin yurt içinde kullanılırken gerek uluslararası gerekse yurtiçinde işlenen verilerin kişisel veri güvenliği kısıtlamalarına uygun olarak farklı sistemler tarafından kolayca uyarlanabilecek bir yapı örneği sunmuş olması düşünülmektedir.

2.2 Kişisel Verilerin Şifrelenmesi

Bulut sistemlerin yaygın olarak üst düzey kuruluşlar tarafından kullanılması ile veri güvenliğine olan ihtiyaç gün geçtikçe hızla artmaktadır. Kuantum bilgisayarların hız artışı, kullanılan kripto algoritmalarını tehdit etmektedir (Sahinaslan ve Sahinaslan, 2019). Yapılan literatür taramasında genel olarak bulut sistemler üzerinde şifreleme

süreçleri dosya tabanlı olarak işletilmiş olup bu çalışmada konu genel olarak anlık metin verisi üzerinde gerçekleştirilecektir. Temel olarak şifreleme algoritmalarında DES, 3DES, AES, RC ve Blowfish ile çalışmalar yapılacak ve bunlar arasında bulut sistemde akıcı bir deneyim ile verinin ilgili kişiye gösterilebilmesi sağlanacaktır. Tablo 3'te DES, 3DES, Blowfish ve AES şifreleme algoritmalarının altyapısı ile ilgili detaylı bilgiye yer verilmiştir. Tablodaki verilerden yola çıkarak Blowfish algoritmasının performans değerlendirmesi bakımından bu teze konu yapılacak uygulamada kullanımının daha uygun olduğu görülmektedir.

Tablo 3. Popüler Algoritmaların Karşılaştırması

Nitelik	**DES**	**3DES**	**Blowfish**	**AES**
Anahtar Uzunluğu	56 bit	112 veya 168 bit	448 bit	128, 192 veya 256 bit
Blok Boyutu	64 bit	64 bit	64 bit	128 bit
Geliştirilme Tarihi	1975	1978	1993	2000
Performans	Yavaş	Yavaş	Hızlı	Hızlı
Güvenlik	Zayıf	Zayıf	Orta	Kuvvetli
Saniyede 50 milyar anahtar denemesi ile çözülme süresi	400 gün	800 gün	Yaklaşık 3200 gün	Yaklaşık $5x10^{21}$ gün

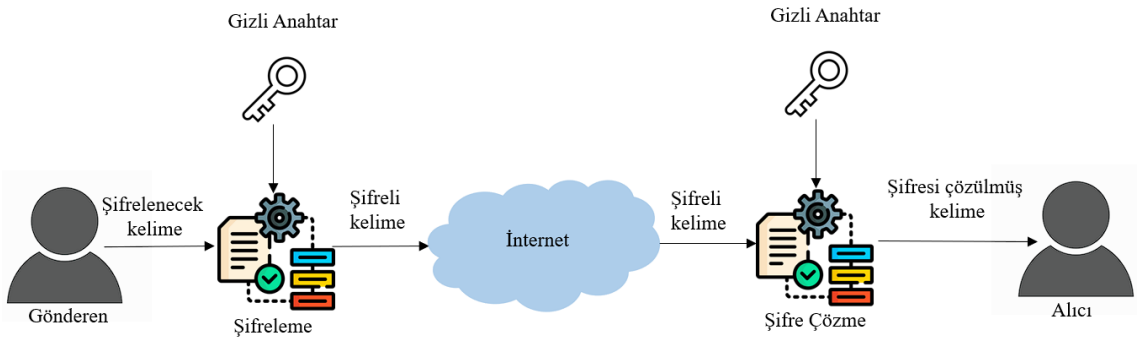
Kıyaslama için telefon numarası, e-posta adresi, kimlik numarası, pasaport numarası gibi doğrudan kişilere ulaşılabilecek nitelikteki veriler kullanılarak belirtilen şifreleme algoritmaları ve uygulanacak maskeleme yöntemleri ele alınacaktır. Verinin karakteristik özelliğine göre akıllı seçim süreçleri kurgulanarak performans kaybının önüne geçilmesi hedeflenmektedir. Bu çalışma içerisinde temel alınacak konu farklı ülkelerdeki kişisel veriye erişim mevzuatlarının uygulanabilir olmasını sağlamak olduğundan oluşturulacak yapının bu değişimlere göre dinamik olarak çalışabilmesi ön planda tutulacaktır. GDPR ve KVKK verinin mahremiyetini koruyan mevzuatların tek bir sistem üzerinde veriye uygulanabilmesi çok uluslu şirketler açısından gizlilik sürecine katkı sağlayacaktır. Geçmişten günümüze Caesar, Vigenere, Enigma gibi birçok klasik şifreleme yönteminin yerini DES, RSA, PGP, AES, SHA-3 gibi daha güçlü modern yeni şifreleme yöntemleri almıştır (Sahinaslan ve Sahinaslan, 2019).

2.2.1 DES

Simetrik veri şifreleme algoritması olan DES (Data Encrypton Standard) 1970'li yıllarda IBM tarafından 1974'te geliştirilen LUCIFER'ın 1977 yılında geliştirilmiş bir versiyonu NBS tarafından duyuruldu. 1980'li yıllarda ise bankacılık işlemlerinde kabul görmüş bir standart olarak kullanılmaya başlandı (Ahmed ve El-Henawy, 2017). Yayınlandığı dönemde sağladığı güvenlik sebebiyle başta finans sektörü olmak üzere birçok alanda kullanılırlığa ulaşmış ve birçok denemeye rağmen kırılamamıştır (J.Shepherd, 1995).

DES algoritması yapısı ve günün teknolojik koşulları gereği 1997 yılına kadar güvenilirliğini korumaya devam etmiştir. Ancak saldırganlar tarafından sürekli açığı aranan algoritma ilk kez 1997 yılında başarılı bir saldırıya uğramıştır. DESCHALL grubu tarafından gerçekleştirilen bu saldırıda internet ortamında bir araya getirilmiş on binlerce bilgisayarın gücünden faydalanılarak anahtar arama saldırı gerçekleştirilmiştir. Teknolojinin ilerlemesi ve maliyetleri düşmesiyle birlikte bu süre 2000'li yılların başında 3.5 saate kadar düşmüştür (C.-W.Phan, 2007).

Şekil 6'da gözüktüğü gibi DES şifreleme algoritması basit seviyede gizli anahtar ile veriyi şifrelemektedir. Şifrelenen veri şifreleme anahtarı bilinen başka bir sistem tarafından şifre çözme algoritması kullanılarak şifrelenme öncesi haline çevrilmektedir.



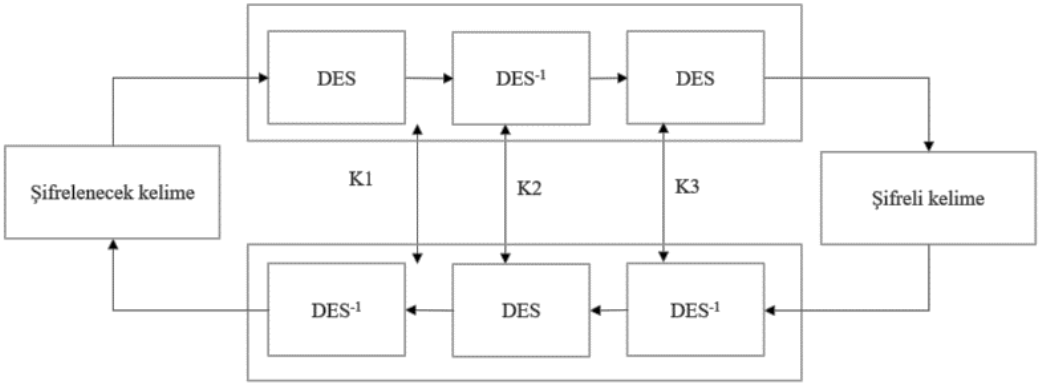
Şekil 6. Simetrik şifreleme sistemi

Bu yöntem ile basit anlamda şifrelenen verinin farklı sistemler arasında transferi aşamasında ele geçirilmesinde anahtar bilgisine sahip olmayan sistem veya kötü niyetli kullanıcı tarafından anlamlı hale getirilmesi engellenmiştir.

DES algoritması finans ve bankacılık sektöründe aktif olarak kullanılmıştır, kart işlemleri, elektronik ödeme işlemleri ve finansal bilgi güvenliğinin artırılmasında fayda sağlamıştır. Ağ seviyesinden bakıldığında ise iletişimde verilerin şifrelenmesi sürecinde kullanılmıştır. Aynı zamanda günümüz modern tarayıcılarında sıklıkla karşımıza çıkan SSL ve TLS gibi iletişim protokollerinin içerisinde kullanılan algoritmalardan birisidir.

2.2.2 3DES

Triple DES olarak adlandırılan bu şifreleme algoritması Ulusal Standartlar Bürosu (NBS) tarafından 1977 yılında kabul gören DES 1994 yılında FIPS (Federal Bilgi İşleme Standartları Yayını) tarafından son hali ile yeniden onayladı. Triple DES ise 3 kez DES algoritmasının uygulanması yöntemini baz alacak şekilde düzenlenmiştir. Burada şifreleme-şifre çözme-şifreleme (EDE) yöntemi her bir DES uygulaması sırasında farklı anahtarlar kullanılacak şekilde kurgulanmıştır (Kitsos, Goudevenos ve Koufopavlou, 2003). DES algoritmasının açıkları temel alınarak çift taraflı çalışan 3DES algoritması ortaya çıkmıştır. K1, K2 ve K3 olarak adlandırılan anahtarlar sırasıyla metnin DES şifrelemesi, şifre çözme ve tekrar şifreleme için kullanılır. Belirtilen bu anahtarlar aynı olabilir. Bu durumda basit DES algoritması olarak değerlendirilir (Yao-Hua, 2014). DES şifreleme algoritmasının süreçleri birebir 3 kez uygulanarak oluşturulan bu şifreleme yöntemine ait akışa Şekil 7'de yer verilmiştir.



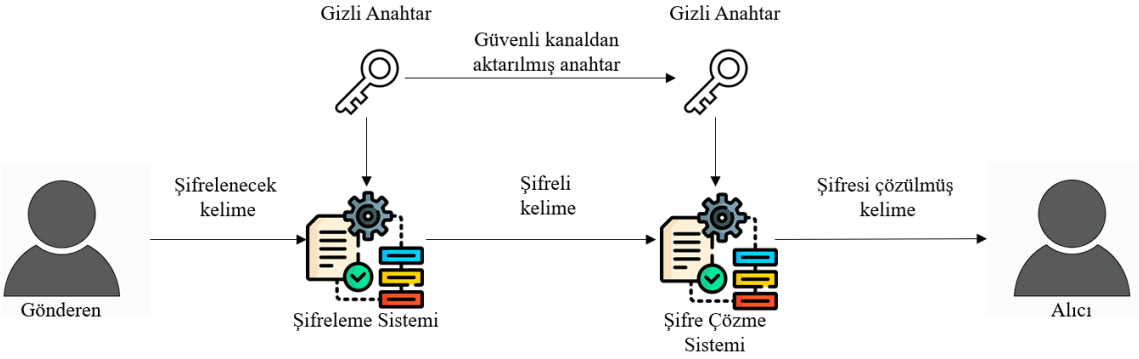
Şekil 7. 3DES şifreleme/şifre çözme uygulaması diyagramı

Şifrelenmiş verinin tekrar tekrar şifrelenmesi ile güvenilirliği daha da artırılmıştır. Anahtar bilgisini de ele geçiren kötü niyetli kişi veya sistem, DES şifreleme

algoritmasında olduğu gibi tek seferde uygulayacağı şifre çözme süreci ile gerçek veriye ulaşamayacaktır. Bu sayede şifrelenmiş verinin robotik sistemler tarafından çözülebilmesi daha da zorlaşmış olacaktır.

2.2.3 AES

DES algoritmasının zafiyet durumlarının artması ve güncel teknolojide yetersiz kalması nedeni ile farklı anahtar uzunluklarını destekleyecek yapıca simetrik blok şifreleme yöntemine dayalı "Gelişmiş Şifreleme Standardı (AES)" olarak duyurulmuştur. Şekil 8'de şifre paylaşımı yönteminin ve genel şifreleme sürecinin akışına yer verilmiştir.



Şekil 8. AES Algoritması Çalışma Prensibi

AES algoritması genel olarak elektronik ortamda oldukça uzun bir süre kullanılan DES algoritmasının yerini almayı hedeflemiştir. Yapılan duyuru sonrasında sunulan farklı algoritmalardan 2000 yılında Rijndale algoritması seçilip AES olarak adlandırılmıştır (Utami, Arifudin ve Alamsyah, 2020).

Kişisel verilerin şifrelenerek saklandığı uygulamaların birçoğunda AES şifreleme yöntemi kullanılmıştır. Yapılan literatür araştırmasında bunun sebebi olarak farklı anahtar uzunlukları kullanılması, saldırılara karşı dirençli olması gibi detayları örnek olarak gösterilmiş ve endüstri standardı olarak kabul edilmiştir ve bu sebeple günümüzde askeri ve devlet uygulamalarında aktif olarak kullanıldığı görülmektedir.

2.2.4 RC algoritmaları

RC algoritmaları Ron Rivest tarafından geliştirilmiş simetrik anahtar şifreleme algoritmalarıdır. Birkaç versiyondan (RC1, RC2, RC3, RC4, RC5, RC6) oluşan algoritmalar her versiyonda bir önceki algoritmada yaşanan performans sorunlarını ve

dönemin popüler güvenlik açıklarını kapatmak üzere çalışmalar yapılarak geliştirilmiştir (Padmavathi, Sirisha ve Lakshman, 2014). Tablo 4'te RC algoritmaları ile ilgili kronolojik bilgiye yer verilmiştir.

Tablo 4. RC algoritmasının versiyonları

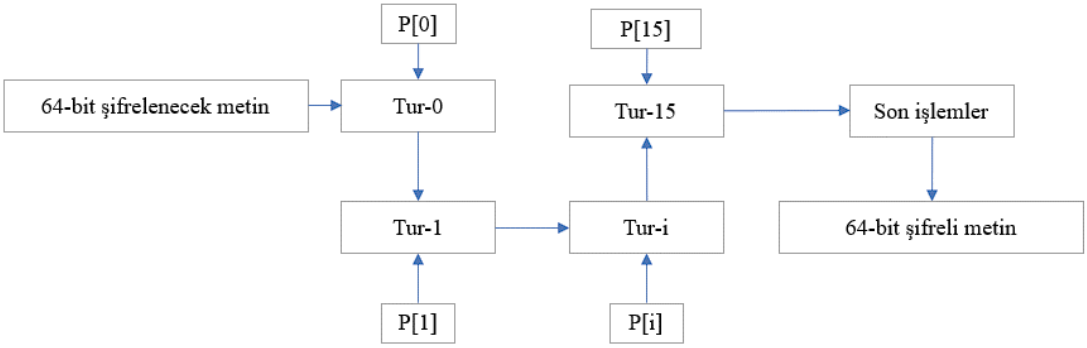
RC1	Hiç yayınlanmadı
RC2	1987 yılında 64bit'lik blok şifreleme ile yayınlandı
RC3	Kullanıma başlamadan kırıldı
RC4	Dünya çapında en çok kullanılan akış şifreleme algoritması
RC5	1994 yılında geliştirildi ve 32/64/128 bitlik blok şifreleme yöntemlerini destekledi
RC6	1997 yılında RC5 baz alınarak 128 bitlik blok şifreleme yöntemi ile geliştirildi. AES finalist algoritmalarından birisidir.

RC4 algoritması, kablosuz ağların şifrelemesinde IEEE 802.11 standartlarına göre kullanılmaktadır. Kablosuz ağlardaki WEP şifreleme türünün altyapısını oluşturmaktadır (Hossain, Hossain, Uddin ve Imtiaz, 2016). WEP şifreleme türü her ne kadar güncelliğini yitirmiş bir kablosuz ağ şifrelemesi de olsa, günümüzde hala sadece bu şifreleme türünü destekleyen kablosuz bağlantıya sahip cihazlar bulunmaktadır. Bu sebeple RC4 algoritması aktif olarak hayatımızda yer almaktadır. Bu çalışmada yapılacak şifreleme testlerinde kullanılacak olan sürüm yine RC4 olarak seçilmiştir.

2.2.5 Blowfish

Blowfish algoritması Feistel fonksiyonu kullanan bir blok şifreleme algoritmasıdır. Yazılış amacı ise DES'in yerini almak ve diğer algoritmaların ortaya çıkarttığı sorunları çözmek olmuştur. Genel olarak mevcut şifreleme işlemlerini 16 kez tekrar ederek kuvvetli bir şifreleme yapısı oluşturmaktadır ve sahip olduğu karmaşık anahtar yapısı bu durumu ayrıca desteklemektedir (Kumar, Saha ve Rai, 2012). Diğer algoritmalarda olan

sorunları çözüp daha esnek bir algoritmaya sahip olmak amaçlanmıştır (Cody, Madigan, MacDonald ve Hsu, 2007). Cody ve arkadaşlarının yaptığı çalışmada yer alan Blowfish algoritmasının akışına Şekil 9'da yer verilmiştir.



Şekil 9. Blowfish Algoritması (Cody, Madigan, MacDonald ve Hsu, 2007)

Feistel fonksiyonun kullanıldığı turlar 16 kez tekrarlanarak şifreleme işlemi gerçekleştirilmektedir. Bu çalışmada testler sırasında kullanılacak algoritmalar arasında Blowfish algoritması değerlendirmeye alınacaktır. Böylece farklı prensiplere sahip algoritmalar ile bulut uygulama ortamında kullanılacak verilerin şifrelenmesinde performans değerlendirmesi yapılabilecektir.

2.3 Kişisel Verilerin Maskelenmesi

Verilerin maskelenmesi kişisel verilerin gizliliğinin korunması adına oldukça önemli bir yere sahiptir. Maskeleme sırasında kişisel nitelikte olan verilerin anonimleştirilerek asıl kimliğinin saklanmasına yardımcı olur. Böylece gerçek kişiye ulaşılmayı sağlayacak verinin kötü kullanıma maruz kalmasının önüne geçilmiş olur.

İletişim ve finans alanında birçok maskeleme çalışması yapılmıştır. Yapılan çalışmaların temelindeki tasarım süreci hemen hemen aynıdır. Giderek artan ve karmaşıklaşan verinin güvenlik nedeniyle işlenme gereksinimi hızlıca artmaktadır (Wang, Wu, Chen ve Li, 2022). Artan bu gereksinimleri karşılamak için farklı modeller sunulmuştur.

2.3.1 K-Anonimlik modeli

Şahısların veriler okunarak tespit edilmesini engelleyen bir yaklaşımdır. Modelin adında bulunan k parametresi kayıt sayısını temsil eder. Veri üzerinde yapılacak çalışmalarda

şahıs verisini tanınmaz hale getirerek mahremiyeti korumaya yardımcı olur. Teknik olarak bakıldığında gruplama sonucunda k-1 kayıt bulunması gerekir ve bu gruba göre bakıldığında doğrudan kişiye özel bir bilgiye ulaşılamamaktadır. Genel amaç anonimleştirme yapıldıktan sonra verinin hala yapılacak çalışma açısından fayda sağlayabilecek nitelikte kalmasıdır. Ancak burada dengeli bir yaklaşım gözetmek gerekir. Anonimleştirme ve sağlanacak faydayı koruyabilmek adına iyi bir denge kurulmasına ihtiyaç vardır. Burada kümeleme ile anonimleştirme yapılarak denge sağlamak sınırları daha net çizmektedir (Loukides ve Shao, 2008). Bu çalışmada kullanılan verinin detayları Tablo 5 ve Tablo 6'da belirtilmiştir.

Tablo 5. Orijinal Veri (Loukides ve Shao, 2008)

Yaş	**Posta Kodu**	**Tanı**
30	NW10	HIV
32	NW15	HIV
37	NW12	HIV
40	NW13	HIV
45	NW20	Nezle
46	NW30	Soğuk Algınlığı
57	NW30	Soğuk Algınlığı
60	NW25	Öksürük

Tablo 6. Tablo 5'in Anonimleştirilmiş Hali (Loukides ve Shao, 2008)

Yaş	**Posta Kodu**	**Tanı**
[30~46]	{NW10~30}	HIV
[30~46]	{NW10~30}	HIV
[30~46]	{NW10~30}	Nezle

[30~46]	{NW10~30}	Soğuk Algınlığı
[37~60]	{NW12~30}	HIV
[37~60]	{NW12~30}	HIV
[37~60]	{NW12~30}	Soğuk Algınlığı
[37~60]	{NW12~30}	Öksürük

Yukarıdaki tablolarda anlaşılacağı üzere Tablo-5'te açık bir şekilde erişilebilen kayıtlar kümeleme yöntemi ile birleştirilerek Tablo-6'da olduğu gibi doğrudan veriye erişimi kısıtlamıştır.

2.3.2 L-Çeşitlilik modeli

K-Anonimlik modelinin çeşitliliği garanti edememesi üzerine anonimleştirmeden sonra etkin saldırılarla verinin açığa çıkması riskine karşılık L-Çeşitlilik modeli önerilmiştir.

Bu modelin arkasındaki temel düşünce hassas olarak değerlendirilen verilerin modellenmiş her grupta en iyi şekilde temsil edilmesi gerekliliğini savunur. Böylece yayıncı tarafından, bilgiye ulaşmış kişilerin elinde ne olduğunu bilmeden gizliliği sağlamış olur (Machanavajjhala, Gehrke, Kifer ve Venkitasubramaniam, 2006). Yapılan bu çalışmada kullanılan verilere Tablo 7'de yer verilmiştir.

Tablo 7. Orijinal Maaş/Hastalık tablosu (Machanavajjhala, Gehrke, Kifer ve Venkitasubramaniam, 2006)

No	**Posta Kodu**	**Yaş**	**Maaş**	**Hastalık**
1	47677	29	3000	Mide ülseri
2	47602	22	4000	Gastrit
3	47678	27	5000	Mide kanseri
4	47905	43	6000	Gastrit
5	47909	52	11000	Nezle

6	47906	47	8000	Bronşit
7	47605	30	7000	Bronşit
8	47673	36	9000	Zatürre
9	47607	32	10000	Mide Kanseri

Tablolarda belirtilen verilere bakıldığında maaş ve hastalık bilgisi hassas veri olarak kabul edilebilir. Buradan yola çıkarak açık bir şekilde verilerin gösterildiği tabloda, hastalık bilgisine ve yaş bilgisine sahip olan bir kişi, kişinin doğrudan maaşını bilebilir. Tablo 7'de orijinali verilen ve üçlü gruplama ile Tablo 8'de maskelenen verilerin detayına yer verilmiştir.

Tablo 8. Tablo 7'nin l-çeşitlilik modeli ile maskelenmiş hali (Machanavajjhala, Gehrke, Kifer ve Venkitasubramaniam, 2006)

No	**Posta Kodu**	**Yaş**	**Maaş**	**Hastalık**
1	476**	2*	3000	Mide ülseri
2			4000	Gastrit
3			5000	Mide kanseri
4	479**	≥ 40	6000	Gastrit
5			11000	Nezle
6			8000	Bronşit
7	476**	3*	7000	Bronşit
8			9000	Zatürre
9			10000	Mide Kanseri

Tablo 8'de yapılan anonimleştirme çalışması sonucunda ise, posta kodu ve yaş bilgilerince birinci grupta yer alan kişinin maaşının bilinmesi sonucunda hastalığı ile ilgili hassas veriye ulaşılabilir (Li, Li ve Venkatasubramanian, 2006). Kısaca aynı çeşitlilik seviyesindeki gruplamalar farklı gizlilik seviyeleri sağlayabilir. Değer olarak veriler arasında anlamsal ilişki bulunması verinin gizliliğini olumsuz anlamda etkileyebilir.

2.3.3 T-Yakınlık modeli

L-Çeşitlilik modelinin yetersiz olmasını konu alarak önerilen bir modeldir. Paylaşılan veri tablosunun t-yakınlık modeline uygun olabilmesi için tabloda bulunan bütün verilerin t-yakınlık ihtiyaçlarını tamamen karşılar nitelikte olmalıdır. Veriye sahip olan kişi değerlerin nasıl dağıtıldığını bilse dahi kategorize edilmiş veriler hakkında kısıtlı bilgi edinmiş kabul edilir (Vural, 2017). Tablo 9'da Li ve arkadaşlarının yaptığı yakınlık modeli ile maskeleme sonucuna yer verilmiştir.

Tablo 9. Tablo 7'nin yakınlık modeli uygulanmış hali (Machanavajjhala, Gehrke, Kifer, ve Venkitasubramaniam, 2006)

	Posta Kodu	Yaş	Maaş	Hastalık
1	4767*	≤ 40	3000	Mide ülseri
2			5000	Mide kanseri
3			9000	Zatürre
4	4790*	≥ 40	6000	Gastrit
5			11000	Nezle
6			8000	Bronşit
7	4760*	≤ 40	4000	Gastrit
8			7000	Bronşit
9			10000	Mide Kanseri

Tablo 9'da maaş ve hastalık bilgilerini anonimleştirebilmek için posta kodu ve yaş bilgilerinde yakınlığa göre gruplama yapılarak çalışma gerçekleştirilmiştir. Böylece yaş ve posta kodu bilgisine göre hastalığı bilinen bir kişinin maaş bilgisine ulaşılması zorlaşmıştır.

2.4 Mevzuat Değerlendirme

Teknolojinin hızla gelişmesi ve depolama maliyetlerinin önemli ölçüde düşmesi ile oldukça büyük miktarlarda veri saklanabilmektedir. Oluşan bu verilerin bir kısmı kişisel nitelikte bilgi barındırılarak depolanmaktadır. Açık veya açıkça ulaşılabilir gerçek bir kişiye ait bilgilerin tamamı "kişisel veri" olarak tanımlanmaktadır. Enformasyona dayalı büyük verilerin paylaşıldığı günümüzde verinin korunması, saklanması ve erişilmesi kritik öneme sahiptir (Şahinaslan ve Şahinaslan, 2022) . Bu verilerin korunmasına dair kabul gören ilk uluslararası belge 28 Ocak 1981 tarihinde kabul edilmiştir (Özdiker, 2018). Zaman içerisinde teknolojinin gelişmesi ve saklanan kişisel nitelikteki verilerin artması sürecinde veri mahremiyetini kısıtlayabilmek adına Türkiye'de "Kişisel Verileri Koruma Kurumu (KVKK)" ve Avrupa'da "Genel Veri Koruma Kısıtları (GDPR)" ortaya çıkmıştır. Bu yönetmelikler ile kişisel nitelikli veriyi yöneten servis sağlayıcılara daha sıkı kurallar getirilip elde edilen kişisel verinin kullanımının kontrol altına alınması hedeflenmiştir (Yalçınkaya ve Diri, 2022). Her iki mevzuatın getirdiği ayrıca yönetim yükümlülüğü bulunmaktadır. Verinin gerçek sahibinin kendine ait bilgi üzerinde tam anlamlı erişim ve kontrol hakkı olmalıdır. Böylece gerçek verinin sahibi kolayca görüntüleme, değiştirme ve silme yetkileri ile kendi verisini yönetebilmektedir. Bunun gibi örneklere abonelik, tercih yönetimi gibi internet sayfalarında rastlayabiliyoruz. Yönetmelik gereğince firmalar tarafından kullanıcılara gönderilen elektronik postalarda bülten aboneliklerinden çıkma fırsatı tanınabiliyor ve bununla beraber kişilerin kendi bilgilerini (ad, soyad, telefon, e-posta), abone olmak istediği kategorileri yönetme fırsatı sunuluyor.

Veri miktarının önemli ölçüde büyüdüğü bir alan olan sağlık sektörü oluşturduğu çıktılar ile birçok alanda üzerinde çalışma yapılabilecek nitelikte veri kümesi oluşturmaktadır. Bu çalışmalarda kullanılacak verilerin herkes tarafından erişime açık bir şekilde yayınlanması kişisel bilgi güvenliğini, veri mahremiyetini zedeleyecektir. Bu sebeple sağlık sektöründe ABD tarafından korunan sağlık bilgilerinin (PHI) kullanımı ve

dağıtılmasını kısıtlamak için HIPAA kabul edilmiştir (Shuaib, Alam, Alam ve Nasir, 2021). Bu kabul ile hastaların tıbbi bilgilerinin paylaşımı gerekli güvenlik önlemleri altında gerçekleşip sadece yetkili kişilerle paylaşılması garanti altına alınmaya çalışılmıştır. Dünya çapında veri mahremiyetine yönelik yapılan düzenlemelerin detayına Tablo 10'da yer verilmiştir.

Tablo 10. Kişisel Verilerin Korunmasıyla İlgili Uluslararası Genel Düzenlemeler

Düzenleme	**Tarih**
İnsan Hakları Evrensel Beyannamesi	1948
Avrupa İnsan Hakları Sözleşmesi	1950
OECD Rehber İlkeleri	1980
Avrupa Konseyi 108 sayılı Sözleşme	1981
BM Genel Kurulu Rehber İlkeler	1990
AB Veri Koruma Direktifi	1998
GDPR	2018

Tabloda yer verilen tarihlerden anlaşıldığı üzere, bulut sistemler hayatımıza 2000'li yıllardan sonra girdi ancak oluşturabileceği güvenlik zafiyeti ile ilgili önlemler çok daha eskiye dayanmaktadır. Buradan yola çıkarak, bir kez daha dünya çapında kişisel bilgilerin önemine vurgu yapıldığını görebiliyoruz.

2.4.1 Kişisel verilerin korunması kanunu

Teknolojinin gelişmesi, kullanımının yaygınlaşması ve internetin cihaz seviyesinde elimize ulaşması ile ciddi anlamda veri birikimi ortaya çıkmaktadır (Savaş, Zaim ve Aydın, 2020). Bu verilerin kurum ve kuruluşlar tarafından depolanması yine onlar adına işlenecek, kullanılacak ve hatta son kullanıcıya karşı davranış analizi yapılıp ürün-hizmet satmaya yönelecek türde çalışmalar yapılabilmesinin önünü açmıştır. Bu çalışmaların temelinde yatan verinin kişisel olması ciddi anlamda güvenlik ve mahremiyet ihtiyacını doğurmaktadır. Bu bağlamda ülkemizde de mahremiyeti sağlayabilmek adına hukuki ve teknik anlamda çalışmalar yapılmaya başlanıp çeşitli yönetmelikler hazırlanmıştır. 7 Nisan 2016 tarihinde 6698 numaralı kanun ile yürürlüğe giren "Kişisel Verilerin Korunması Kanunu" kişisel verilerin işlenirken özel hayatın gizliliğini, kişisel temel hak ve özgürlüklerin korunmasını ve bu kişisel verilerin işleyen işletmelerin uymaları gereken

yükümlülükleri düzenlemektedir. Mevzuatta kişisel verinin tanımı açık bir şekilde "Kimliği belirli veya belirlenebilecek gerçek kişiyse ait tüm bilgi" olarak yer almaktadır. Kişisel veri olarak nitelendirilen bilgilerin içeriği kanunda ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep, sivil toplum kuruluşu üyeliği, sağlık durumu, cinsel hayatı, sicil kaydı ve biyometrik-genetik bilgileri özel nitelikli kişisel veri olarak gruplanmıştır (KVKK, 2016). Bu verilerin işlenmesi ile ilgili şartlarda farklı kısıtlar yine kanun ile belirlenmiş olup çeşitli istisnaların uygulandığı açıkça görülebilir. KVKK'ya uyum konusunda yükümlülüklerin yerine getirilmesi gelecekte yaşanabilecek zorluklarla başa çıkma sürecinde kuvvetli bir temel oluşturmaktadır. Böylece işletmeler bilginin korunması ve güvenliği açısından her geçen gün daha güçlü bir durumda olacaktır. Şekil 10'da kişisel olarak tanımlanan bilgilerin bir kısmına yer verilmiştir.



Şekil 10. Kişisel bilgi olarak kabul edilen bilgiler (KVKK, 2016)

Kanunda yer alan tanımlara göre kişisel verinin açık rıza olmadan yurt dışına aktarılması kısıtlanmış olup işleyen kurumların bireylerden doğrudan açık rıza alarak verileri yurt dışında saklayabileceği belirtilmiştir. Ancak bu verilerin yurt dışında saklanabilmesi için yeterli korumanın bulunması veya bulunmaması durumunda korumanın yeterli bir şekilde taahhüt edilip kurul izninin bulunması şartı aranmaktadır.

Ülkemizde KVKK ile ilgili ilk olarak 28.01.1981'de "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme" imzalanmıştır (Ertekin, 2022). Kişisel verilerin korunmasına yönelik alınacak önlemler sadece bunun gibi genel başlıklar halinde imzalanan sözleşmeler ve yasa maddeleriyle değil, sektörel bazda yayınlanan düzenlemelerle de kontrol altına alınmaya çalışılmıştır. Türk Ticaret Kanunu'nda 2. Kısım 24. Maddede toplanan verilerin kişisel verilerin korunmasına ilişkin mevzuata uygun olarak yapılması gerektiği belirtilmiştir. Yine aynı şekilde Elektronik Haberleşme Kanunu'nda 2. Bölüm 6. Maddede yer alan tanıma göre kurum görev ve yetkileri ile ilgili tanımlarda toplanan verilerin mevzuata uygun bir şekilde korunması gerektiğine değinilmiştir.

2.4.2 Genel veri koruma kısıtları (GDPR)

Temel amacı Avrupa Birliği vatandaşlarının kişisel bilgilerini koruma altına almak için hazırlanan bu yönetmelik 25 Mayıs 2018 tarihinde Avrupa Birliği'ne üye tüm ülkelerde yürürlüğe girerek yönetmelikte yer alan kısıtların bu ülkelerde yer alan büyük işletmelerin sahip oldukları kişisel bilgiyi güvence altına almaktadır. GDPR'ın temeli 1950 yılların başına dayanmaktadır. Süreç 1950 yılında "Avrupa İnsan Hakları Sözleşmesi" ile başlamıştır. Devamında gizliliğin öneminin arttığı görülüp yeni kısıtlar getirilmiştir. 1981 yılında ise oldukça geniş kapsamlı bir sözleşme imzalanarak Avrupa Birliği ülkelerinin sözleşme içeriğinin ülke hukukuna katılması zorunluluğu getirilmiştir. Veri korunmasındaki en büyük gelişme 1995 yılında hazırlanıp 1998 yılında yürürlüğe giren "Avrupa Birliği Veri Koruma Direktifi" ile Avrupa birliğine üye bütün ülkelerde geçerli olacak temel kanunlar belirlenip koruma mevzuatına uygun olmayan ülkelere veri çıkışı yasaklanmıştır (Paşaoğlu ve Vural, 2018). Bu yasak verilerin akışının korunma altına alınması açısından önemli bir adım olup hassas verilerin yetkisiz kişilerce erişilmesinin önüne geçilmesini sağlanmıştır.

Mevcutta var olan düzenlemelerin farklı Avrupa Birliği ülkelerinin kanunlarda farklı şekilde yer alması ve teknolojinin hızla ilerlemesi sebebiyle daha sıkı önlemlerin alınması gerektiğine karar verilip hazırlanan "Genel Veri Koruma kısıtları" AB Veri Koruma Direktifini kaldırıp yerine geçmiştir (Paşaoğlu ve Cevheroğlu, 2020). Böylece GDPR Avrupa Birliği ülkelerinde geçerli hale gelmiştir.

2.4.3 HIPAA

Sağlık sektöründe teknolojinin gelişmesiyle birlikte kişisel nitelik taşıyan veri anlamında en çok veri depolayan sektördür. Bu nedenle burada ihtiyaç duyulan kısıtlar daha büyük önem taşımakta. Bireylerin isim, yaş, sağlık durumu, adresi, telefon numarası gibi kişisel nitelikte olan bilgilerin bir arada bulunması ve açık bir şekilde paylaşılıyor olması kişisel veri mahremiyetini ihlal etmektedir. Akademik çalışmalara konu olan bu veriler doğrudan açık bir şekilde paylaşılıp gizliliğin ihlal edildiği durumlarda bireylerin zarar görmemesi için genel anlamda bir kısıtlamaya ihtiyaç duyulmuştur. "Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası (HIPAA)"; sağlık kuruluşlarının bireylerin sağlık bilgilerini açık bir şekilde paylaşılmasını ve bu verilerin izinsiz bir şekilde kullanılmasını engellemek için yükümlülükler getirmiştir. Aynı zamanda HIPAA tarafından getirilen güvenlik standartları arasında bu bilgiye erişimin denetlenmesi ve erişimlerin kayıt altına alınmasını yükümlülük haline getiren oldukça katı kurallara sahiptir (Zhou ve Liu, 2005).

1996 yılında yayınlanan HIPAA 2003 yılında resmi olarak yürürlüğe girerek sağlık hizmeti veren kuruluşların Nisan 2005'e kadar HIPAA uyumlu hale gelmelerini zorunlu hale getirmiştir. Burada genel amaç diğer kısıtlamalarda olduğu gibi sağlık sektöründe de verilerin mahremiyetini korumak ve güvenliğini sağlamak adına standartları belirleyip uygulanmasını sağlamaktır.

HIPAA tarafından standart haline gelmiş denetim sürecinin aşağıdaki şartları sağlanması gerekmektedir (Cao, Huang ve Zhou, 2003).

- Verilere erişen kişinin kimliği
- Erişilen bilgilinin kayıt altına alınması
- Verinin erişildiği konum
- Veriye erişim zamanı (tarih ve saat olarak)
- Erişim tipi (oluşturma, görüntüleme, silme, güncelleme)
- Erişim durumu (başarılı veya başarısız olması durumu)

Belirtilen şartların sağlanmaması durumda oluşacak ihlallerde para cezası, uygunluk soruşturması, itibar kaybı, hukuki sorunlar ve iş sürekliliği sorunları gibi yaptırımlar ortaya çıkabilir.

2.5 Bulut Sistemlerde Veri Mahremiyeti

Bulut sistemler birçok kullanıcı ve kurum tarafından oldukça yaygın bir şekilde kullanılmaktadır. Popülerliğinin hızlı bir şekilde artmasının en büyük nedeni herhangi bir cihazdan hızlıca erişilebilir ve altyapı maliyetlerinin fiziksel sistemlere göre oldukça uygun olmasıdır. Bu esneklik ve uygun maliyet sonucunda ortaya veri gizliliği ile ilgili çeşitli sorunlar çıkabilmektedir. Günümüz sanal ortamında mahremiyet hakkı da siber tehdit altındadır (Şahinaslan, 2013). Bulut sistemlerde saklanan veriler sistemin yapısına göre birçok sunucuda saklanabilir, yetkisiz kişilerce erişime açık olabilir. Bulut sistemler bu tarz sorunlarla karşılaşmamak adına altyapılarında ciddi önlemler alıp çeşitli güvenlik kuruluşlarınca uygun standartlarla denetime tabi tutulmaktadır.

Fiziksel ihlal haricinde sistemsel ihlallerde söz konusudur. Burada ihlal durumu kullanılan bulut sistemin uygulanma yöntemine bağlı olarak değişiklik gösterebilir. Şekil 11'de verilerin korunmasına yönelik önerilen güvenlik ve gizlilik tedbirleri ile ilgili detaylı şemaya yer verilmiştir.



Şekil 11. Güvenlik ve Gizlilik Ayrımı

Sistemlerde rol, hiyerarşi, bölge gibi yapılara göre veri gizliliği konumlandırılıp yetkisiz kişilerin veriye erişimi engellenebilir. Ancak burada ülkelerde yer alan veri koruma kanunlarına göre sistemlerin tamamında karşılanamayan durumlar oluşmaktadır. Verilerin bulut sistemlerde şifreli olarak yer alması, bulut veri tabanından getirilen bilgilerin uygun çözücülerle veriyi görüntüleyecek kişinin yetki seviyesine göre

görüntülenmesinin sağlanması gerekmektedir. Sistemler tarafından bu işlemler genel olarak dünyaca bilinen GDPR, HIPAA gibi kısıtlamalara göre PII (Kişisel tanımlanabilir bilgiler) olarak nitelendirilen alanlar özelinde uygulanmaktadır. Ülkemiz açısından baktığımızda uluslararası ölçekte kullanılan bulut sistemlerde KVKK ile ilgili doğrudan bir önlem bulunmamaktadır.

3. YÖNTEM

Bu bölümde bulut sistemler literatürde yapılan çalışmalara dayanarak detaylı bir şekilde değerlendirilecektir. Ayrıca bulut sistem sağlayıcıları hakkında karşılaştırmalı bilgilendirme yapılıp, uygulama sürecinde buradan çıkan sonuca göre uygun bir çalışma ortamı seçimi yapılacaktır.

Bulut sistemlerin son kullanıcılar tarafından tercih edilmesinde önem kazanan güvenlik sertifikaları süreci yine bu bölümde detaylandırılıp içerikleri bakımından bulut sistemler üzerindeki faydalarına değinilecektir.

Bu bölümde yapılan çalışmalardan sonra, burada belirtilen standartlar çerçevesinde bir sonraki bölüm olan uygulamada çalışmanın detaylarına değinilecektir. Bu çalışma içerisinde yapılan literatür araştırmalarından elde edilen bilgilere dayanarak, verinin yerel ortamda güvenli bir şekilde saklanmasını sağlamak için bir altyapı oluşturulacak, çalışmada yer verilen yöntemler kullanılarak verinin güvenli bir şekilde saklanması sağlanacaktır.

3.1 Bulut Sistem Sağlayıcıları

Günümüzde kurumların ileri seviyede iş yapma süreçlerine yardımcı olacak bulut tabanında çalışabilen birçok çözüm bulunmaktadır. Kurumlar açısından bakılacak olduğunda bu altyapılara sahip olunmadığında müşteri ile ilişkiyi yönetmek oldukça imkânsız hale gelecektir. Kurum bünyesinde bulundurulan bir CRM sistemi kurulumu beraberinde lisans, bakım, ölçeklendirme ve sürdürülebilirlik gibi ekstra ciddi maliyetler oluşturacağından bulut sistemlerin tercih edilmesi her geçen gün daha da artmaktadır (Petkovic, 2010). Özellikle bakım ve sürdürülebilirlik açısından işletmelerce tercih edilme sebebi olmaktadır.

Yapısal özellikler olarak SaaS modelinde hizmet veren sağlayıcıların CRM ürünleri Tablo 11'de belirtilmiştir. Buna göre Dynamics ve Maximizer sağlayıcılarının sunduğu hizmetler hem bulutta hem de yerel ortamda çalışabilmektedir.

Tablo 11. Hizmet Sağlayıcı Karşılaştırması (Souri, Asghari ve Rezaei, 2017)

SN	Sağlayıcı	Ortam	Kategori	Ölçek	Fiyatlama	Mobil Uyumluluk
1	Salesforce	Bulut	Büyük İşletme	K/O/B	Yüksek Maliyet	iOS / Android / Windows
2	Oracle	Bulut	Büyük İşletme	K/O/B	Yüksek Maliyet	iOS / Android / Windows
3	Netsuite	Bulut	Büyük İşletme	K/O	Yüksek Maliyet	iOS / Android / Windows
4	Microsoft Dynamics	Yerel / Bulut	Büyük İşletme	K/O/B	Yüksek Maliyet	iOS / Android / Windows
5	Infusionsoft	Bulut	Kobi	K	Ortalama	iOS / Android
6	Hub Spot	Bulut	Kobi	K/O	Ortalama	iOS / Android
7	Sugar	Bulut	Kobi	K/O/B	Ortalama	iOS / Android / Windows
8	Zoho	Bulut	Kobi	K/O/B	Düşük Maliyet	iOS / Android / Windows
9	PipelineDeals	Bulut	Kobi	K/O	Düşük Maliyet	iOS / Android
10	Maximizer	Yerel / Bulut	Kobi	K	Düşük Maliyet	iOS / Android

Tablo 11'de yer alan sağlayıcıların kullanıcılar tarafından 1'den 10'a kadar kullanım, kurulum ve destek kalitesi süreçlerine Tablo 12'de yer verilmiştir.

Tablo 12. Sağlayıcıların Kalite Puanlamaları (Souri, Asghari ve Rezaei, 2017)

Sıra	Sağlayıcı	Kullanım Kolaylığı	Kurulum Kolaylığı	Destek Kalitesi
1	Salesforce	9	9.5	8.8
2	Oracle	7.1	6.3	6.9
3	Netsuite	5.7	5.4	6.1
4	Microsoft Dynamics	6.8	6.2	7
5	Infusionsoft	7.5	8.8	6.2
6	Hub Spot	9	8.9	8.9
7	Sugar	7.3	6.8	7.5
8	Zoho	8.9	9.1	8.6
9	PipelineDeals	9	8.9	9.2
10	Maximizer	8.3	7.8	8.5

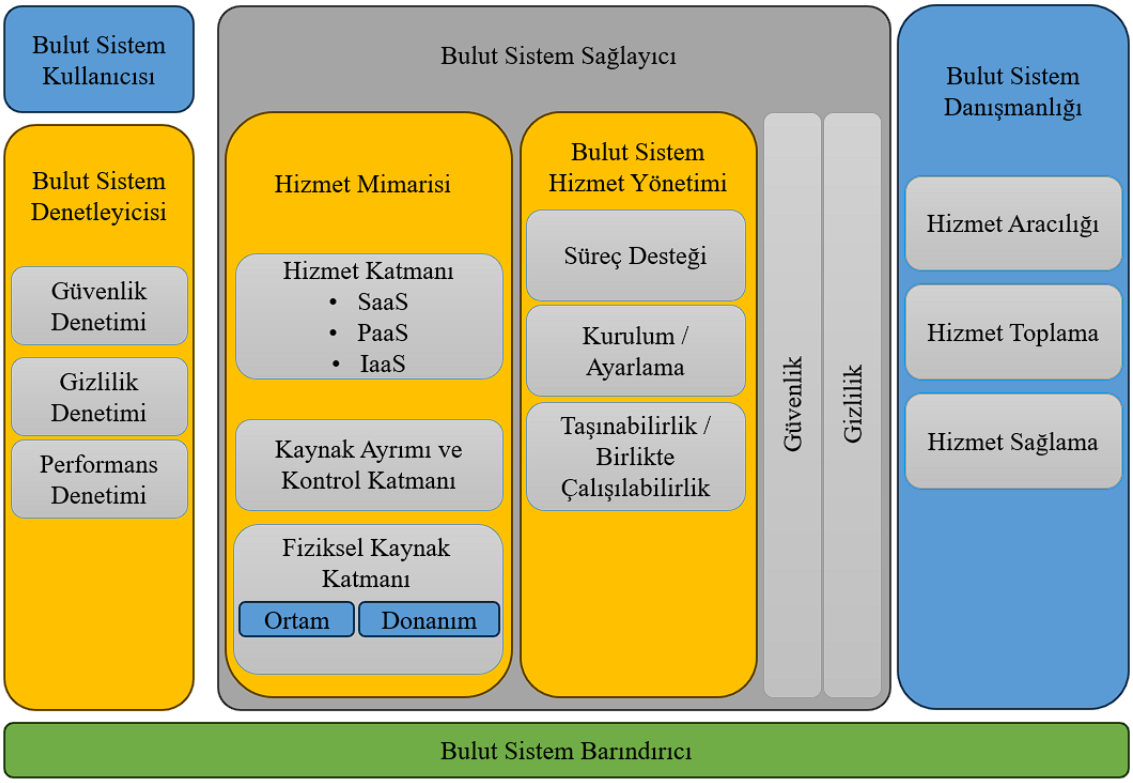
Tablo 12'de yer verilen puanlamaya göre Souri ve arkadaşlarının yapmış olduğu bu çalışmada Salesforce'un yüksek puan aldığı gözükmektedir (Souri, Asghari ve Rezaei, 2017).

Uygulama bölümünde CRM pazarında lider olarak adlandırılan ve üst düzey seviyede kullanılırlığı ile bilinen Microsoft Dynamics, Oracle CRM, Salesforce ve SAP uygulamaları üzerinde kolaylıkla entegre edilebilecek bir yapı hazırlanacaktır.

Geliştirme ortamı seçiminde karşılaştırılan sistemler arasında kullanıcı dostu yaklaşım göz önünde bulundurularak herhangi bir lisans maliyeti olmadan, hızlıca demo ortamı oluşturulabilme özelliği olması sebebiyle Salesforce platformu seçilmiştir.

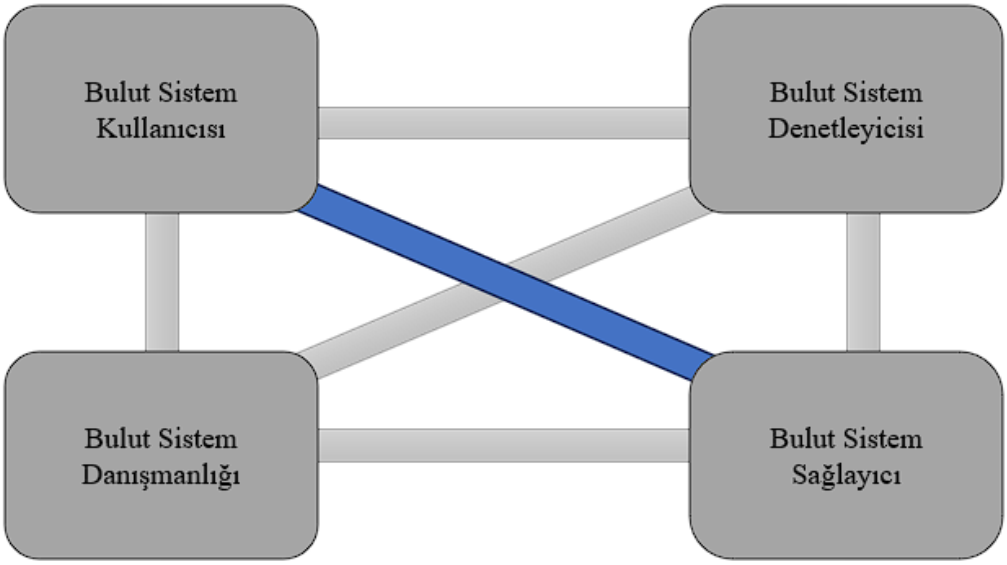
3.2 Bulut Sistem Aktörleri

Bu bölümde tez çalışmamızda değindiğimiz bulut sistemleri detaylı bir şekilde inceleyip veri gizliliği ve korunması açısından uygunluklarını ele alacağız. Şekil 12'de NIST tarafından belirtilen bulut sistem aktörleri ve bu aktörlerin hizmet alanları detaylı bir şekilde paylaşılmıştır (Liu, ve diğerleri, 2011)



Şekil 12. NIST bulut mimari aktörleri ve katmanları (Liu ve diğerleri, 2011)

Şekil 12'de belirtildiği üzere NIST'e göre tanımlanan aktörlerin her birisi bulut bilişim mimarisinde işlem veya süreçlere katkı sağlayan kişi ve kuruluşları temsil etmektedir ve yapılan bu modelleme ile devlet seviyesindeki bilgi teknolojileri uzmanlarına daha iyi bir anlatım sağlanması amaçlanmıştır (Bohn ve Messina, 2011). Şekilde belirtilen referans mimaride 5 ana aktör yer almaktadır. Her aktör bir kişi veya bir organizasyon olabilir.



Şekil 13. Bulut Sistemlerde Aktörler Arasındaki ilişki (Liu ve diğerleri, 2011)

Bu bölümde yer alan referans mimariye göre ve Şekil 13'te belirtilen şemaya göre bulut sistem kullanıcısı doğrudan veya bir danışman aracılığıyla sağlayıcıdan hizmet talebinde bulunabilir. Burada işleyen bütün süreç ise denetleyiciler tarafından ihtiyaç duyulan bilgiler toplanarak incelenir. Referans mimarinin aktörlerinin detayları ile ilgili ayrıntılı bilgiye çalışmanın ilerleyen bölümlerinde yer verilmiştir.

3.2.1 Bulut sistem kullanıcısı

Bulut sistemler üzerinden servis veren sağlayıcılarla kontrat yaparak hizmet alan kurum veya kuruluşları temsil eder. Doğrudan bulut uygulamayı kullanacak kişidir. Bu kişi hizmet sağlayıcılarının ürün yelpazesini inceleyip kendisine uygun hizmeti seçerek sağlayıcı ile hizmet sözleşmesi yapar (Hogan, Liu, Sokol ve Tong, 2011). Bulut sistem kullanıcıları talep edilen sistem detaylarına göre farklılık gösterebilir. Hogan ve arkadaşlarının yaptığı çalışmaya göre kullanıcının hizmet sağlayıcıdan farklı seviyelerde talep ettiği hizmetlere ait içeriklere Tablo 13'te yer verilmiştir.

Tablo 13. Bulut Kullanıcısı ve Hizmet Sağlayıcı ilişkisi (Hogan, Liu, Sokol ve Tong, 2011)

Tip	Kullanıcı İşlemleri	Sağlayıcı İşlemleri
SaaS	Uygulama ve hizmetleri iş süreçlerinin yürütülmesi için kullanımı	Kurulum, yönetim, bakım ve destek gibi süreçleri bulut altyapısında yürütür.
PaaS	Geliştirme, test etme, canlı geçişi ve uygulama yönetiminin bulut ortamda yapılması.	Kullanıcılar için altyapı ve yazılımı tedarik edip yönetir. Geliştirme, geçiş ve yönetim için araçlar temin eder.
IaaS	Yükleme, yönetim ve servislerin izlenmesi.	Fiziksel aktivite, depolama, ağ operasyonları ve uygulamanın barındırılmasını yönetir.

Tablo 13'te hizmet tipine göre kullanıcı ve sağlayıcı arasındaki talep-talebi karşılama ilişkisine yer verilmiştir. Bu aşamada talepte bulunacak kullanıcı sahip olduğu bulut sistemin yeteneklerini, sunabileceklerini sözleşme öncesinde çok iyi bir şekilde incelemeli ve ihtiyaçlarını bu sınırlar çerçevesinde karşılaştırmalıdır.

3.2.2 Bulut sistem sağlayıcısı

Bulut sistem servislerini sağlayan kişi veya kuruluşlardır. Genellikle büyük ölçekli veri merkezine sahip olup bunları hizmet alacaklara sunmak için kullanırlar. Aynı zaman servis sağlayıcılar fiziksel katmanda kaynak yönetimi ve bunların dağıtımından sorumludurlar. Kaynakların dağıtımı ve etkili kullanımını sağlayabilmek için kaynak değişimi, ölçümleme izleme gibi süreçleri işletmeleri gerekmektedir. Böylece sunulan hizmetin sürdürülebilirliğini olası bir altyapı hatası durumunda başka bir ortama taşınarak hizmetin sürekli çalışır durumda kalmasını sağlamaktadır.

3.2.3 Bulut sistem denetleyicisi

Sistemin uygunluğunu ve genel olarak güvenliğini değerlendiren kurum veya kişilerdir. Bu kurumlar veya kişiler uluslararası çapta belirli standartları göz önünde bulundurarak bulut hizmetlerinin sağladığı faydaların güvenilirliğini ve uygunluğunu ön planda tutmakla sorumludur.

Yaptığı kontroller sonucunda sürecin doğru bir şekilde uyarlandığını, sitemin aktifliğini, beklenen çıktıyı ürettiğini güvenlik vizyonunu göz ardı etmeden takip altında tutmalıdır.

3.2.4 Bulut sistem danışmanlığı

Satın alınan bulut hizmetlerin doğrudan kullanımı karmaşık olabilir. Bu durumda danışmanlıklar devreye girerek uygulanacak süreci kullanıcının ihtiyacına göre çözümleyip, gerekirse hizmete yeni değerler ekleyerek son kullanıcının ihtiyaçlarını karşılayabilir hale getirmektedir.

Bulut sistem danışmanları hizmet sağlayıcıya karşı müşteri olarak gözükebilirken, bulut sistem kullanıcısına ise hizmet sağlayıcı gibi gözükebilir.

3.2.5 Bulut sistem barındırıcı

Bulut sistem üzerinde bulunan verileri uç noktalar arasında transfer edebilmek için fiziksel olarak altyapı hizmeti veren kurumlardır. Bu kurumlar kullanıcı ile sağlayıcı arasında köprü kurmaktadır. Kurulan bu köprünün devamlılığı ile yükümlüdür.

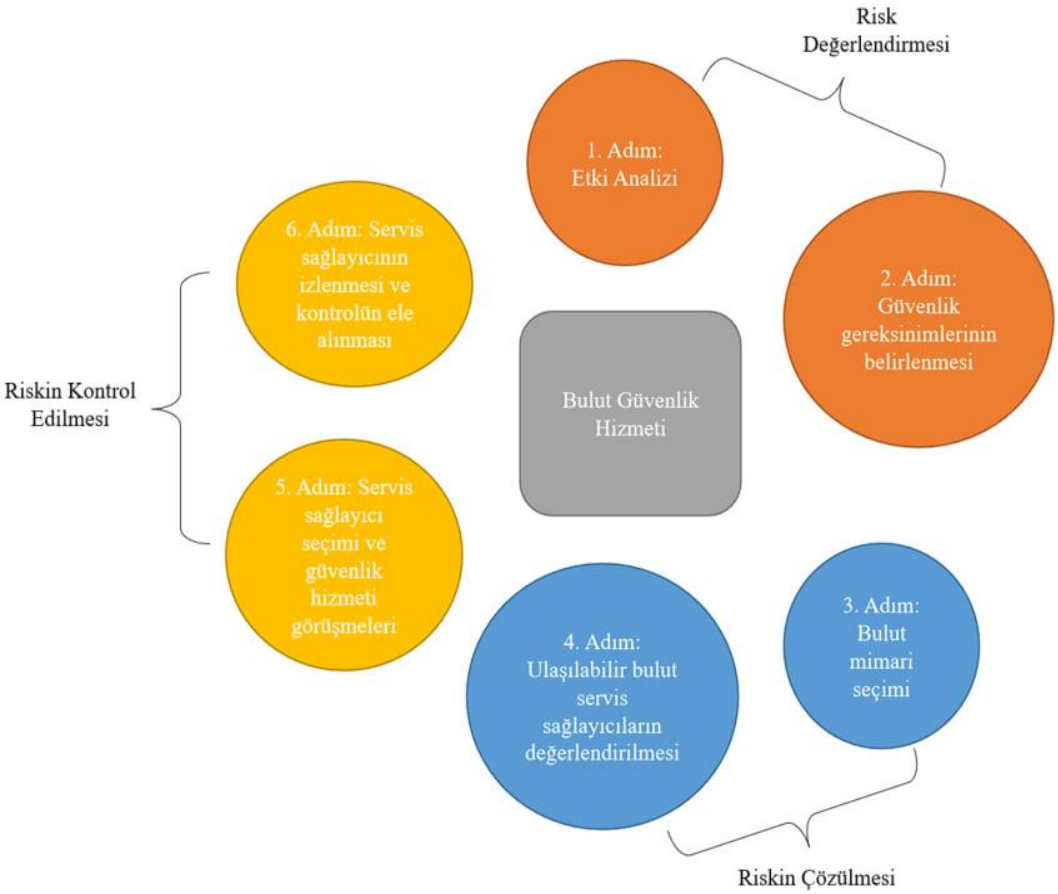
3.3 Bulut Sistemlerde Veri Güvenlik Sertifikaları

Bulut sistemler yapıları gereği sakladığı verileri uluslararası standartlara uygun olarak koruyabilecekleri altyapılara sahip olmalıdır. Bu altyapıları uygun hale getirebilmek için yine uluslararası standartlarda değerlendirmelere tabi olup sertifikasyon süreçlerinden geçmeleri gerekmektedir. Bu bağlamda herhangi bir kurum/kuruluş bulut tabanlı sistem seçimi yaparken mutlaka kullanılacak uygulamanın güvenlik altyapılarını değerlendirmeli, sahip olduğu güvenlik sertifikalarını incelemeli ve kendi alanında uygun olan sertifikasyonlara sahip olup olmadığını kontrol etmesi gerekmektedir.

Güvenlik sertifikaları servis sağlayıcılarının belirli güvenlik standartlarını eksiksiz karşıladığını denetleyerek doğrulayan bağımsız kuruluşlar tarafından verilmektedir. Servis sağlayıcılar bu sertifikalar ile sistemler üzerinde saklanan verilerin güvenliği, şifrelenmesi, erişimde kimlik doğrulamaları, ağ güvenliği ve fiziksel anlamda güvenlik olmak üzere farklı vizyonlardaki güvenlik durumunun dünya standartlarında ihtiyacı karşılar nitelikte olduğunu kanıtlamaktadır. Servis sağlayıcılar bu sertifikaları bulundurdukları süre boyunca düzenli denetimler ile verinin korunması, veri ihlali riskinin azaltılması, müşterinin güven duyması ve güncel gereksinimlere uyumluluk sağlaması açısından da büyük önem taşımaktadır.

Bulut tabanlı hizmet sunan uygulamalar incelemeye alındığında bulundukları konum gereği dışarıdan gelebilecek her türlü tehdide açık oldukları kaçınılmaz bir gerçektir. Bu sebeple bu tarz uygulamaların kurumsal altyapıda kullanılması için yapılacak seçimlerde uygulamaların sahip olduğu başlıca güvenlik sertifikaları değerlendirilmeli ve bu sertifikaların uygulanacak çözüme uygunluğu dikkate alınmalıdır.

NIST ve EC raporlarına göre servis sağlayıcıların hizmet seviyesinde güvenlik sağlaması müşterilerini elde tutmak ve yeni müşteri çekebilmek adına oldukça ilgi duyulur hale getirmektedir (Luna, Suri, Iorga ve Anil, 2015). Böylece müşterilerin güvenlik ile ilgili konularda önlem alındığına dair güvende hissetmeleri sağlanabilecektir. Şekil 14'te gözüktüğü üzere NIST tarafından açıklanan başarılı bir bulut tabanlı risk yönetimi çerçevesine göre 6 ana adımda risk yönetimi stratejisini ele almak güvenli hizmet verebilmek için oldukça önemli bir yaklaşımdır.



Şekil 14. Güvenlik İçin Risk Yönetim Süreci (Force ve Initiative, 2010)

Risk Yönetimi Çerçevesine göre yapısal olarak bu adımlar bilgi güvenliği ve risk yönetimi aktivitelerini sistem geliştirme yaşam döngüsüne entegre eden disiplini sağlamaktadır (Force ve Initiative, 2010).

KVKK, GDPR ve HIPAA gibi daha önce açıklanan regülasyonların haricinde bulut sistemlerin sahip olacağı ISO 27001, SOC 2, PCI DSS ve CSA Star gibi sertifikalar hizmet sağlayıcının güvenlik konusunu ciddiye aldığını ve bu anlamda güncel gereksinimleri karşıladığını göstermektedir. Amazon, Salesforce, Microsoft, Google ve IBM gibi bulut servis sağlayıcıları bunlar gibi birçok güvenlik sertifikasına ve standartlarına sahip olup akreditasyonlarını devam ettirmektedirler (Tariq ve Santarcangelo, 2016). Tariq ve arkadaşlarının yaptığı çalışmada yer alan uyumluluk bilgilerine Tablo 14'te yer verilmiştir.

Tablo 14. Servis Sağlayıcılarının Güvenlik Sertifikasyonları ve Akreditasyonları (Tariq ve Santarcangelo, 2016)

Sağlayıcı	**Güvenlik Uyumluluğu**
Amazon	SOC 1, SOC 2, SSAE 16, ISAE 3402, FISMA, DIACAP, FedRAMP, PCI DSS Level 1, ISO 27001, FIPS 140-2, HIPPA, CSA ve MPAA
Salesforce	ISO 27001, SysTrust, SAS ve 70 Type II
Microsoft	FISMA, PCI DSS, HIPAA, SOX, ISO 27001, SAS 70 TYPE 1-2 ve NIST SP 800-53
Google	SAS 70 Type II, FISMA, ISO 27001 ve NIST SP 800-53
IBM	FISMA, SAS 70 Type II, ISO 27001-2002, SSAE 16, SOC 2, NIST SP 800-53 ve HIPPA

Tablo 14'te görüldüğü üzere, günümüzde bulut tabanlı hizmetler sunan büyük ölçekli servis sağlayıcılarda farklı alanlarda farklı disiplinlerin denetlendiği birçok güvenlik uyumluluğu sertifikası bulunmaktadır.

3.3.1 ISO 27001

Bu sertifika, bilgi güvenliği yönetim sistemi için uluslararası bir standarttır. Herhangi bir veriye ulaşmanın günümüz teknolojisinde bu kadar kolay olması, erişilen bilgilerin konumdan bağımsız olarak ulaşılabilir olması durumları incelendiğinde bilgi güvenliği için standartlar vazgeçilmezdir (Marttin ve Pehlivan, 2010). Bir CRM sağlayıcısının ISO 27001'e sahip olması, veri güvenliği, risk yönetimi ve sürekli iyileştirme konularında belirli gereksinimleri karşıladığını gösterir. ISO 27001 ve bunun gibi birçok bilgi güvenliği sertifikasyonu olmasına rağmen hiçbir zaman bu önlemler tek başına yeterli olmamaktadır (Tariq ve Santarcangelo, 2016). Şekil 15'te belirtildiği gibi ISO 27001 uyumluğunun 8 temel adımı bulunmaktadır.



Şekil 15. ISO 27001 Uyum Adımları

Bulut tabanlı sistemlerin bu disiplinleri benimsemiş olması hizmet sağlayıcının uyumluluk sürecine verdiği önemi göstermektedir.

3.3.2 SOC 2

Bu sertifika, hizmet sağlayıcıların veri gizliliği, güvenlik, iş sürekliliği ve sistemlerin işleyişine ilişkin kontrolleri doğrular. SOC 2 sertifikalı bir CRM sağlayıcısı, bu kontrolleri yerine getirmek için bağımsız bir denetimden geçmiştir.

Herhangi bir işletmenin zafiyete sebep olabilecek durumları Tablo 15'te yer verilen tanımların uygunluğu denetlenmiştir.

Tablo 15. SOC 2 Sertifikasyon İçeriği

Kategori	**Kontrol Detayları**
Mahremiyet	- Erişim kontrolü - Çift aşamalı kimlik doğrulama - Şifreleme
Güvenlik	- Ağ ve uygulama katmanları için güvenlik duvarı - Çift aşamalı kimlik doğrulama - İzinsiz giriş tespiti
Kullanılabilirlik	- Performans izleme - Felaket kurtarma senaryoları - Güvenlik olayların yönetimi
İşleme ve Bütünlük	- Kalite güvencesi - İşlem izleme
Gizlilik	- Şifreleme - Erişim Kontrol - Ağ ve uygulama katmanları için güvenlik duvarı

Tablo 15'te belirtilen kategorilerde kontrol edilen detaylar sertifikasyon süreci için denetlenmektedir ancak sertifika almak istemeyen veya başka sertifikalarla güvenilirliğini kanıtlamak isteyen bulut sistemlerin, en temelde tabloda belirtilen ihtiyaçları karşılayabiliyor olması gerekmektedir.

3.3.3 PCI DSS

Özellikle e-ticaret veya ödeme işlemleri yapan işletmeler için önemlidir. 2004 yılında dört büyük kredi kartı şirketinin ortaklığı ile ortaya çıkmıştır (Visa, MasterCard, Discover ve American Express). Bu sertifika, kredi kartı bilgilerinin güvenli bir şekilde işlenmesi ve saklanması için gereken kontrolleri belirler. Bu kontrollerden geçen işletmeler ve kart bilgisi kullanan servis sağlayıcılar sanal ortamda yaşanacak dolandırıcılık riskinin

azalmasına yol açarken bankalar, satıcılar ve kart markaları açısından kayıpları en az seviyeye indirir (Durkin, 2012). Böylece kart bilgisi ile yapılacak işlemlerde sisteme duyulan güvenin artması sağlanmış olur. PCI DSS uyumluluğu için gereken detaylara Tablo 16'da tabloda yer verilmiştir.

Tablo 16. PCI DSS Gereksinimleri (Durkin, 2012)

Güvenli ve sürdürülebilir bir ağ	1. Kart sahibinin verilerini korumak için güvenlik duvarı oluşturulması ve sürdürülmesi 2. Sistem şifreleri ve diğer güvenlik parametreleri için varsayılan bilgilerin kullanılmaması
Kart sahibi verisinin korunması	1. Saklanan kart bilgisinin korunması 2. Herkese açık ve ulaşılabilir ağlar üzerinden iletilen kart ve kart sahibi bilgilerinin şifrelenerek taşınması
Güvenlik açığı yönetimi süreci	1. Düzenli olarak güncellenen antivirüs yazılımlarının kullanılması 2. Güvenli ve sürdürülebilir uygulamalar geliştirilmesi
Güçlü erişim kontrol yöntemleri	1. İşletmelerin ihtiyacı olan verilere göre kart sahibi bilgilerine erişimin kısıtlanması 2. İşlem yapan her kişiye ait tekil bir kimlik bilgisi oluşturulması 3. Kart sahibi bilgilerine fiziksel erişimin kısıtlanması
Düzenli izleme ve ağ kontrolleri	1. Kart bilgilerine ve ağ kaynaklarına tüm erişimlerin kayıt altına alınması ve izlenmesi 2. Güvenlik sistemleri ve süreçlerinin düzenli olarak teste tabi tutulması

Bakım ve bilgi güvenliği politikası	1. Tüm personeller için bilgi güvenliğini detaylı tanımlayan bir politika oluşturulması

Tablodan anlaşılacağı üzere PCI DSS bir ödeme sürecini uçtan uca tanımlayarak, her noktada uygulanması gereken güvenlik önlemlerini adım adım belirtmiştir.

3.3.4 CSA STAR

Bulut hizmet sağlayıcılarının güvenlik kontrolleri ve uygulamaları hakkında açık bir şekilde bilgi sağlamak için Cloud Security Alliance (CSA) tarafından sunulan bir programdır. CSA STAR sertifikalı bir CRM sağlayıcısı, bulut güvenliği en iyi uygulamalarını takip ettiğini gösterir. Bu çalışmada adı geçen standartları ve daha fazlasını kapsayan bir denetleme süreci ile bulut tabanlı sistemlerin denetim ve uyum adına yetkinliğini garanti altına almaktadır. Şekil 16'da belirtildiği gibi STAR birçok farklı disiplini bir arada tutmaktadır.

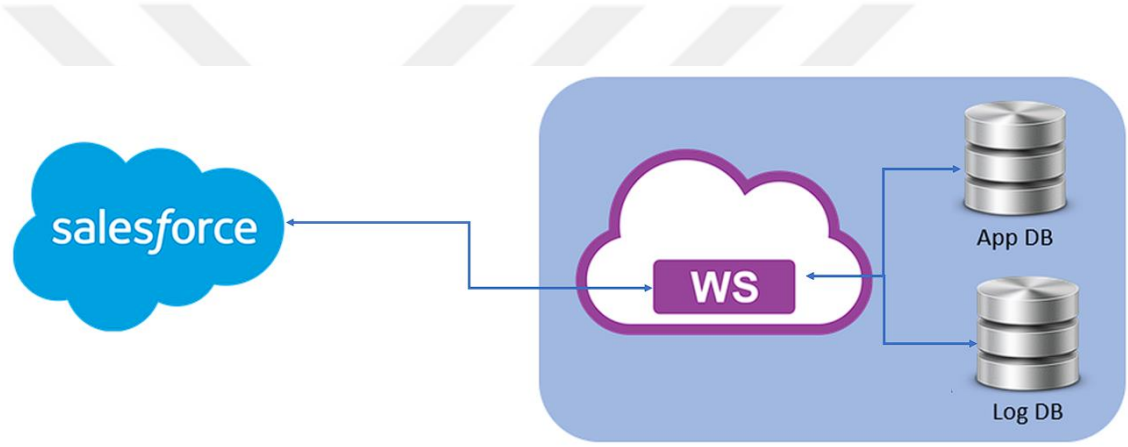


Şekil 16. CSA STAR Standartları

Bu birliğe katılan uygulamalar arasında sektörde bilinen büyük bulut uygulamaların birçoğu yer almaktadır (Srinivasan, 2014). Bunlardan başlıcaları Amazon Web Services, Microsoft, Salesforce, IBM, Cisco. STAR kelimesi ise Güvenlik, Güven ve Güvence Kaydı (Security, Trust and Assurance Registry) anlamına gelmektedir.

4. UYGULAMA

Bu tez çalışması içerisinde bir bulut uygulamayla birlikte yerel veritabanı ile haberleşmek için web servis ihtiyacı bulunmaktadır. Kullanılacak bulut uygulama Yöntem bölümünde belirtilen sağlayıcıların karşılaştırması ve kullanıcı puanlamaları göz önünde bulundurularak Salesforce olarak belirlenmiştir. Burada hazırlanacak web servis doğrudan Salesforce ortamından gelen istekleri karşılayıp ihtiyaç duyulan bilgiyi dönecek nitelikte olacaktır. Şekil 17'de önerilen mimariye ait şablon paylaşılmıştır.



Şekil 17. Veri Yerelleştirme İçin Genel Mimari

Şekil 17'de belirtildiği gibi bulut sistem olarak oldukça popüler olan Salesforce CRM ürününün geliştirici versiyonu üzerinde müşteri bilgileri ile ilgili verinin lokal ortamda şifrelenerek saklanması için çalışma yapılacaktır. Verilerin niteliği ile ilgili detaylar doğrudan platformun sağladığı alan niteliklerinden elde edilebilir. Böylece saklanan veriler ile ilgili yapılacak çalışmada şifrelenecek verinin kategorisine göre uygun yöntemin belirlenmesi için seçici bir bilgiye sahip olunacaktır.

4.1 Yerel Ortam Web Servis

Yapılacak çalışmada bulut tabanlı CRM uygulaması üzerinde yapılacak geliştirmenin veriyi lokal ortamda güvenli bir şekilde saklaması için web servis hazırlanacaktır. Bu web servis sayesinde uygulamadan gelen bilgiler kurulacak veritabanında aşağıdaki bilgiler

göz önünde bulundurularak saklanıp örnek veriler ile erişim ve görüntüleme performansları göz önünde bulundurulacaktır.

- Verinin CRM Id'si
- Verinin CRM üzerinde saklandığı alan bilgisi
- Verinin CRM üzerindeki değeri (test amaçlı tutulmuş olup canlı kullanımda yer almayacaktır)
- Verinin CRM sistemi üzerindeki tipi
- Verinin lokal veritabanına gönderilme tarihi
- Verinin lokal veritabanında güncellenme tarihi
- Verinin şifrelenmiş hali

Id	RecordId	RecordKey	CreatedDate	UpdatedDate	RecordValueEnc
1	0018e000009rY7AAAU	Contact_Person__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	yLxBq85f6JDBIXxYDaQZCOmpLiMLMpNwm8Ex1yoOY8o=
2	0018e000009rY7AAAU	Phone	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	XpMcavio0lwzgnihQ4sBtg==
3	0018e000009rY7AAAU	Email__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	jyMkvTEXDdtmUDSqx+eOsCOsG89Jfj4FvyqDT+ts6Zo=
4	0018e000009rY7AAAU	Website	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	7NLp3F04P47JHR/JELK+VWrfndXlqy/+xBF73FtrGNFNbGTl6ctaDw...
5	0018e000009rY7BAAU	Contact_Person__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	iZhdxy0Qakb+R/IPvlzvEA==
6	0018e000009rY7BAAU	Phone	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	HlWuOJ9b685UPiMsC2tSHw==
7	0018e000009rY7BAAU	Email__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	vH1A2+r4dAVwwdlJFc6LzA==
8	0018e000009rY7BAAU	Website	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	GxZtdNpIP/2LG+sinO98bkrNML0KK8M1ZzaIS9IPp6vK0H7LwetBGi...
9	0018e000009rY7CAAU	Contact_Person__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	Zn727tqil5FavkdD8mAHVQ==
10	0018e000009rY7CAAU	Phone	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	d/RR3dTtr7ANr4rv+B81uQ==
11	0018e000009rY7CAAU	Email__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	4SvucaQ7j61DtKng8eep+fMj2cf5hYsYKrurdvXJP2A=
12	0018e000009rY7CAAU	Website	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	J6C+SpOoWOOa6wFqBF6ORQaQHRNncd3oXXaAhJ4lJRzNTlDcw...
13	0018e000009rY7DAAU	Contact_Person__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	euWcEKODxXj/QXCrA2o9Dw==
14	0018e000009rY7DAAU	Phone	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	+FYB+cy318NqRJHquUB2rA==
15	0018e000009rY7DAAU	Email__c	2023-03-19 17:57:47.4482982	2023-03-19 17:57:47.4482982	d19nVrbd+sHF/syB0TJb4g==

Şekil 18. Yerel Veritabanında Saklanan Örnek Bir Veri

Hazırlanan web servis ile doğrudan kayıt oluşturma veya kayıt ekranı üzerinde hassas veriyi görüntüleme değil, ihtiyaç halinde tekil olarak bir alana ulaşılmasını sağlayacak alternatif bir fonksiyon daha hazırlanmıştır.

Bu fonksiyon ile bulut tabanlı sistem üzerinde sistemin mevcut özellikleri kullanılmak istendiğinde ilgili fonksiyon üzerinden istenilen veri alınabilir, iş sürecine dahil edilebilir. Böylece sistemin standartta verdiği uyarlama süreçlerini uçtan uca hazırlanan bu çalışma ile yürütülebilir olması sağlanmıştır.

4.1.1 Web servis mimarisi

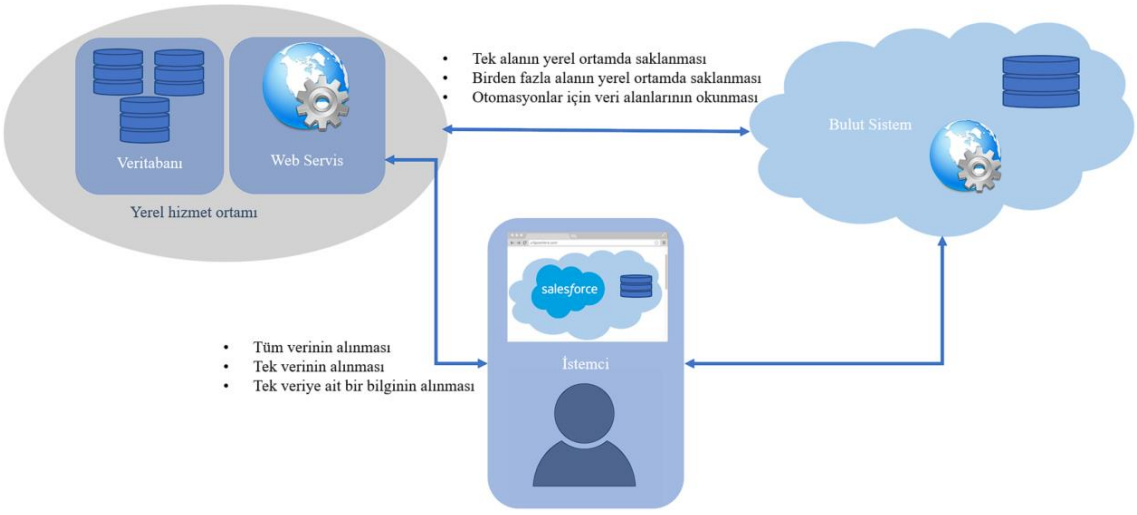
Web servis mimarisi oluşturulurken, yapılan çalışmada temel alınan ihtiyaçlar göz önünde bulundurulmuştur. Bu mimaride ihtiyaçların değerlendirilmesi aşaması kullanılan

CRM uygulamalarının kullanım amaçları ile doğrudan örtüşecek şekilde tanımlanmıştır. Bu sebeple sadece kullanıcı gözünden uygun yetki seviyesinde verinin gösterilmesi ile sınırlı kalmadan, CRM uygulamalarının sunduğu kolaylıkları yine CRM uygulamalarının otomasyon araçları ile kullanılabilmesi için tasarım yapılmıştır.

Mimari yapı kurgulanırken, sistem üzerinde belirlenen tekil alanların dinamik olarak gönderileceği web servis fonksiyonları tasarlanmıştır. Bu fonksiyonlar ile kullanılacak sürece bağlı olarak tekil kayıt gönderimi (kayda ait alan-değer bilgileri) yapılabildiği gibi toplu veri aktarım durumlarında regülasyonlara uygun bir şekilde verinin yerel sunucuya hızlıca taşınabilmesi için toplu veri alan ek fonksiyon hazırlanmıştır. Böylece anlık kullanıcı bazlı güncellemelerde hızlıca işlem yapılabilmesi hedeflenmiştir.

Web servis mimarisi tasarlanırken, verilerin güvenli bir şekilde saklanabilmesi için bu çalışmada konu edilen güvenli şifreleme yöntemleri kullanılmış ve hassas veriye erişimin güvenli olması sağlanmıştır.

Yerel ortam üzerinde bulunan servisler üzerinde güvenlik seviyesini bir üst noktaya taşıyıp CRM uygulaması haricinde veri yazma veya güncelleme yöntemi ile sunucu üzerinde oluşabilecek kötü niyetli veri bozmaya yönelik atakların önlenmesi için güvenlik duvarı ve IP filtreleme süreçlerinden faydalanılmalıdır. Güvenlik duvarı üzerinde tanımlanacak IP adres veya adres aralıkları veri entegrasyonunun yapılacağı CRM platformu tarafından sağlanmalı ve web servis erişimi için kısıtlamalar yönetilmelidir.



Şekil 19. Web Servis Fonksiyonları

Yerel veritabanına web servis aracılığıyla kaydedilen verilerin kullanıcı ekranlarında uygun yetki koşullarına bağlı olarak görüntülenmesi için hazırlanan servisler ile ekranda açık olan kaydın şifrelenmiş tüm alanlarının şifresi çözülerek kullanıcıya görüntülenebilmesi hedeflenmiş ve bu sayede gereksiz veri dönüşü ile sistem üzerinde oluşabilecek ekstra yükün önüne geçilmiştir.

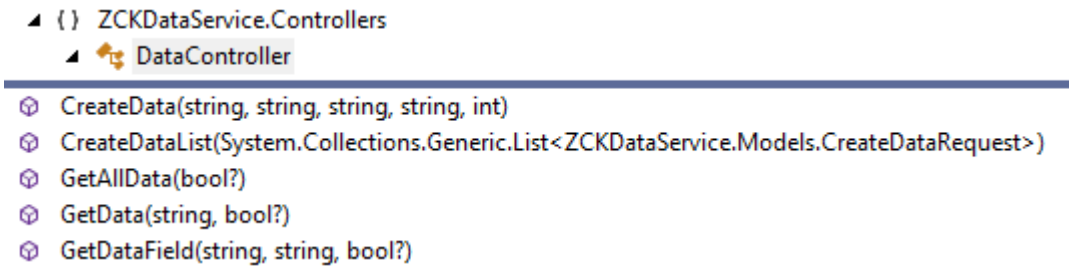
Temel veri gösterim süreçlerinin haricinde, CRM sistemi üzerinde kurulacak otomasyon süreçlerin bulutta yer almaması nedeniyle sekteye uğramaması için, kayda özel alan bazı veri sorgulama yapısı ile ihtiyaç duyulan alandaki verinin görüntülenmesi sağlanmıştır.

4.1.2 Web servis fonksiyonları

Web servis mimarisi hazırlanırken belirlenen süreçler için farklı parametrelerle çalışabilecek fonksiyonlar hazırlanmıştır. C# programlama dili kullanılarak hazırlanan web servis içerisinde verinin görüntülenmesi için birden fazla fonksiyon bulunmaktadır. Görüntülenecek veriye dair tüm bilgiler, ihtiyaç duyulan tekil bilgi sorgulaması gibi fonksiyonlar yer alırken verinin yerel veritabanına yazılması için kullanılan yapıda tekil alan kaydetme/güncelleme ve çoklu veri kaydı fonksiyonları yer almaktadır.

Tüm fonksiyonlarda temel performans ölçümleri yapılabilmesi için istek başlangıç ve bitişlerinde zaman damgası alınarak geçen sürenin hesaplanması ve kullanılan kayıt günlüğü tutma kütüphanesi ile veritabanında raporlanabilir şekilde saklanması

sağlanmıştır. Böylece elde edilecek bilgi ile sistem üzerinde sıkışmaya yol açan fonksiyonların tespiti hızlıca yapılarak ihtiyaç durumunda düzenlenebilmesi için destek sağlayacaktır.



Şekil 20. Web Servis Fonksiyon Görümünü

Veri kaydetme servisleri bulut sistemden gelen istekleri işleyip olası yük artışlarını engellemek üzere tasarlandığından şifreleme karar mekanizması bulut sistem üzerinde kurulmuştur. Böylece sunucu tabanlı yaşanabilecek performans sorunlarının önüne geçilmiş olup olası yükün bulut sistem üzerinde bırakılması hedeflenmiştir. Bulut sistem üzerinden gelen güvenlik algoritmaları web servis uygulamasında Şekil 21'de belirtildiği gibi enum olarak tanımlanıp temel şifreleme algoritmaları için tam sayı değişken atamaları yapılmıştır.

```
13 references
public enum SecurityAlgorithms
{
    AES = 1,
    BlowFish = 2,
    DES = 3,
    DES3 = 4,
    RC = 5
}
```

Şekil 21. Tanımlı güvenlik algoritmaları

Şifreleme ve şifre çözme süreçleri için yardımcı fonksiyonlar oluşturularak gelen isteklerin web servis fonksiyonları içerisinde dinamik olarak işlenmesi sağlanmıştır. Algoritmalar için yardımcı sınıflar oluşturulup, Şekil 22'de gösterildiği gibi şifreleme ve

Şekil 23'te gösterildiği gibi şifre çözme fonksiyonları üzerinden kontrollü yönlendirme yapılmıştır.

```
public static string encryptData(string recordId, string fieldKey, string value, Models.SecurityAlgorithms securityAlgorithm)
{
    string retVal = null;
    string keyData = generateKey(new List<string>() { recordId, fieldKey }); //to combine source system recordId and field api key
    if (securityAlgorithm == Models.SecurityAlgorithms.AES)
    {
        Helpers.Algorithms.AES aesSecurity = new Helpers.Algorithms.AES();
        retVal = aesSecurity.Encrypt(keyData, value);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.BlowFish)
    {
        var iv = Encoding.UTF8.GetBytes(fieldKey);
        int blockSize = 8;
        var ivpadded = Algorithms.BlowFish.PadOrTrimIV(iv, blockSize); //field key block size doesn't enough for vector, padded.

        var plainTextByteData = Encoding.UTF8.GetBytes(value);
        var recordIdByteData = Encoding.UTF8.GetBytes(recordId);
        var result = Algorithms.BlowFish.BlowfishEncrypt(plainTextByteData, recordIdByteData, ivpadded);
        retVal = Convert.ToBase64String(result);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.RC)
    {
        var plainTextByteData = Encoding.UTF8.GetBytes(value);
        var key = Encoding.UTF8.GetBytes(keyData);
        var encryptedData = Helpers.Algorithms.RC.RCApply(plainTextByteData, key);
        retVal = Convert.ToBase64String(encryptedData);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.DES)
    {
        retVal = Helpers.Algorithms.DES.Encrypt(value, keyData);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.DES3)
    {
        retVal = Helpers.Algorithms.DES3.Encrypt(value, keyData);
    }
    return retVal;
}
```

Şekil 22. Şifreleme Fonksiyonu

```
public static string decryptData(string recordId, string fieldKey, string value, Models.SecurityAlgorithms securityAlgorithm)
{
    string retVal = null;
    string keyData = generateKey(new List<string>() { recordId, fieldKey });
    if (securityAlgorithm == Models.SecurityAlgorithms.AES)
    {
        Helpers.Algorithms.AES aesSecurity = new Helpers.Algorithms.AES();
        retVal = aesSecurity.Decrypt(keyData, value);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.BlowFish)
    {
        var iv = Encoding.UTF8.GetBytes(fieldKey);
        int blockSize = 8;
        var ivpadded = Algorithms.BlowFish.PadOrTrimIV(iv, blockSize);
        var converted = Convert.FromBase64String(value);

        var recordIdByteData = Encoding.UTF8.GetBytes(recordId);
        var result = Algorithms.BlowFish.BlowfishDecrypt(converted, recordIdByteData, ivpadded);

        retVal = Encoding.UTF8.GetString(result).Replace("\0", "");
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.RC)
    {
        var plainTextByteData = Encoding.UTF8.GetBytes(value);
        var key = Encoding.UTF8.GetBytes(keyData);
        var encryptedData = Helpers.Algorithms.RC.RCApply(plainTextByteData, key);
        retVal = Convert.ToBase64String(encryptedData).Replace("\0", "");
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.DES)
    {
        retVal = Helpers.Algorithms.DES.Decrypt(value, keyData);
    }
    else if (securityAlgorithm == Models.SecurityAlgorithms.DES3)
    {
        retVal = Helpers.Algorithms.DES3.Decrypt(value, keyData);
    }
    return retVal;
}
```

Şekil 23. Şifre Çözme Fonksiyonu

Dinamik anahtar üretimi için fonksiyon hazırlanarak, düz metin listesi alıp "_" ile birleştiren bir fonksiyon hazırlanmıştır. Fonksiyon detayına Şekil 24'te yer verilmiştir. Şifreleme ve şifre çözme fonksiyonlarında bu anahtar üretme fonksiyonu aktif olarak kullanılmaktadır. Web servis özelinde anahtar üretme fonksiyonu kaydın bulut sistemde sahip olduğu tekil anahtar verisi ve alanın bulut sistem üzerindeki alan adını kullanarak çalışacak şekilde çağırılmıştır.

```
/// <summary>
/// This function concatenates given string list items with "_"
/// </summary>
/// <param name="keyList"></param>
/// <returns>Generated Key Value as String Property</returns>
2 references
private static string generateKey(List<string> keyList)
{
    string keyRawData = String.Join("_", keyList);
    return keyRawData;
}
```

Şekil 24. Anahtar Üretme Fonksiyonu

4.1.3 Şifreleme algoritmasının belirlenmesi ve verilerin şifrelenmesi

Şifreleme algoritmasının belirlenmesi, ürünün dışında farklı bir ortamda saklanacak verinin güvenliğini üst seviyeye çıkarmak adına oldukça kritik öneme sahiptir. Şifrelenecek verinin karakter boyutuna bağlı olarak seçilecek algoritmanın performansı farklılık göstermektedir. Farklı şifreleme algoritmasının farklı avantajları ve dezavantajları olduğunu unutmamak gerekir. Yapılan bu çalışmada yetkili kişi, telefon numarası, mail adresi ve web sitesi bilgisi üzerinde şifreleme yapılmaktadır. Bu verilerin şifrelenmesinde güvenliğin önemi yüksek olduğu kadar şifrelenmiş verinin gösteriminin son kullanıcıya hızlı bir şekilde dönebilmesi için performansında bir o kadar iyi olması gerekmektedir.

Ayrıca şifreleme türünün uzun vadeli çalışmalarda değişiklik ihtiyacı olduğu kesinlikle göz önünde bulundurulmalıdır. Şifreleme algoritmalarının güvenlik durumu incelendiğinde zaman içerisinde şifreleme türlerinin çeşitli saldırılara karşı güvenliğinin azaldığı gözlemlenmiştir (Gnatyuk, Kinzeryavyy, Iavich, Prysiazhnyi ve Yubuzova, 2018). Bu nedenle hazırlanacak uygulamanın kullanacağı şifreleme algoritmasının güncel ihtiyaçlara göre güncellenebilir olması gerekmektedir. Böylece gelecekte ihtiyaç duyulacak daha güvenli ve daha performanslı algoritmalara hızlıca geçiş yaparak bulut sistem üzerinde görüntülenen verinin erişim performansı her geçen gün artarken çeşitli güvenlik zafiyetlerine karşı önlem alınabilmiş olunacaktır.

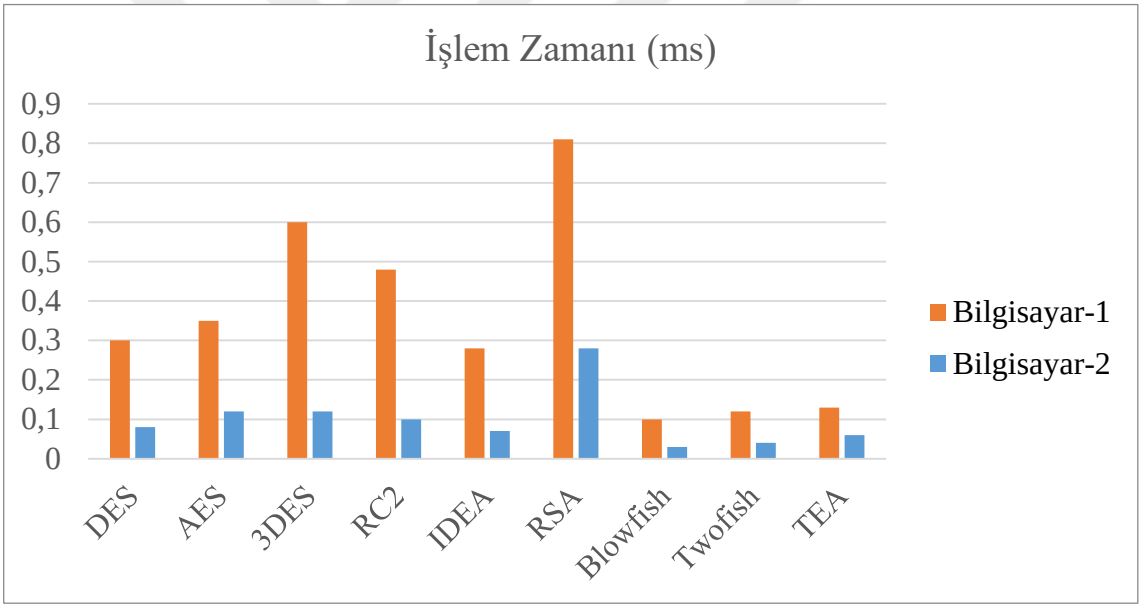
Şifreleme aşamasında uygulama geliştirilirken veri tipine bağlı olarak farklı algoritmaların kullanımı değerlendirilmiştir ancak şifrelenecek verinin boyutunun hassas veri bazında nitelendirildiğinde farklı tiplerde gözle görülür bir farklılık göstermemesi nedeniyle raporlanabilecek bir farklılık tespit edilememiştir.

Farklı bilgisayarlar kullanılarak yapılan şifreleme işlemlerinde AES, DES gibi oldukça popüler algoritmaların 102 bytelık bir veriyi 1 saniyenin altında şifreleyebildiği ve farklı algoritmalarda da sürenin yine 1 saniyenin altında kaldığı gözlemlenmiştir (Günden, 2010). Tablo 17'de yer verilen detaylar bu çalışmada kullanılan bilgisayarların özelliklerini göstermektedir.

Tablo 17. Test Sistemlerinin Detayları (Günden, 2010)

	İşlemci	Hafıza	İşletim Sistemi
Bilgisayar-1	Intel Core 2 Duo T7500 2.20GHz	2.00 GB	Windows 7
Bilgisayar-2	Intel Pentium M 1.70Ghz	0.76 GB	Windows XP

Bu çalışmada saklanacak veriler özelinde değerlendirme yapıldığında çok daha az yer kaplayan kelimelerin şifreleneceği düşünülerek süreler arasındaki farklılıklar kaybolacaktır.



Şekil 25. Farklı Şifreleme Algoritmalarının 102 Byte'lık veriyi işleme süresi (Günden, 2010)

Şekil 25'te belirtilen işlem süreleri farklı donanım ve yazılım altyapısına sahip sistemlerde test edilerek elde edilmiştir. Farklı donanım bilgilerinin detaylarına ise Tablo 13'te yer verilmiştir. Bu verilerin elde edilmesinde, doğru sonucu üretebilmek adına 50 kez şifreleme ve şifre çözme işlemi uygulanması ile elde edilen çıktıların ortalaması kullanılmıştır.

Şifreleme sürecinde başlangıç olarak AES şifreleme yöntemi kullanılmıştır. AES şifreleme yönteminde ihtiyaç duyulan anahtar dinamik olarak üretmektedir. Anahtar üretilirken kaydın bilgisi olan CRM ID'si ve alan adı belirli bir şablonda birleştirilerek üretilmiştir.

Blowfish algoritmasında blok boyutu 64 bit olduğundan üretilen dinamik anahtar için düzenleme yapılması gerekmektedir. Bunun için ayrıca bir fonksiyon hazırlanıp istenilen değere göre çıktı oluşturulması sağlanmıştır.

Blowfish algoritması üzerinde yapılan çalışmalarda şifreli verinin çözülmesi ve istemci tarafına gelmesi ilk sorgulamada 1,5 saniyenin üzerinde bir sürede dönmektedir. Farklı şifreleme algoritmalarının şifre çözme süreleri ile ilgili çıktı geliştirmeler tamamlandıktan sonra toplu olarak yapılan işlemlerin transfer hızları baz alınarak seçilecektir.

4.1.4 Verilerin kayıt altına alınması

Yapılan bu çalışmada verilerin şifrelenip saklanmasına ek olarak erişim ile ilgili bilgilerin ayrıca saklanıp ihtiyaç halinde raporlanabilmesi KVKK gereğince alınması gereken aksiyonlardan birisidir. Bunun için çalışmada kayıt altına almak için uygulama marketinden hazır olarak temin edilecek bir kütüphane kullanılmıştır. Bu kütüphane ile asenkron olarak hazırlanan kayıt bilgisinin veritabanında uygun formatta saklanması sağlanmıştır.

Burada önemli olan konu erişimi kayıt altına alırken veritabanı kaynaklı darboğazların önüne geçmek için farklı bir veritabanı kullanılmasıdır. Farklı veritabanı konfigürasyonu sayesinde canlı ortamlarda kullanılması planlanan bu tarz servis uygulamalarının altyapılarında fiziksel olarak farklı sunucular belirlenerek verinin hızlıca kayıt altına alınması sağlanmıştır.

4.1.5 Verilerin çözümlenmesi ve yorumlanması

Bu çalışma ile elde edilen şifrelenmiş verilerin çözülme ve istemciye geri dönme süreleri verilerin kayıt altına alınması ile ilgili başlık altında detaylı bir şekilde anlatılmıştır. Bu aşamada toplanan veriler üzerinden basit çıktılar alarak tercih edilen şifreleme yöntemine göre ortalama olarak harcanan sürenin belirlenmesi sağlanmıştır.

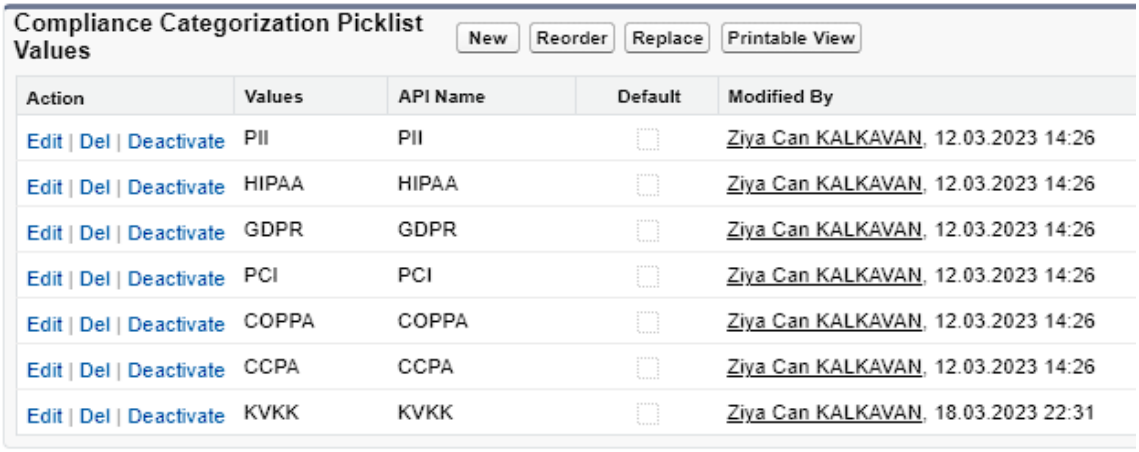
4.2 Verilerin Kategorizasyonu

Verinin kategorize edilmesi süreci işletme kültürü, iş modeli, süreç gereksinimi gibi farklı alanlardaki ihtiyaçlara göre değişiklik göstermektedir. Bu çalışmada önerilen yöntem ile, KVKK ve GDPR kısıtlamalarında belirtildiği gibi, doğrudan bireye ulaşmayı sağlayabilecek herhangi bir verinin sisteme kolaylıkla dahil edilebilmesi sağlanmıştır.

Kullanılan bulut çözümün, verileri kategorize etmede alan bazlı işaretleme yaptırması uyarlanacak çözümün uyarlanma hızını artırmaktadır. Salesforce üzerinde bu süreç varsayılan olarak aşağıdaki başlıklar halinde bulunmaktadır;

- CCPA
- COPPA
- GDPR
- HIPAA
- PCI
- PersonalInfo
- PII

Yukarıda tanımlanan kategorilere ek olarak sistem üzerinde kullanıcı tanımlı kategoriler oluşturulabilmesine imkan sağlanmaktadır.



Şekil 26. Ön tanımlı ve sonradan tanımlanan kategoriler

Şekil 26'da görüldüğü üzere sistemin oluşturulduğu tarihte daha önce bahsedilen kategoriler bulunurken, KVKK ayrıca eklenmiştir. Bu çalışmada mevcut kategorilere KVKK eklenerek veri transfer süreci ele alınacaktır. Bu yöntem ile sunucu tarafında herhangi bir ek çalışma gerektirmediğinden sadece ilgili sistem yöneticisi tarafından basit ayarlar ile uygulanabilmektedir. Kategorize edilmiş verilerin seçimi, sistem standartlarında basit bir sorgulama ile yapılabilmektedir.

```
SELECT Label, DeveloperName, Length, DataType, ValueTypeId, ComplianceGroup FROM FieldDefinition WHERE
EntityDefinitionId in ('Account') and ComplianceGroup != null
```

Query Results - Total Rows: 4

Label	DeveloperName	Length	DataType	ValueTypeId	ComplianceGroup
Website	Website	255	URL(255)	string	KVKK
Email	Email	80	Email	string	KVKK
Contact Person	Contact_Person	150	Text(150)	string	KVKK
Phone	Phone	40	Phone	string	GDPR;KVKK

Şekil 27. Alan tanımları tablosu üzerinde kategori sorgulaması

Sistem yöneticisi tarafından kategorize edilmiş verilere Şekil 27'de gösterildiği gibi erişim sağlanmaktadır. Bu yöntem ile yerel sistem üzerinde çalışacak web servis iletişiminde şifrelenecek alanların yönetimi yazılımdan bağımsız, dinamik olarak gönderilebilecektir.

Hazırlanan sorguda ComplienceGroup olarak belirtilen alan, Şekil 26'da yer verilen kategorileri barındırabilmektedir. Yetkili kullanıcı tarafından seçilebilen bu alanlar, uygulama içerisinde dinamik olarak sorgulama sürecinde fayda sağlamaktadır.

Şekil 27'de gözüktüğü üzere, verilen örnek için Phone alanı GDPR ve KVKK için kategorize edilmiş. Bu sayede, farklı kısıtlamalara tabi bölgelerde faaliyet gösteren işletmelerin, sahip oldukları veri şemasını hizmet alanlarındaki ihtiyaçlara göre birden fazla kategoride saklayabilmesi sağlanmıştır.

Bu çalışmada gerçekleştirildiği gibi KVKK ve GDPR için kategorize edilmiş alanların sistem üzerinde belirlenebilir olması, kişisel verilerin korunmasında raporlama açısından yol gösterici niteliktedir. Bu sayede olası bir denetlemede işletmelere ilgili denetleyici kuruluşlara, burada yer alan kısıtlamalarla ilgili uygulanan tedbirleri hızlı bir şekilde gösterebilir, tedbirlerle birlikte hangi verilerin hangi standartlarda kategorize edildiğini

sunabilir. Standart yazılımlarda bunun gibi kategorizasyon işlemlerinde yüksek eforlu ve maliyetli geliştirme süreçleri yer alırken, bulut tabanlı gelişmiş sistemlerde özelleştirmeye açık yapılar hazır bir şekilde gelmektedir. Sistem yöneticilerinin uygulanacak güvenlik, gizlilik çözümüne göre düzenleme yapması günümüz teknoloji dünyasının gereksinimlerine uygun bir veri yönetimi kültürünü ortaya çıkartmada büyük önem taşımaktadır. Bunun gibi düzenlemeler ile veri gizliliğine yönelik tehditler önemli ölçüde azalabilir.

4.3 Bulut Geliştirme Ortamı

Salesforce uygulaması kendi içerisinde farklı disiplinlerde geliştirme yapılabilmesine olanak sağlayan bir bulut bilişim uygulamasıdır. Salesforce ortamında geliştirme yapılırken mevzuata uygun bir şekilde saklanan verinin görüntülenebilmesi için Lightning component, verilerin senkronizasyonu için apex class kullanılacaktır. Böylece uluslararası ortamlarda saklanan verilerin lokal kopyalarına istemci tarayıcısı üzerinden bağlantı sağlanarak verinin yurtdışında dolaşımı engellenmiş olacaktır. Ürünün sağlamış olduğu güvenlik altyapıları sayesinde ürün üzerinde geliştirilen uygulamanın dışarıdan erişilebilirliği sistem özelinde kısıtlanmış olacaktır. Ürün kimlik doğrulama ve yetkilendirme özellikleri sayesinde ürün üzerinde geliştirilen hizmetlere erişimde oldukça geniş kapsamlı bir güvenlik çözümü sunacaktır. Bu sayede verilerin ülke içinde tutulmasını sağlayan altyapı ile iletişim uluslararası güvenlik önlemleri alınarak sağlanacaktır.

Salesforce üzerinde dikkat edilmesi gereken başka bir konu ise veri saklama modeli. Veri saklama erişme modelinde ürünün kendine özgü tanımları bulunmaktadır. Günümüz modern veritabanlarında tablo, sütun olarak adlandırılan kavramlar Salesforce veritabanında nesne ve alan olarak adlandırılmaktadır. Standart bir Salesforce uygulamasında bulunan nesnelere ek olarak yeni nesneler ve yeni alanlar açılması durumunda geliştirici tarafından özelleştirilmiş bir sürece bağlı olarak bunların açıldığını ifade edebilmek amacıyla farklı bir isimlendirme yapısı kullanılır.

Bu çalışma içerisinde Salesforce tarafında müşteri bilgilerinin tutulduğu “Account” olarak adlandırılan nesne aktif olarak kullanılmıştır. Bu nesne üzerinde çalışmalar yapılırken kullanılacak yeni alanlar açılmıştır. Açılan bütün bu alanlara Salesforce

otomatik olarak "__c" eklemektedir. Böylece başka bir geliştirici veya ürün üzerinde yönetici yetkisine sahip bir kişi veri yapısını kontrol ettiğinde bu alanın standart dışı bir ihtiyaca yönelik olarak açıldığını anlayabilmektedir.

Nesne ve alanlar üzerinde kullanılan bu isimlendirmeler API adı olarak tanımlanmaktadır. Son kullanıcılar bu tanımları nesne veya alan açılırken girilen API adları yerine kullanıcılarına tanımlı dil ile eşleşen çevrim karşılığını görmektedir. Böylece çok uluslu şirketlerde kullanılan bu uygulama üzerinde entegre edilen çözümler çoklu dil seçeneği ile ortak olarak kullanılabilmektedir.

4.3.1 Veri transferi

Transfer sürecinin yapılabilmesini sağlayabilmek adına CRM uygulamasında bulunan altyapılar dikkate alınarak kişisel bilgi niteliği taşıyabilecek alanlar belirlenerek arka planda verinin iletilmesini sağlayacak yapı hazırlanmıştır.

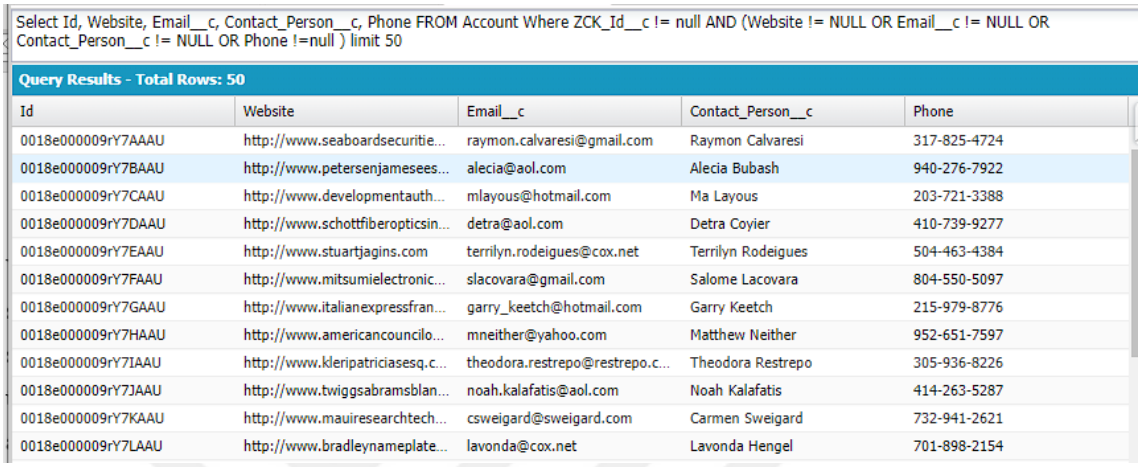
Çalışma özelinde aşağıda belirtilen alanlar baz alınarak sistem üzerinde kişisel bilgi olarak belirlenip sürece dahil olması sağlanmıştır.

- Telefon Numarası (Phone)
- Yetkili Kişi Adı Soyadı (Contact_Person__c)
- E-Posta Adresi (Email__c)
- Web Sitesi (Website)

Yukarıda API adlarıyla belirtilen alanlar altyapıda belirlenerek dinamik bir şekilde sorgulanıp dolu olması halinde web servis ile lokal sunucuya iletilip şifreli bir şekilde saklanmaktadır. Belirlenen alanların yönetimi kategorizasyon sürecinde detaylandırıldığı üzere işaretli alanların dinamik sorguya eklenmesi ile gerçekleşecektir. Böylece yeni bir alanın kısıtlamaya katılması süreci sadece kategori seçimi ile belirleneceğinden çalışmanın bu aşamasında yapılacak olan geliştirmeye farklı bir düzenleme yapma ihtiyacı ortadan kalkacaktır.

