T.C.
NECMETTİN ERBAKAN
ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bulut Veri Güvenliğinde Şifreleme Yöntemlerinin Performans Değerlendirmesi

Furkan KARAGÖZ

YÜKSEK LİSANS TEZİ

Bilgisayar Mühendisliği Anabilim Dalı

Temmuz-2022
KONYA

ÖZET

YÜKSEK LİSANS TEZİ

BULUT VERİ GÜVENLİĞİNDE ŞİFRELEME YÖNTEMLERİNİN PERFORMANS DEĞERLENDİRMESİ

Furkan KARAGÖZ

Necmettin Erbakan Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Hüseyin HAKLI

2022, 69 Sayfa

Jüri
Doç. Dr. Hüseyin HAKLI
Prof. Dr. Harun UĞUZ
Doç. Dr. Mehmet HACIBEYOĞLU

Günümüzde Endüstri 4.0 ile birlikte siber saldırılar artış göstermekte ve bilişim sistemlerine oldukça büyük zararlar vermektedir. Bu saldırılardan korunmak için çeşitli güvenlik önlemleri alınmaktadır. Alınan güvenlik önlemleri, manuel olarak sistemlere entegre edilebilen yazılımlar veya yapay zeka destekli otomatik çalışan yazılımlar ile günümüze kadar gelmiş ve gelişmeye de devam etmektedir. Bu gelişmelerle birlikte bilişim sistemlerini güvenli hale getirmek için çeşitli şifreleme algoritmaları önerilmiştir. Bu algoritmalar simetrik ve asimetrik şifreleme algoritmaları olarak ikiye ayrılmaktadır. Bu çalışmada güvenli ve etkili simetrik şifreleme algoritmaları olan DES, 3DES, AES, RC, Blowfish algoritmaları kullanılmıştır. Bu tez çalışmasının amacı DES, 3DES, AES, RC, Blowfish algoritmalarının metin dosyalarını şifreleme, çeşitli görselleri şifreleme ve yine şifrelemiş olduğu görsel ve metin dosyalarındaki şifre çözme becerisinin performans analizini sunmaktır. Materyal olarak DES, 3DES, AES, RC, Blowfish algoritmaları açık kaynak platformda yer alan çeşitli alanlardaki farklı büyüklükteki dosya boyutlarına sahip pdf uzantılı kitapların üzerinde ve açık kaynak görseller üzerinde denenmiştir. Kitaplar içerisinde resimli veya resimsiz ibareler içermeksizin her biri eşdeğer kabul edilip boyutları üzerinden bir kıyaslama yapılmıştır. Hesaplanan süreler işlemciye bağlı olarak değişkenlik gösterebileceği için her bir uygulama 15 çalışma zamanında gerçekleştirilmiştir. Buna göre ilk bakışta Blowfish algoritmasının küçük dosya boyutlarında hızlı olduğu görülmüş ve diğer yandan yüksek boyutlu metin şifrelemelerinde de oldukça iyi performans göstermiştir. Bulgular doğrultusunda Blowfish algoritması hem küçük hem de büyük boyutlu görsellerin şifrelenmesinde başarılı bir performans göstermiştir. Bu bulguların ve analizlerin sonucunda Blowfish algoritması özellikle şu an hızla büyüyen ve gelişen bulut bilişim sistemleri, nesnelerin interneti ya da diğer birçok alanda AES, DES, 3DES, RC gibi diğer simetrik şifreleme algoritmalarının alternatifi olabilir ve bu algoritmaların yerini alabilir. Şifreleme performansı olarak hızlı bir algoritma olması sayesinde Blowfish algoritması, kritik sistemlerde ve hızın metrik olarak daha fazla önem kazandığı alanlarda önemli bir seçenek olarak ön plana çıkabilir.

Anahtar Kelimeler: Bulut Bilişim, Simetrik Şifreleme, Şifreleme Algoritmaları, Veri Güvenliği, Blowfish Algoritması

ABSTRACT

MS

PERFORMANCE EVALUATION OF ENCRYPTION METHODS IN CLOUD DATA SECURITY

Furkan KARAGÖZ

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCE OF NECMETTİN ERBAKAN UNIVERSITY
THE DEGREE OF MASTER OF SCIENCE
IN COMPUTER ENGINEERING

Advisor: Assoc. Prof. Dr. Hüseyin HAKLI

2022, 69 Pages

Jury
Assoc. Prof. Dr. Hüseyin HAKLI
Prof. Dr. Harun UĞUZ
Assoc. Prof. Dr. Mehmet HACIBEYOĞLU

Today, with Industry 4.0, cyber-attacks have increased considerably and caused significant damage to information systems. Various security measures are taken to protect against these attacks. The security measures taken have survived to the present day with software that can be integrated into the systems manually or software that works automatically with artificial intelligence and continues to develop. Various encryption algorithms have been proposed to secure information systems with these developments. These algorithms are divided into two symmetric and asymmetric encryption algorithms. This study used DES, 3DES, AES, RC, Blowfish algorithms, which are secure and effective symmetric encryption algorithms. This study aims to present the performance analysis of the DES, 3DES, AES, RC, and Blowfish algorithms ability to encrypt text files, encrypt various images and decrypt images and text files that they have encrypted. In this study, DES, 3DES, AES, RC, and Blowfish algorithms were tested on open-source images and pdf books with different file sizes in various fields in the open-source platform. In the books, each of them was accepted as equivalent without including phrases with or without pictures, and a comparison was made over their sizes. Since the calculated times may vary depending on the processor, the application was run 15 times at runtime. Accordingly, at first glance, the Blowfish algorithm was seen to be fast in small file sizes, and on the other hand, it performed well in high-dimensional text encryptions. According to the findings, the Blowfish algorithm performed very well in encrypting small and large images in line. As a result of these findings and analysis, the Blowfish algorithm can be an alternative to and replace other symmetric encryption algorithms such as AES, DES, 3DES, and RC, especially in the rapidly growing and developing cloud computing systems internet of things or in many other fields. Thanks to being a fast algorithm in terms of encryption performance, the Blowfish algorithm can come to the fore as an important option in critical systems and areas where speed is more important as a metric.

Keywords: Cloud Computing, Symmetric Encryption, Encryption Algorithms, Data Security, Blowfish Algorithm

ÖNSÖZ

Yüksek lisans eğitimim boyunca bilgileriyle ışık tutan, yüreklendirici sözleriyle bana ve ben gibi tüm lisansüstü öğrencilerine akademik yolda yürüme şevki kazandıran Necmettin Erbakan Üniversitesi Bilgisayar Mühendisliği bölümündeki tüm hocalarıma sonsuz teşekkür ederim.

Yüksek lisans eğitimi konusunda beni cesaretlendiren sevgili abim Dr. Ahmet KARAGÖZ'e ayrıca bir teşekkürü borç bilirim.

Tüm iş hayatımda, akademik çalışmalarda yanımda olan çok kıymetli aileme ve değerli danışmanım Doç. Dr. Hüseyin HAKLI hocama özverili desteği için ayrıca teşekkür ederim.

Furkan Karagöz
KONYA-2022

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

ÇİZELGELER LİSTESİ

SİMGELER VE KISALTMALAR

ECB : Elektronik Kod Kitabı (Electronic Code Book)

CBC : Şifre Blok Zincirleme Modu (Cipher Block Chaining Mode)

CFB : Şifreli Geri Bildirim Modu (Cipher Feedback Mode)

CPU : Merkezi İşlem Birimi (Central Processing Unit)

DES : Veri Şifreleme Standardı (Data Encryption Standard)

DSA : Dijital İşaret Algoritması (Digital Signature Algorithm)

AES : Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

RC : Rivest Cipher Algoritması

TEA : Ufak Şifreleme Algoritması (Tiny Encryption Algorithm)

DH : Diffie-Helman Algoritması (Diffiee-Helman Algorithm)

ECC : Eliptil Eğri Şifreleme Algoritması (Elliptic Curve Algorithm)

IBM : Uluslararası İş Makineleri (International Business Machines)

NIST : Ulusal Standart ve Teknoloji Enstitüsü (National Institute of Standarts and Technology)

IDEA : Uluslararası Veri Şifreleme Algoritması (International Data Encryption Algorithm)

IaaS : Altyapı olarak Hizmet(Infrastructure as a Service)

PaaS : Platform olarak Hizmet(Platform as a Service)

SaaS : Yazılım olarak Hizmet(Software as a Service)

NSA : Ulusal Güvenlik Teşkilatı (National Security Agency)

RAM : Rastgele Erişimli Hafıza (Random Access Memory)

RC2 : Ron’s Code 2

RSA : Rivest-Shamir-Adleman

SHA : Güvenli Hash Algoritması (Secure Hash Algorithm)

SSL : Güvenli Yuva Katmanı (Secure Socket Layer)

DoD : Amerika Savunma Bakanlığı (U.S Department of Defense)

SPN : Koyma Değiştirme Ağı(Substitution Permutation Network)

IEEE : Elektrik ve Elektronik Mühendisleri Enstitüsü (Institute of Electrical and Electronics Engineers)

1. GİRİŞ

1.1. Tez Çalışmasına Giriş

Günümüzde birçok web, mobil ve masaüstü uygulamaları bulunmaktadır ve bu uygulamalarının çeşitli yollarla birbirleri ile iletişime geçtiği görülmektedir. Bu uygulamaların birbirleri ile iletişimi, internet üzerindeki servisler veya şu an popüler bir yaklaşım olan bulut sistemler aracılığıyla yapmaktadır. Bu iletişim uçtan uca bir yol üzerinde çeşitli yönlendiricilere uğrayarak, son kullanıcıya kadar devam etmektedir ve iletişim sürecinde güvenlik son derece önemlidir. İletişim sürecinde her sistemde olduğu gibi zafiyetler bulunmaktadır. İletişim sürecini farklı şekillerde etkilemek isteyen kişiler ya da çeşitli gruplar, bu iletişimi son kullanıcıya farklı bir mesaj içeriğiyle ileterek veya iletişim mesajını dinleyip farklı amaçlar doğrultusunda kullanabilmektedir. Günümüzde bu iletişim internete ve bilgisayara ait olduğu için siber (cyber) kavramı ile iç içedir. