Bulut Şifreleme Teknikleri ile Kişisel Verilerin Korunması

ADNAN GÖKMEN

İçerik

- Kişisel Veri Nedir?
- Kişisel Verilerin Korunması
- Bulut Bilişim Sistemleri (Cloud Computing Systems)
- Bulut Bilişim Sistemlerinin Avantajları Nelerdir?
- Bulut Bilişim Sistemlerinin Dezavantajları Nelerdir?
- Bulut Bilişimin Sınıflandırılması (Classification of Cloud Computing)
- Bulut Bilişim Sistemlerinde Veri Mahremiyeti
- Bulut Bilişimde Mahremiyet Riskleri (Privacy Risks in Cloud Computing)
- Şifreleme Yöntemleri (Encryption Methods)

Kişisel Veri Nedir?

- Kişisel veri, bir kişiyi doğrudan veya dolaylı yollardan tanımlayan veya başka verilerle eşleştirildiğinde tanımlayabilecek potansiyelde olan yani veri üzerinden kişinin bulunmasına olanak veren verilerdir.

Kişisel Verilerin Korunması

- Bulut bilişim sistemlerinin yaygınlaşmasından önce veriler dâhili depolama birimlerinde veya manyetik bant, disket sürücü, mini disk, taşınabilir bellek, CD/DVD gibi harici depolama birimlerinde tutulmaktaydılar.

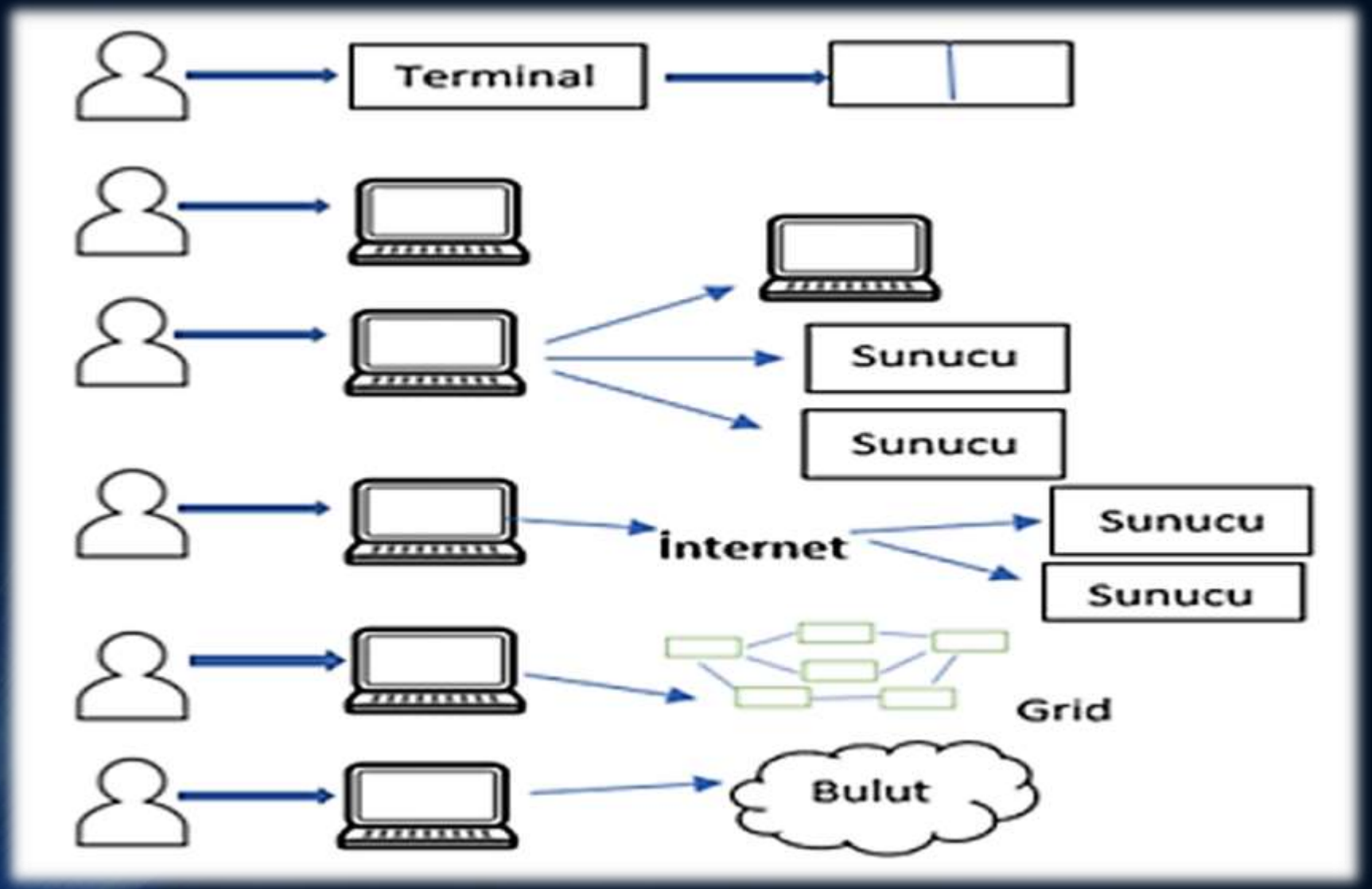
Kişisel Verilerin Korunması

- Bulut bilişimin yaygınlaşmasından sonra ise bahsi geçen depolama birimlerinin kullanımı azaldı ve herhangi bir fiziksel materyale ihtiyaç duyulmadan verilere internet ortamı üzerinden kolayca ulaşılabilir duruma gelindi.

Bulut Bilişim Sistemleri (Cloud Computin Systems)

- Bulut bilişim internet bağlantısıyla erişim sağlanabilen, uzak sunucu desteğiyle beraber verilerin saklanmasını, işlenmesini ve verilere her an erişim sağlanarak kullanılmasını sağlayan bir servistir.

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



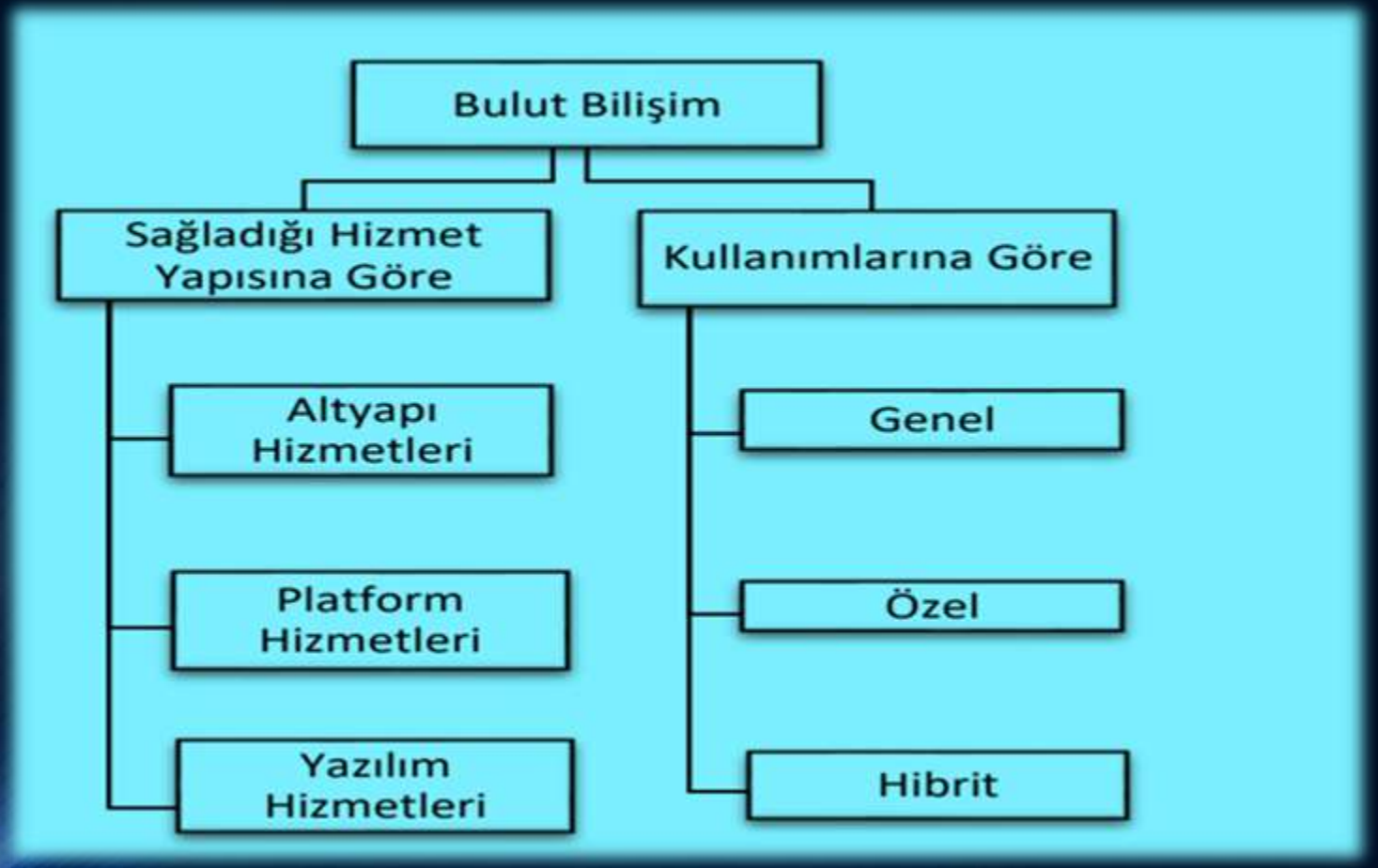
Bulut Bilişim Sistemlerinin Avantajları Nelerdir?

- Kullandığın kadar öde sistemi
- Kapasitenin ihtiyaçlar doğrultusunda azaltılıp arttırılabilmesi
- Platform bağımsız
- Bakım, yedekleme ve lisanslama maliyetleri yoktur
- Yama ve güvenlik yönetimine ihtiyaç yoktur
- İnternet olan her cihazdan veriye erişim imkanı
- Yüksek erişilebilir olma ve kesintisiz hizmet alma ve sağlama imkanı

Peki ya! Bulut Bilişim Sistemlerinin Dezavantajları Nelerdir?

- Ülkemiz için internet bant genişliği
- İnternet hızı
- Veri güvenliği ve gizliliği
- Fiziksel alan ve çalışan personel güvenliği
- Yasal uyumluluk
- Hizmet sağlayıcı bağımlılığı

Bulut Bilişimin Sınıflandırılması (Classification of Cloud Computing)



Sağladığı Hizmetlere Göre (According to the Services)

A) ALTYAPI HİZMETLERİ (INFRASTRUCTURE SERVİCES)

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

Sağladığı Hizmetlere Göre (According to the Services)

B) PLATFORM HİZMETLERİ (PLATFORM SERVİCES)

- Platform hizmetleri kullanıcılara programlama ve bu programları yürütme imkânı sağlar. Kullanıcı desteklenen programlama dilleri, yazılım kütüphaneleri ve araçlar kullanarak kendi uygulamalarını geliştirebilmekte ve bunu kolaylıkla bulut altyapısına dağıtabilmektedir.

Sağladığı Hizmetlere Göre (According to the Services)

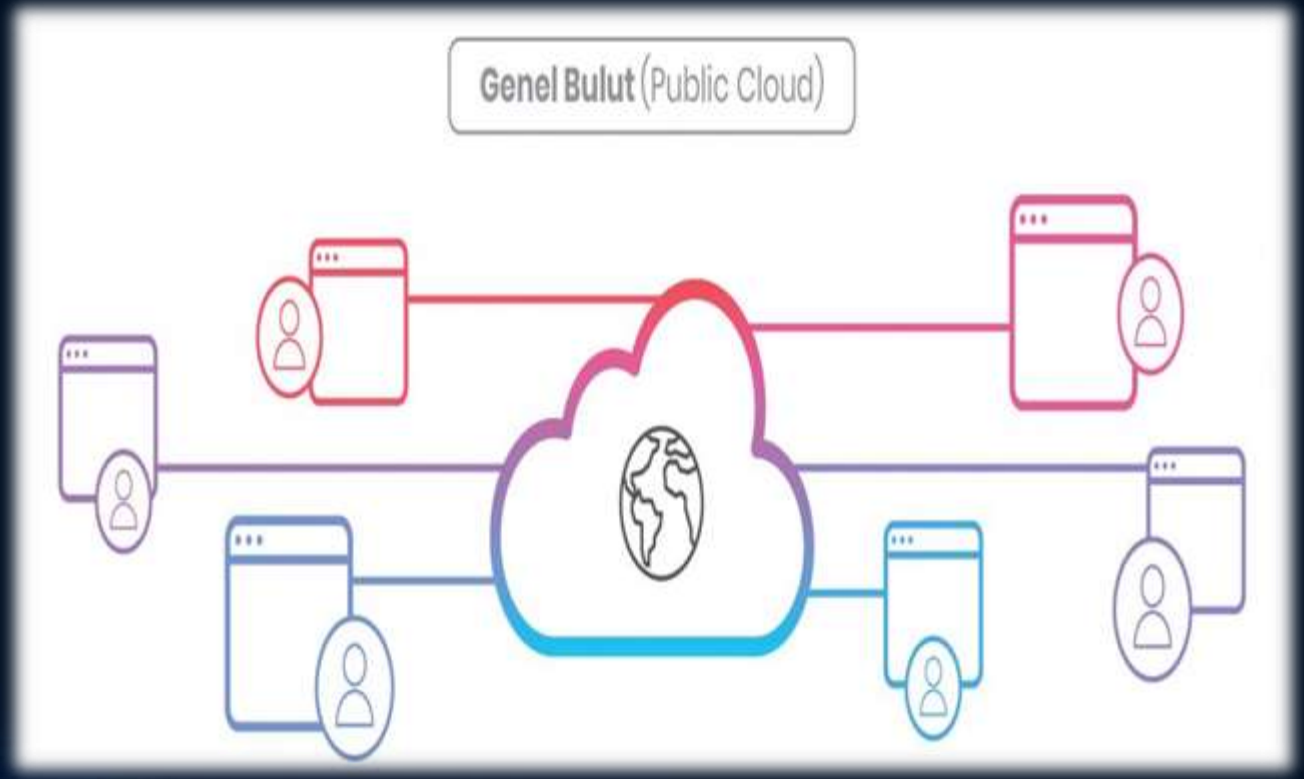
C) YAZILIM HİZMETLERİ (SOFTWARE SERVİCES)

- Bu hizmet kapsamında kullanıcıların yazılımları veya uygulamaları bulutta servis olarak bulundurulur ve kullanıcılar bu yazılım hizmetlerine abonelik açtıklarında tarayıcılar aracılığıyla ulaşırlar.

Kullanım Şekline Göre (According to the way of use)

A) GENEL BULUT (PUBLIC CLOUD)

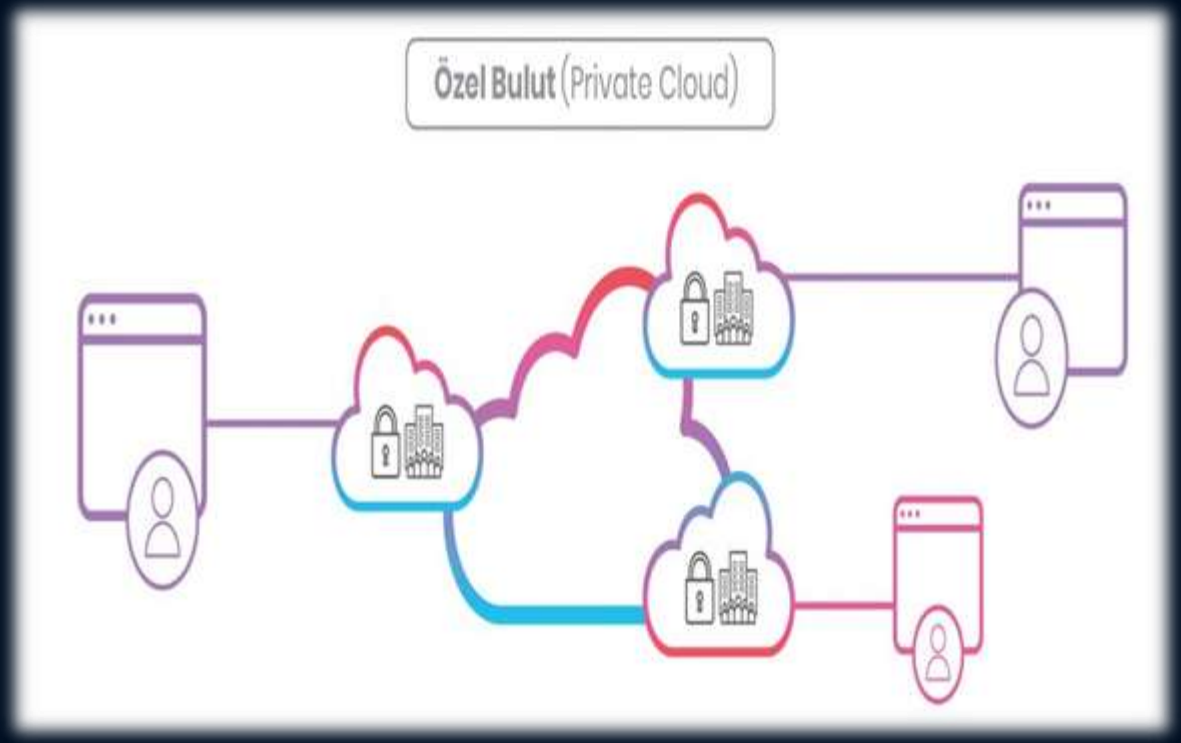
- Genel bulutta kullanıcı sınırlaması yoktur. Bünyesinde bulunan hizmetler sanallaştırılmış bir ortamda toplanmıştır ve internet üzerinden erişilebilirler. Genel bulut servislerine servis olarak yazılım (Saas), bulut tabanlı web barındırma (IaaS) ve yazılım geliştirme ortamları (PaaS) örnek olarak verilebilir.



Kullanım Şekline Göre (According to the way of use)

B) ÖZEL BULUT (PRIVATE CLOUD)

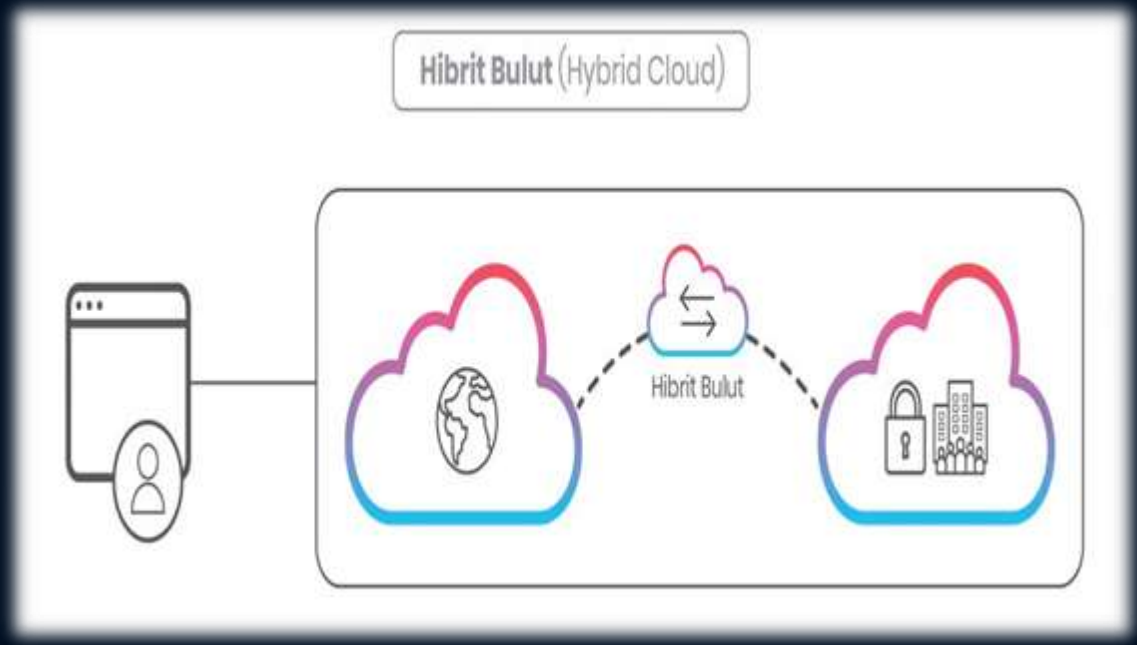
- Belirli bir kurum veya kuruluş için oluşturulmuş olan bu bulutta hizmet sağlayıcı kurumun kendisi olabilir veya üçüncü bir bulut hizmet sağlayıcısından da hizmet satın alınabilir.

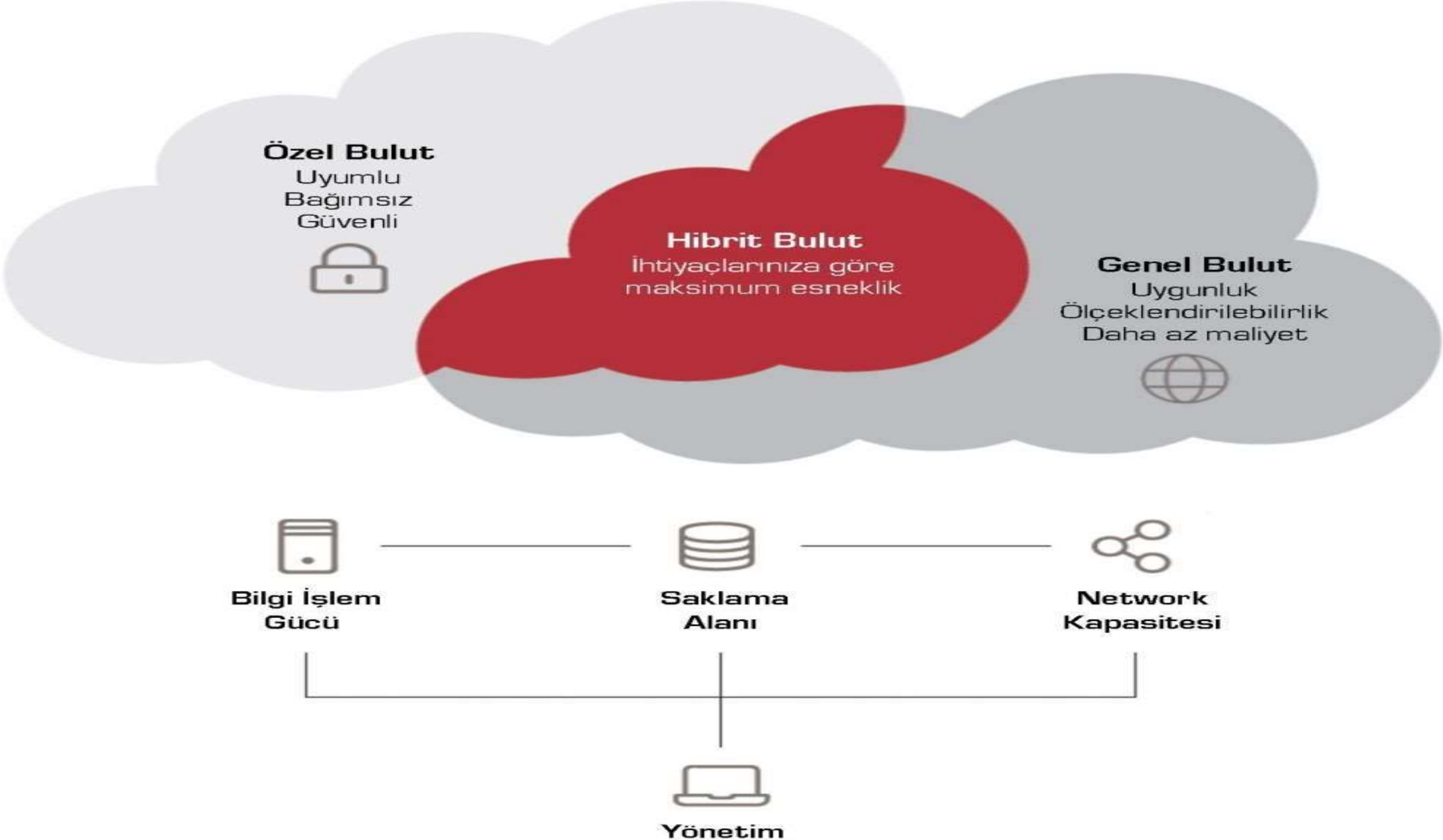


Kullanım Şekline Göre (According to the way of use)

C) HİBRİT BULUT (HYBRID CLOUD)

- İki veya daha fazla bulut çeşidinin birleştirilmiş yapısıdır. Hibrit bulutun avantajı olarak önemli veriler özel bulutta tutulurken, aynı anda daha az kritik veriler genel bulutta tutulabilmektedir.

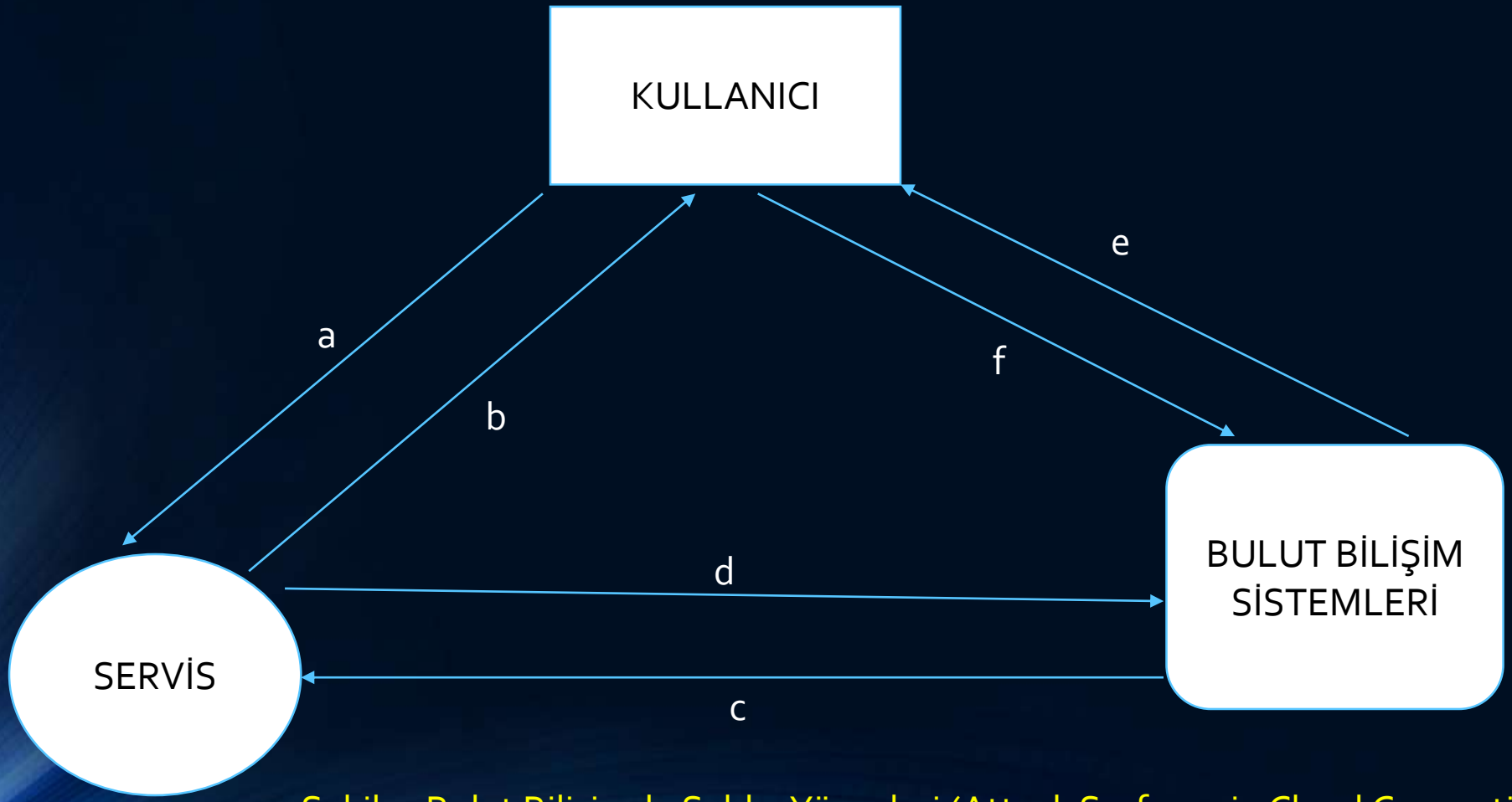



Özel Bulut
Uyumlu
Bağımsız
Güvenli
Hibrit Bulut
İhtiyaçlarınıza göre
maksimum esneklik
Genel Bulut
Uygunluk
Ölçeklendirilebilirlik
Daha az maliyet
Bilgi İşlem
Gücü
Saklama
Alanı
Network
Kapasitesi
Yönetim

Bulut Bilişim Sistemlerinde Veri Mahremiyeti (Data Privacy In Cloud Computing Systems)

- Şüphesiz bilginin elektronik ortamlarda işlenebilir, saklanabilir hale gelmesi insan hayatını kolaylaştırmıştır. Veri adı verilen elektronik ortamda işlenebilir ve saklanabilir bu bilgi türü, hayatlarımızda birçok kolaylık sağlarken bir takım sorunları da beraberinde getirmiştir. Özellikle son zamanlarda verinin kolay saklanabilir olması ile de ilgili olan artan özçekim miktarları, her anı fotoğraflama, kameraya alma ve saklama gibi isteklerin çoğalması kişisel bilgisayarların bellek miktarlarını yetersiz bırakmaktadır.

Bulut Bilişimde Mahremiyet Riskleri (Privacy Risks in Cloud Computing)



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

Şifreleme Yöntemleri (Encryption Methods)

- Bulut bilişim sistemleri kullanırken, yüklemiş olduğumuz kişisel verilerin gizliliği ve üçüncü kişiler tarafından anılan verileri ele geçirme ya da verilere hukuka aykırı olarak erişim hususları düşünüldüğünde, bu tür durumları önlemek adına alınması gereken önlemlerin başında şifreleme işlemleri gelmektedir.

Şifreleme Yöntemleri (Encryption Methods)

HOMOMORFİK (EŞ BİÇİMLİ) ŞİFRELEME (HOMOMORPHİC ENCRYPTİON)

Homomorfik şifreleme, karşı tarafa gönderilmek istenilen metinler üzerinde yapılan cebirsel işlemler ile şifreleme işlemleri sonucunda oluşan yeni şifreli sonucun şifresi çözüldüğünde oluşan sonuç ile aynı cebirsel işlemlerin açık metinlerde yapılmasıyla elde edilen sonucun, aynı olmasını sağlayan bir şifreleme tekniğidir.

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

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

a) Paillier

1999 yılında Pascal Paillier tarafından bulunarak onun adının verildiği olasılığa dayanan bir açık anahtar algoritmasıdır.

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

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

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

b) Goldwasser-Micali

1982 yılında Shafi Goldwasser ve Silvio Micali tarafından geliştirilen asimetrik bir anahtar şifreleme algoritmasıdır.

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

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

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

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

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

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

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

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

c) RSA Algoritması (RSA Algorithm)

Mesajların şifreli formatları üzerinde işlemlerin gerçekleştirilmesi düşüncesi Rivest, Adleman ve Derouzous tarafından belirtilmiştir.

$$Enc(m)=m^c(\text{mod } n)=E \quad (12)$$

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

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

d)El Gamal Algoritması (El Gamal Algorithm)