Bu bölümde ele alınan alanların belirlenmesi ve seçim süreci Verilerin Kategorizasyonu başlığında detaylı bir şekilde değerlendirilmiştir. Buradaki dinamik yapıya, alanların Salesforce üzerinden dinamik bir şekilde sorgulanabilmesini sağlayacak bir başka

dinamik yapı eşlik etmektedir. Sürece ait hazırlanan fonksiyonlar ile kategorize edilmiş alanların listesi çekilerek Şekil 28'de belirtildiği dinamik sorgu hazırlanıp çalıştırılarak sonuç alınmaktadır. Bu sorgudan dönen veriler belirtilen paket boyutlarında sistem tarafından gruplanarak entegrasyon sürecine dahil edilmiştir.



```
Select Id, Website, Email__c, Contact_Person__c, Phone FROM Account Where ZCK_Id__c != null AND (Website != NULL OR Email__c != NULL OR
Contact_Person__c != NULL OR Phone !=null ) limit 50
```

Query Results - Total Rows: 50

Id	Website	Email__c	Contact_Person__c	Phone
0018e000009rY7AAAU	http://www.seaboardsecuritie...	raymon.calvaresi@gmail.com	Raymon Calvaresi	317-825-4724
0018e000009rY7BAAU	http://www.petersenjamesees...	alecia@aol.com	Alecia Bubash	940-276-7922
0018e000009rY7CAAU	http://www.developmentauth...	mlayous@hotmail.com	Ma Layous	203-721-3388
0018e000009rY7DAAU	http://www.schottfiberopticsin...	detra@aol.com	Detra Coyier	410-739-9277
0018e000009rY7EAAU	http://www.stuartjagins.com	terrilyn.rodeigues@cox.net	Terrilyn Rodeigues	504-463-4384
0018e000009rY7FAAU	http://www.mitsumielectronic...	slacovara@gmail.com	Salome Lacovara	804-550-5097
0018e000009rY7GAAU	http://www.italianexpressfran...	garry_keetch@hotmail.com	Garry Keetch	215-979-8776
0018e000009rY7HAAU	http://www.americancouncilo...	mneither@yahoo.com	Matthew Neither	952-651-7597
0018e000009rY7IAAU	http://www.kleripatriciasesq.c...	theodora.restrepo@restrepo.c...	Theodora Restrepo	305-936-8226
0018e000009rY7JAAU	http://www.twiggsabramsblan...	noah.kalafatis@aol.com	Noah Kalafatis	414-263-5287
0018e000009rY7KAAU	http://www.mauiresearchtech...	csweigard@sweigard.com	Carmen Sweigard	732-941-2621
0018e000009rY7LAAU	http://www.bradleynameplate...	lavonda@cox.net	Lavonda Hengel	701-898-2154

Şekil 28. Dinamik Olarak Sorgulanan Örnek Bilgiler

Salesforce sistemi üzerinde belirli kısıtlar bulunduğundan entegrasyon modelinin herhangi bir zaman-limit aşımına uğramaması için parçalı yapıda veri iletimini sağlayacak entegrasyon yöntemi tercih edilmiştir. Bu yöntem ile belirlenen kısıtlara uyan (kişisel bilgi niteliği taşıyan alanları dolu olan) kayıtlar üzerinden istek listesi hazırlanıp 200'lük paketler halinde servis ile iletimi sağlanmıştır. Böylece CRM sistemi üzerinde oluşacak anlık veri işleme yükü minimuma indirilip lokal web servisin bağlı olduğu veritabanlarında oluşacak veri işleme ve yazma yükünün de azaltılması sağlanmıştır.

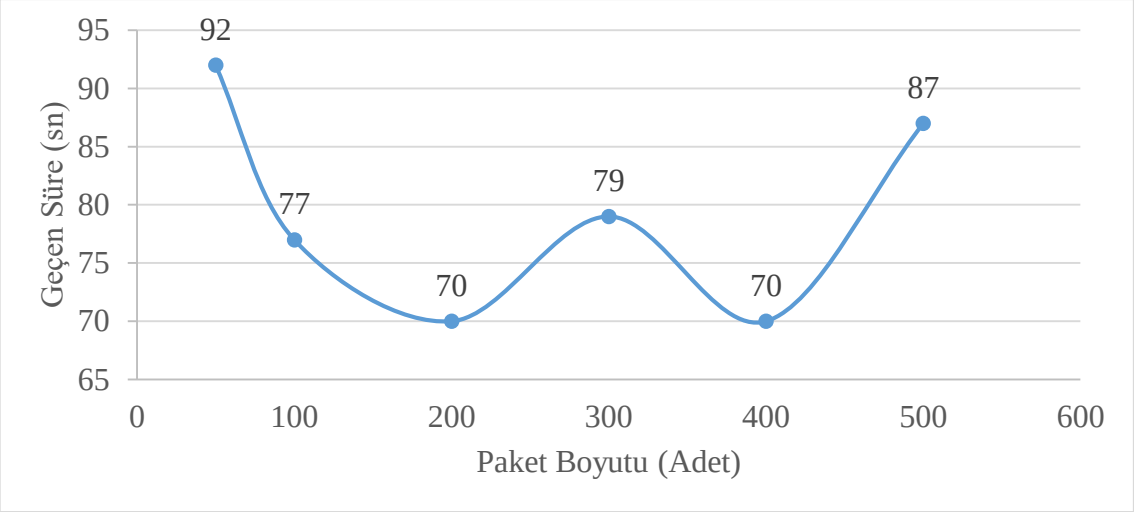
Verinin başarılı bir şekilde lokal sisteme aktarılıp şifreli olarak saklanması sağlandıktan sonra bulut tabanlı CRM sisteminden silinmesi gerekir ancak bu çalışmada veri ile ilgili çeşitli kontroller yapılacağından zaman kaybetmemek adına ilgili alanların boşaltılmasını sağlayacak süreç göz ardı edilip çalışmaya devam edilecektir.

Transfer edilecek veri ile ilgili çeşitli araştırmalara yapılarak bu tarz uygulamalarda yük testi yapılabilmesine olanak sağlayan ve gerçek kurumlar-kişiler olmayan örnek veriler sisteme yüklenmiştir. Paket boyutlarının ölçülebilmesi için transfer sürecinde BlowFish algoritması kullanılmıştır.

Tablo 18. CRM Kayıtlarının Yerel Sisteme Aktarılma Süresi

Kayıt Sayısı	**Transfer Süresi (sn)**
500	16
1000	27
1500	48
2000	70

Tablo 18'de belirtilen sürelerce transfer işleminde harcanan sürelerin lineer olmaması üzerine 2000 kaydın yeniden gönderimi sırasında anlık işlenecek müşteri verisi sayısı farklı boyutlarda değerlendirilerek tekrar deneme yapılmıştır.



Şekil 29. Değişken paket boyutlarına göre aktarım süresi

Paket boyutunda yapılan değişim Salesforce üzerinden merkezi sunucuya yapılan istek sayısını değiştirmiştir. Şekil 29'da ifade edilen grafik ile yapılan isteklerde 200-400 boyutlu paket aralığında optimum performans gösterildiği gözlemlenmiş, altında istek sayısında oluşan artışın; üstünde ise veri boyutunda oluşun artışın performansı olumsuz etkilediği gözlemlenmiştir.

4.3.2 Veri erişimi

Salesforce üzerinde hazırlanan Lightning Component ile lokal sunucuya istek atılarak daha önce sunucu üzerinde şifreli olarak saklanmış olan kaydın getirilmesi sağlanmıştır. Görüntüleme süreci için Lightning Component ile uygulama yapılarak ekran üzerinde sorgulama süresine yer verilmiştir. Son kullanıcı tarafından görüntülenecek ekran görseline Şekil 30'da yer verilmiştir.



Şekil 30. Salesforce Lightning Component ile Hassas Veri Görüntüleme

Ev ortamında hazırlanan sunucu üzerinde ayağa kaldırılan web servis ile yapılan çalışmalarda verinin 0.30 ile 0.70 saniye arasında erişildiği gözlemlenmiştir. Ayrıca yükleme süresi özelinde Salesforce üzerinde kayıt tutulması sağlanarak burada yaşanan gecikme ile ilgili ayrıca rapor üretilmiştir. Yükleme ile ilgili ortalama sürelere Şekil 31'de yer verilmiştir.

Account: Account Name	Average Duration
A All American Travel Inc	553,00
A K Construction Co	476,00
A R Packaging	479,00
Biltmore Investors Bank	419,00
Chanay, Jeffrey A Esq	362,93
Chang, Carolyn Esq	379,00
Chilton Malting Co	515,00
Circuit Solution Inc	453,00
Egnor, W Dan Esq	646,00
Haber, George D Md	379,60

Şekil 31. Hassas Veriyi Görüntüleme Performansı Raporu (ms)

Veriye erişimde erişim hızı kullanıcı deneyimi açısından büyük bir önem taşımaktadır. Uygulamanın halihazırdaki kullanımı bir kenara bırakılıp uyarlanmış bir çözüm ile farklı bir kaynaktan veriyi temin edip görüntülemek ister istemez erişim zamanını olumsuz etkilemektedir. Bu aşamada veri yoğunluğunu göz önünde bulundurarak, her bir kayıt görüntüleme sürecinde bir istek atılacak şekilde çalışma yapılmıştır. Böylece yerel sunucuya erişim için atılan isteğin bir kez kanal açması sağlanmış olup ağ katmanındaki başlatma ve bitirme sürelerinin ortadan kaldırılması hedeflenmiştir.

4.4 Şifreleme Yönteminin Belirlenmesi

Şifreleme yönteminin belirlenmesinde en önemli konu şifreleme/şifre çözme aşamasının performans değerlendirmesi olacaktır. Bu açıdan bakıldığında Salesforce ve yerel sistem arasında gerçekleşen toplu veri aktarım süreleri Tablo 19'te belirtilen özelliklerdeki farklı sunucular kullanılarak test edilmiştir. Toplu veri aktarımlarında kullanılan paket boyutu optimum süreyi yakalayabilmek için Veri Transferi bölümünde yapılan değerlendirme sonucuna bağlı kalarak 250 olarak belirlenmiştir. Testlerin gerçekleştiği, yerel sunucu olarak konumlandırılan sunucu, ev ortamında 100 MBit internet hızına sahip bir dış ağ

erişimi, içeride ise 2.4GHz wifi bağlantısı ile modeme yaklaşık 5 metre mesafede konumlandırılmıştır.

Tablo 19. Yerel Ortam Test Sunucuları

Donanım	**Sunucu 1**	**Sunucu 2**
İşlemci	Intel Core 2 Duo T8300 2.40 GHz	Intel Core i5-8600 3.1GHz
Çekirdek	2	6
Harddisk	Hitachi 5400 RPM 160 GB	Sandisk SSD PLUS 240 GB
Hafıza	4 GB (2+2 GB SODIMM) 667 MHz	32 GB (16+16 GB) DIMM 2667 MHz

Test-1 ve Test-2 sunucuları, hazırlanan web uygulamasını barındırmak için Windows IIS kurulumları tamamlanmış ve ana modemden ilgili port yönlendirmeleri yapılmıştır. Test-1 sunucusunun donanım özelliklerinden anlaşılacağı gibi, günümüz teknolojisine göre oldukça eski bir donanıma sahip olan basit seviyedeki sunucular ile bu işlemler pratik bir şekilde gerçekleştirilebilmektedir. Günümüzde işletmeler yerel ortamda bulunan ölçeklendirilebilir sanal sunucular kullanarak daha performanslı yapılar ayağa kaldırabilmektedir. Bu durumu değerlendirmek için hazırlanan Test-2 sunucusu ile yapılan testlerin sonucuna Tablo 20'da yer verilmiştir. Test sunucularının işletim sistemi, veritabanı ve IIS ayarları varsayılan kurulum ayarları ile kullanılmış ve herhangi bir performans düzenlemesi yapılmamıştır.

Tablo 20. Farklı şifreleme algoritmalarının aktarım süreleri

Şifreleme Algoritması	Sunucu -1 Aktarım Süresi (sn)	Sunucu -2 Aktarım Süresi (sn)
DES	350	410
3DES	389	422
AES	78	28
RC	89	27
Blowfish	77	27

Tablo 20'de görüldüğü üzere şifreleme algoritmaları arasındaki farklardan yola çıkarak, geliştirme sürecinde farklı sunucularda en iyi performans gösteren Blowfish algoritması kullanılmıştır. Entegrasyon sürecinde en hızlı algoritmanın seçilmesinin temel sebebi ise uygulanacak olan yapının uzun vadede çoklu veri aktarımlarını karşılayabilir düzeyde olmasını sağlamaktır. Böylece sistem geçişlerinde, faaliyet alanı değişimi ile farklı kısıtlamalara tabi olunması durumunda olası bir kısıtlama dışı faaliyette bulunma süresi aktarım hızı arttığından en aza indirgenmiş olacaktır.

4.5 Önerilen Kullanım Senaryoları

Otomasyon süreçlerinin şifrelenmiş veriler ile kullanım pratiğini anlamak, bu çalışmanın temelinde kullanılan verilerin şifrelenmesi ve görüntülenmesi konusunu detaylıca anlamayı gerektirir. Böylece kullanılacak otomasyon süreçlerinde ihtiyaç duyulan hassas veri uygun yöntemlerle işlenip, crm uygulamasının sunduğu otomasyon süreçlerine dahil edilerek gizlilik ihlali olmadan güvenli bir şekilde sürece katılımı sağlanabilecektir.

4.5.1 Otomatik doğum günü tebriği maili gönderimi

CRM uygulaması üzerinde yer alan doğum günü ve e-posta bilgilerinin hassas veri olarak işlendiği ve lokal ortamda şifreli olarak saklandığı senaryoda CRM sisteminin mevcut

araçları ile günlük otomatik tebrik maili atması mümkün olmayacaktır. Bu sebeple kurulacak otomasyon sisteminde otomasyonu kuracak kişinin bilgi güvenliği süreçlerine hakim olması ve otomasyon araçlarını çok iyi tanıması gerekmektedir. Böylece otomasyon kurulumu yapılırken kullanılacak bilgilerin ilgili web servislerden istenmesi ve sürece dahil edilmesi sağlanabilecektir.

4.5.2 Kampanya e-posta gönderimi

CRM araçlarının en önemli kullanım alanlarından bir tanesi de kullanıcı segmentasyonu ile uygun kampanya üretimidir. Bu aşamada kullanıcının hassas veri içermeyen davranış geçmişini analiz ederek uygun fiyatlama ile kişiye özel oluşturulan kampanyanın sms veya e-posta ile müşteriye iletilmesi gerekmektedir. Yine burada telefon numarası ve e-posta adresi kişisel bilgi olarak nitelendirildiğinden doğrudan nihai tüketiciye ulaşmak mümkün olmayacaktır. Bu durumda kampanya süreci kurgusunun arkasında çalışacak e-posta veya sms gönderim sürecinin ihtiyaç duyduğu iletişim bilgisinin kullanılabilmesi için lokal ortamla haberleşen yapının otomasyona dahil edilmesi gerekmektedir.

4.5.3 Servis durumu bilgilendirmesi

Müşterinin arızalı ürünü firmaya göndermesi ile başlayan sürecin müşteri tarafından tüm aşamalarının haberdar olmasını sağlamak için kurulan otomasyonlarda kullanıcıya tercihince bilgilendirme iletileri gönderilebilir (sms veya mail). Bu süreç için diğer örneklerde olduğu gibi kurulacak otomasyonlarda sistem arıza kaydına tanımlı tekil kişi bilgisi ile lokal sistemden kişinin iletişim bilgisini okuyup bulut sistem üzerinde herhangi bir kişisel bilgi tutmadan gönderimin yapılmasını sağlayabilir.

5. BULGULAR VE TARTIŞMA

Bu bölümde çalışmaya konu gizlilik durumun sürdürülebilmesine ve gizlilik için önerilen çözümün kullanılabilirliğinin değerlendirilmesine yer verilmiştir. Bu çalışmada yerel ve uluslararası kısıtlamalar değerlendirilmiş olup kısıtlama alanında kullanılabilecek bir çalışma önerilmiş ve gerçekleştirilmiştir.

5.1 Bulgular

Bu çalışmada ülkemizde ve dünyada veri güvenliği/gizliliği ile ilgili yapılan araştırmalar incelenmiş olup dünyada uygulanan yöntemlerin ülkemizde de benzer şekilde uygulanmaya çalışıldığı gözlemlenmiştir. Bunun için ortaya çıkan KVKK ile korunmayı amaçlayan süreç uluslararası yazılımlar tarafından yeterince desteklenmediği bulgusuna varılmıştır. Bu sürecin çözümü için hazırlanan uygulamada çözüm bulguyu kapatacak şekilde başarı ile uygulanmıştır. Uygulama bölümünde yer verilen çalışmada belirtildiği gibi yerel sistem üzerinde kurulan bir yazılım ile bulut sistem üzerinde saklanan verilerin yerel ortamda saklanabileceği ve iş süreçlerine dahil edilebileceği gözlemlenmiştir. Ayrıca test ortamında farklı donanım özelliklerine sahip sunucularla yapılan testlerde donanım farklılıklarının performansa olan etkisi belirtilmiştir. Böylece işletmelerin bunun gibi altyapılar kurarken ihtiyaçlarına yönelik, daha iyi performans sunacak donanım konfigürasyonu belirleyebilmesi sağlanmıştır.

Yine bu çalışma içerisinde örneklerle detaylı bir şekilde açıklanmaya çalışan entegre etme yöntemlerine değinerek tespit edilen bulguya çözümler üretilmiştir.

Bir diğer bulgu ise, uygulanan çözümün performans durumudur. Yapılan çözüm ile bir müşteriye ait verilerin tekil sorgulanması yerine toplu olarak sorgulanması sağlanarak, kısıtlı sayıda kişisel veri olarak nitelendirilebilecek verilerin ağ katmanı üzerinde taşınması sağlanmıştır. Böylece tekil kayıt sorgulamalarında istemci ve sunucu arasında açılacak ağ bağlantısı sayısı bire düşürülüp zaman kaybı önlenmiştir.

5.2 Tartışma

Bu çalışmada verilerin bulut tabanlı ortamlarda saklanmasının ülkemizde uygulanan kısıtlamalara uygunluğu araştırılmış ve buna uygunluğu sağlamak adına bir uygulama hazırlanmıştır. Örnek çıktılarda verinin farklı algoritmalarla saklanabilmesi değerlendirilip uygun çözümler getirilmiştir.

Elde edilen çıktılar ışığında verinin bulut ortamda tutulmaması KVKK'ya göre kişisel bilgi taşıyan verinin yurtdışında saklanmaması için alternatif bir önlem oluşturulmuştur. Yurt içerisinde bulunan sunucularda saklanacak verinin bulut tabanlı uygulama ile haberleşmesi için oluşturulan uygulama ile verinin güvenli ve performanslı bir şekilde saklanması başarıyla tamamlanmıştır.

Literatürde yapılan çalışmalar incelendiğinde, Odun ve arkadaşlarının yaptığı IBM ve Amazon bulut depolama karşılaştırmaları ele alınmış, buradan çıkan sonuçlar neticesinde bulut sistemlerin kullanımının artmasıyla beraber bu alanda yapılacak güvenlik ve gizlilik çalışmalarının devam etmesi gerektiğine vurgu yapılmıştır (Odun-Ayo, Ajayi, Akanle ve Ahuja, 2017). Bu tez çalışmasında hazırlanan uygulamaya farklı işlevler eklenerek üzerinde çalışmalar yapılmaya devam edilmelidir. Böylece gelişen teknolojinin sağlayacağı güvenlik ve performans faydalarından maksimum seviyede verim alınmaya devam edilebilir.

Shi, herkese açık bulut ortamlarda veri güvenliği ve gizliliği ile ilgili yaptığı çalışmada bu tez çalışmasından farklı olarak veriyi yerel ortamda kullanmak için tekil bir web servis yerine dağıtık mimaride bir çalışma önermiştir (Shi, 2018). Burada vardığı sonuçta ise önbellekleme ve ölçeklendirme süreçlerinde yaşanan sorunların önüne geçilmesi gerektiğini belirtmiştir. Hesaplamaların bulut ortamda yapıldığını belirtmiş ve bunun yerel ortamda yapılabileceğinden bahsetmiş. Bu tez çalışmasında, burada belirtildiği gibi bir yaklaşımda bulunularak şifreleme işlemi yerel sunucu üzerinde yapılmıştır. Böylece bulut sistem üzerinde yaşanabilecek performans sorunlarının önüne geçilerek yerel sistem donanım gücünden faydalanılmıştır.

Çalışma sırasında elde edilen bilgiler ışığında verilerin yurtiçi sunuculardaşifreli bir şekilde saklanması, saklanan verinin yetkili kişilerce şifresinin çözülerek

görüntülenebilmesi süreci son kullanıcı tarafından kabul edilebilir bir gecikme ile gösterilebilmiştir. Ancak bulut tabanlı hazır sistemlerin kullanıcılarına sunduğu araçlardan faydalanma aşamasında ekstra bir yük oluşturmuştur. Yapılan bu çalışmanın işletme içerisinde akıcı ve fayda sağlar bir şekilde kullanılabilmesi için, uygulamanın sunmuş olduğu veri görüntüleme servislerinin, bulut sistem araçları ile bütünleşmiş hale getirilmesi zorunluluğunu bulundurmaktadır.

6. SONUÇ ve ÖNERİLER

Yapılan bu çalışmanın içeriğinde tamamlanan uygulama ile kişisel veri güvenliğini ve mahremiyetini ön planda tutan süreçler işletmelere yol gösteren bir kılavuz oluşturulmuştur. Böylece uluslararası popüler uygulamalar kullanılırken işletmeler bu çalışmada belirtilen yöntemleri uygulayarak yaşanabilecek olumsuzlukları azaltmaya yönelik önlem almış olacaklar.

Şifreleme sürecinde karşılaşılan bir diğer durum ise, sahip olunan bilgi ile gerçek kişiye ulaşmayı sağlayan veri parçalarının içerikleri göz önünde bulundurulduğunda uygulanacak şifreleme yönteminin performansında gözle görülür bir değişiklik gözlemlenmemiştir. Ancak sistemin ilk kez hayata geçirilmesi sürecinde veri göçü olarak adlandırılan (data migration) süreç toplu olarak bulut sistemde sahip olunan kişisel verinin şifrelenerek saklanmasını gerektirmektedir.

Bu sürecin hızlı bir şekilde uygulanabilmesi için çalışma içerisinde farklı parametrelerle veri aktarımı denemeleri yapılarak optimum aktarım süresine ulaşılabilecek parametreler belirlenmiştir. Çalışmada belirlenen kişisel bilgi alanları işletmelerin topladığı bilgiye göre farklılık gösterebilir. Bu durumda sistem yöneticilerinin benzer yöntemlerle testlerini yapıp olabilecek en mantıklı aktarım süresini belirlemesi gerekmektedir. Uygulanan uyarlamada temel anlamda, şifreleme ile ilgilenmiş herkesin aklına gelebilecek şifreleme algoritmaları kullanılmıştır. Yapılan bu çalışmada gerek kullanılan şifreleme yöntemi gerekse kullanılan yerel sunucu yapısı uygulayan işletmeler tarafından daha iyi sonuçlar verecek şekilde iyileştirilebilir. Her geçen gün mevcut algoritmalar güvenilirliğini veya geçerliliğini yitirirken, araştırmacılar diğer yandan bu algoritmaları daha güçlü hale getirmek ve yeni algoritmalar üretmek için çalışmalarına devam etmektedir.

Ülkemizde veri işleme sürecine sahip olan işletmelerin bulut tabanlı uluslararası uygulamalar kullanırken özellikle dikkat etmesi gereken konular bu çalışmanın giriş bölümünde değerlendirilmiştir. Burada kesinlikle göz ardı gereken konu bulut tabanlı sistemler kullanılırken uygulama üzerinde saklanacak verinin niteliğinin belirlenmesi. Veri niteliği belirlendikten sonra çalışmada belirtilen yöntem ile KVKK uyumlu bir

kullanım uygulanacağı aşamada veri yükü hesaplanmalı ve yerel ortamda kurulacak sunucu kapasiteleri bu ihtiyaçları karşılayacak düzeyde belirlenmelidir.

KAYNAKLAR

Adejo, O., Ewuzie, I., Usoro, A. ve Connolly, T. (2018). E-Learning to m-Learning: Framework for Data Protection and Security in Cloud Infrastructure. *International Journal of Information Technology and Computer Science*.

Ahmed, K. ve El-Henawy, I. (2017). Increasing robustness of data encryption standard by integrating DNA cryptography. *International Journal of Computers and Applications*. doi:10.1080/1206212x.2017.1289690

Altan Akın, N. (2014). Bulut Bilişim'de Kişisel Verilerin Güvenliği ve Mahremiyet Nasıl Sağlanabilir? *XIX. Türkiye'de İnternet Konferansı.* İzmir.

Arshad, M., Umair, M., Munawar, S., Naveed, N. ve Naeem, H. (2020). Improving Cloud Data Encryption Using Customized Genetic Algorithm. *International Journal of Intelligent Systems and Applications*. doi:10.5815/ijisa.2020.06.04

Aydın, Ö. (2022). *Bilgisayar Sistemlerinde Güvenlik Ve Gizlilik.* İstanbul: Efe Akademi Yayınları.

Barta, G., Ludvai, N. ve Puskás, A. (2020). The analysis of data privacy incidents and sanctions in Europe after GDPR. *Internatıonal Winter Conference of Economics Phd Students and Researchers,* 35-48.

Bohn, R. ve Messina, J. (2011). NIST Cloud Computing Reference Architecture. *2011 IEEE World Congress on Services*.

C.-W.Phan, R. (2007). Reducing the exhaustive key search of the Data Encryption Standard (DES). *Computer Standards & Interfaces*. doi:10.1016/j.csi.2006.11.010

Canbay, Y., Sağıroğlu, Ş. ve Vural, Y. (2022). A New Anonymization Model for Privacy Preserving Data Publishing: CANON. *Balkan Journal of Electrical and Computer*

Engineering, *10*(3), 307-316. https://doi.org/10.17694/bajece.1061910 adresinden alındı

Cao, F., Huang, H. ve Zhou, X. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics*. https://doi.org/10.1016/s0895-6111(02)00073-3 adresinden alındı

Chen, D. ve Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *012 International Conference on Computer Science and Electronics Engineering*.

Cody, B., Madigan, J., MacDonald, S. ve Hsu, K. (2007). High Speed SOC Design for Blowfish Cryptographic Algorithm. *2007 IFIP International Conference on Very Large Scale Integration*, 284-287.

Utami, H. D. J. R. H., Arifudin, R. ve Alamsyah, A. (2020). Security Login System on Mobile Application with Implementation of Advanced Encryption Standard (AES) using 3 Keys Variation 128-bit, 192-bit, and 256-bit. *Scientific Journal of Informatics*. doi:10.15294/sji.v6i1.17589

Durkin, P. (2012). Can PCI DSS compliance be achieved in a cloud environment? *University of London*.

Ertekin, İ. (2022). Kamu Yönetimi Ve Halkla İlişkiler Yönüyle Kişisel Verilerin Korunması Kanunu (KVKK). *Ombudsman Akademik*, 39-67.

Force, J. T. ve Initiative, T. (2010). Guide for applying the risk management framework to federal information systems. *NIST special publication*.

GDPR. (2016, Mayıs 4). *General Data Protection Regulation.* Şubat 11,2023 tarihinde https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 adresinden alındı

Gnatyuk, S., Kinzeryavyy, V., Iavich, M., Prysiazhnyi, D. ve Yubuzova, K. (2018). High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks. *Proceedings of the 14th International*

Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, 657-668.

Günden, Ü. (2010). Şifreleme algoritmalarının performans analizi. (Yayın no. 274765) Yüksek Lisans Tezi / *Sakarya Üniversitesi*. https://acikerisim.sakarya.edu.tr/handle/20.500.12619/80357 adresinden alındı

Hogan, M., Liu, F., Sokol, A. ve Tong, J. (2011). Nist cloud computing standards roadmap. *Special Publication 500-291*.

Hossain, A., Hossain, B., Uddin, S. ve Imtiaz, S. (2016). Performance analysis of different cryptography algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*.

J.Shepherd, S. (1995). A high speed software implementation of the Data Encryption Standard. *Computers & Security*. http://dx.doi.org/10.1016/0167-4048(95)00007-u adresinden alındı

Kahrobaei, D., Najarian, K., Shpilrain, V. ve Wood, A. (2019). Private naive bayes classification of personal biomedical data: Application in cancer data analysis. *Computers in Biology and Medicine*. https://doi.org/10.1016/j.compbiomed.2018.11.018 adresinden alındı

Kitsos, P., Goudevenos, S. ve Koufopavlou, O. (2003). VLSI implementations of the triple-DES block cipher. *10th IEEE International Conference on Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003*. doi:10.1109/icecs.2003.1301980

Kumar, G., Saha, R. ve Rai, M. (2012). DSAB – A Hybrid Approach for Providing Security in MANET. *International Journal of Information Security Science*.

KVKK. (2016, Nisan 7). *Kişisel Verilerin Korunması Kanunu (Sayı: 26530)* . Şubat 11,2023 tarihinde https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf adresinden alındı

Li, N., Li, T. ve Venkatasubramanian, S. (2006). t-Closeness: Privacy Beyond k-Anonymity and l-Diversity. *2007 IEEE 23rd international conference on data engineering*, 106-115.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. ve Leaf, D. (2011). NIST Cloud Computing Reference Architecture. *NIST Special Publication*.

Loukides, G. ve Shao, J.-H. (2008). An Efficient Clustering Algorithm for k-Anonymisation. *Journal of Computer Science and Technology*.

Luna, J., Suri, N., Iorga, M. ve Anil, K. (2015). Leveraging the potential of cloud security service-level agreements through standards. *IEEE Cloud Computing*, *2*(3), 32-40.

Machanavajjhala, A., Gehrke, J., Kifer, D. ve Venkitasubramaniam, M. (2006). L-diversity: privacy beyond k-anonymity. *22nd International Conference on Data Engineering (ICDE'06)*.

Majeed, A. ve Lee, S. (2021). Anonymization Techniques for Privacy Preserving Data Publishing: A Comprehensive Survey. *IEEE Access (Volume:9)*, 8512-8545.

Marttin, V. ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme. *Mühendislik Bilimleri ve Tasarım Dergisi*, 49-56.

Mell, P. ve Grance, T. (2011). The NIST Definition of Cloud Computing. *NIST Special Publication 800-145*.

Mowbray, M. ve Pearson, S. (2009). A client-based privacy manager for cloud computing. *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE*.

Odun-Ayo, I., Ajayi, O., Akanle, B. ve Ahuja, R. (2017). An Overview of Data Storage in Cloud Computing. *2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS)*, 29-34.

Özdiker, O. (2018). KVKK ve GDPR Hakkında Bilinmesi Gerekenler. *Bursa Barosu Dergisi*, 83-86.

Padmavathi, M., Sirisha, D. ve Lakshman, R. (2014). he Security of Cloud Computing System Enabled by Shamir's Secret Sharing Algorithm. *International Journal of Research Studies in Science, Engineering and Technology*, 103-109.

Paşaoğlu, C. ve Cevheroğlu, E. (2020). Bulut Bilişim Sistemleri Kapsamında Kişisel Verilerin Şifreleme Yöntemleri ile Korunması. *Bilişim Teknolojileri Dergisi, 13*(2), 183-195. doi:10.17671/gazibtd.559235

Paşaoğlu, C. ve Vural, Y. (2018). Dünyada ve Türkiye'de Kişisel Verilerin Korunması. *Siber Güvenlik ve Savunma Farkındalık Caydırıcılık*, 282-309.

Pearson, S., Shen, Y. ve Mowbray, M. (2009). A Privacy Manager for Cloud Computing. *Lecture Notes in Computer Science*.

Petkovic, I. (2010). CRM in the cloud. *IEEE 8th International Symposium on Intelligent Systems and Informatics*. doi:10.1109/sisy.2010.5647402

Rajani, S. ve Vijay, R. (2017). Secure online encryption with partial data identity outsourcing: An exemplar for cloud computing. *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)*. doi:10.1109/wocn.2017.8065841

Rao, R. ve Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. *Procedia Computer Science*, 204-209.

Sajjan, R. ve Ghorpade, V. (2017). Secure online encryption with partial data identity outsourcing: An exemplar for cloud computing. *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)*.

Sahinaslan, E., Sahinaslan, O. (2019). Cryptographic methods and development stages used throughout history. *AIP Conf. Proc.* 2 April 2019; 2086 (1): 030033. https://doi.org/10.1063/1.5095118

Sahinaslan, O., Sahinaslan, E. (2019). Cross-object information security: A study on new generation encryption. *AIP Conf. Proc.* 2 April 2019; 2086 (1): 030034. https://doi.org/10.1063/1.5095119

Savaş, R. N., Zaim, A. H. ve Aydın, M. A. (2020). KVKK ve GDRP Kapsamında Firmaların Mevcut Durum Analizi Üzerine Bir İnceleme. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 19*(38), 208-223.

Shaqrah, A. (2016). Cloud CRM: State-of-the-art and security challenges. *International Journal of Advanced Computer Science and Applications 7.4*.

Sharma, Y., Himanshu, G. ve Khatri, S. (2019). A Security Model for the Enhancement of Data Privacy in Cloud Computing. *2019 Amity International Conference on Artificial Intelligence (AICAI)*, 898-902.

Shi, Y. (2018). Data Security and Privacy Protection. *2018 IEEE International Conference on Big Data (Big Data)*, 4812-4819.

Shuaib, M., Alam, S., Alam, M. S. ve Nasir, M. S. (2021). Compliance with HIPAA and GDPR in blockchain-based electronic health record. *Materials Today: Proceedings*. http://dx.doi.org/10.1016/j.matpr.2021.03.059 adresinden alındı

Soni, R., Ambalkar, S. ve Bansal, P. (2016). Security and privacy in cloud computing. *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*.

Souri, A., Asghari, P. ve Rezaei, R. (2017). Software as a Service based CRM Providers in the Cloud Computing: Challenges and Technical Issues. *Journal of Service Science Research*.

Srinivasan, S. (2014). Cloud Computing Security. *Cloud Computing Basics*, 81-100.

Sun, Y., Zhang, J., Xiong, Y. ve Zhu, G. (2014). Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*.

Şahinaslan, Ö. (2013). Siber Saldırılara Karşı kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma (Yayın no. 307648), Doktora Tezi / Trakya Üniversitesi Fen Bilimleri Üniversitesi, s. 29.

Şahinaslan, E. ve Şahinaslan, Ö. (2022). Microsoft SQL Sunucusunda Veritabanı Kurtarma Teknikleri. *International Journal of Innovative Engineering Applications, 6* (1) , 158-169. DOI: 10.46460/ijiea.1070325

Şahinaslan, E., Köksal, A. ve Şahinaslan, Ö. (2023). A Study on Remote Detection of Turkey Digital Identity Card Hologram Element. *Politeknik Dergisi*, 26 (4), 1-1 . DOI: 10.2339/politeknik.1167225

Tariq, M. ve Santarcangelo, V. (2016). Analysis of ISO 27001: 2013 Controls Effectiveness for Cloud Computing. *ICISSP*, 201-208.

Voss, W. ve Houser, K. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal*.

Vural, Y. (2017). p-kazanım: Mahremiyet korumalı fayda temelli veri yayınlama modeli. (Yayın no. 478487) Doktora Tezi / Hacettepe Üniversitesi https://tez.yok.gov.tr/UlusalTezMerkezi/tezDetay.jsp?id=Dm0oBiLE8VQPEAI8IiEVUQ&no=5aRS3SxIRfBprk2Rt04n3g adresinden alındı

Wang, E. K., Jia, B. ve Ke, N. (2017). Modeling Background Knowledge for Privacy Preserving Medical Data Publishing. *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*.

Wang, Q., Wu, L., Chen, Y. ve Li, L. (2022). A Data Masking Method Based on Genetic Algorithm. *2022 2nd Asia Conference on Information Engineering*, 13-17.

Yalçınkaya, B. ve Diri, N. (2022). Blokzincir Uygulamalarında Kişisel Veri Problemi: Depolama Riskleri ve Öneriler. *Bilgi Yönetimi*. 5(1), 47-67.

Yao-Hua, G. (2014). Application of the Information Encryption Technology in the Industrial Control Network Based on FPGA. *Sensors & Transducers*(175), 226-233.

Yılmaz, T., Arıkan, S. M., Su, F. ve Yurekten, O. (2020, Ekim). Protecting Personal Information in Enterprise Applications. 2020 Turkish National Software Engineering Symposium (UYMS). İstanbul.

Zhou, Z. ve Liu, B. (2005). HIPAA compliant auditing system for medical images. *Computerized Medical Imaging and Graphics*. doi:10.1016/j.compmedimag.2004.09.009

ÖZGEÇMİŞ

Ziya Can KALKAVAN

Eğitim

Derece	Yıl	Üniversite, Enstitü, Anabilim/Anasanat Dalı
Lisans	2015	Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği

İş/İstihdam (Varsa)

Yıl	Görev
2015-2018	Microsoft Teknolojileri Danışmanı
2018-2020	Kıdemli Danışman
2020-	Yazılım Geliştirme Takım Lideri

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

"A Modern Approach to Data Privacy with Federated Learning", 7th International Conference of Mathematical Sciences (ICMS 2023)