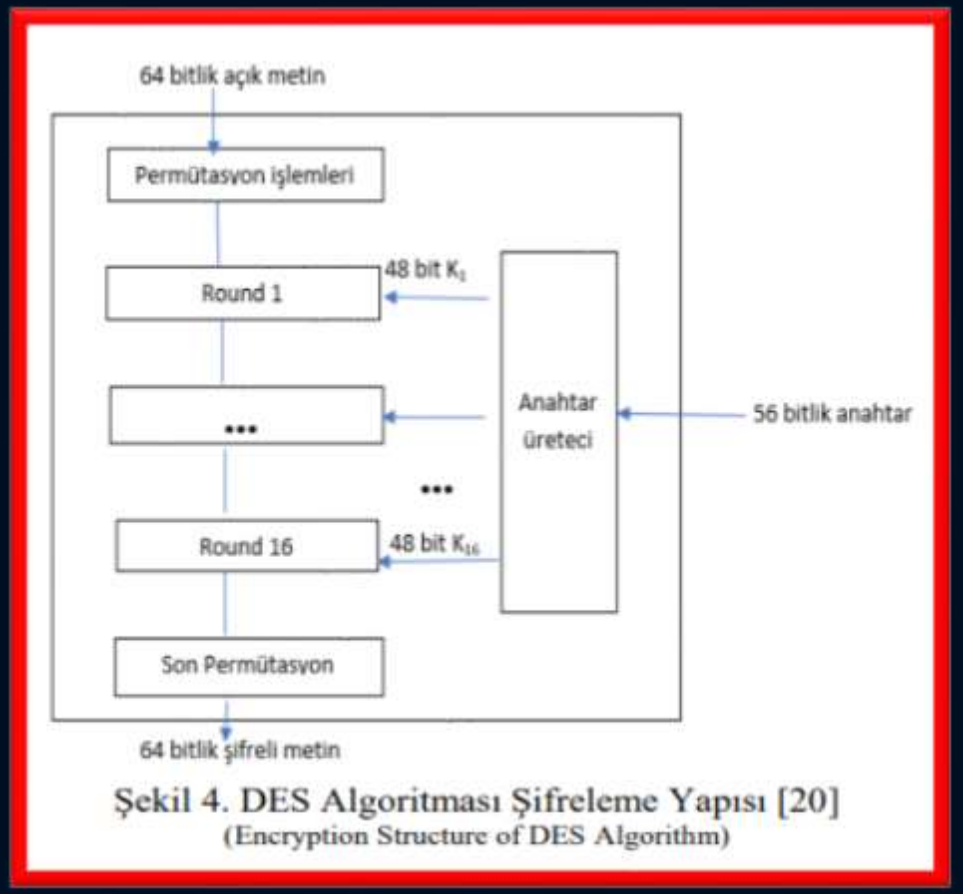
1985 yılında Taher Elgamal tarafından bulunan açık anahtar şifrelemeli bir algoritmadır. Dairesel gruplar üzerindeki ayrık logaritma zorluğuna dayanan bir algoritmadır.

DES Algoritması (DES Algorithm)

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

DES Algoritması (DES Algorithm)

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



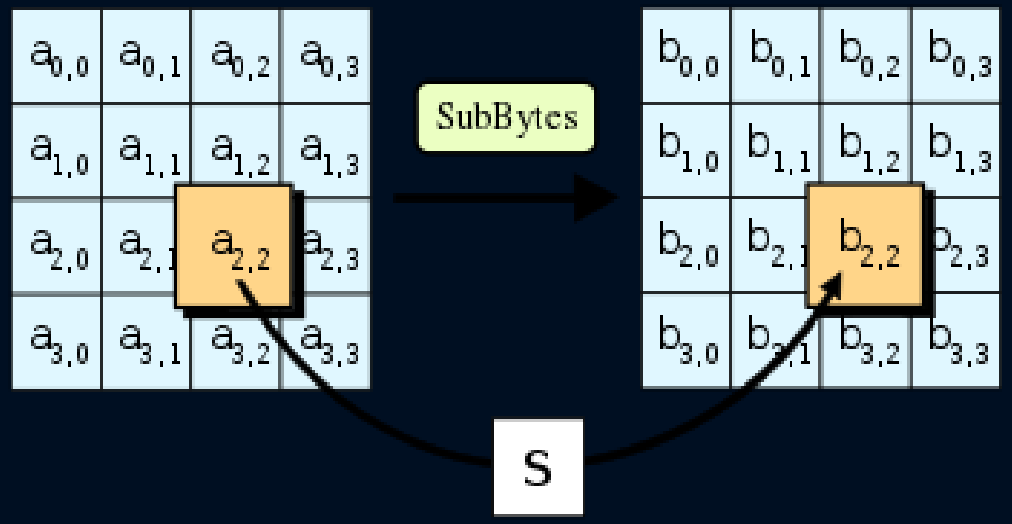
Şekil 4. DES Algoritması Şifreleme Yapısı [20]
(Encryption Structure of DES Algorithm)

BLOWFISH Algoritması (BLOWFISH Algorithm)

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

AES Algoritması (AES Algorithm)

AES ile tanımlanan şifreleme algoritması, hem şifreleme hem de şifreli metni çözmede kullanılan anahtarların birbiriyle ilişkili olduğu, simetrik-anahtarlı bir algoritmadır. AES için şifreleme ve şifre çözme anahtarları aynıdır.



AES çevrimindeki dört adımdan biri olan Bayt Değiştir işlemi

BENİ DİNLEDİĞİNİZ İÇİN
TEŞEKKÜR EDERİM..

adnangokmen_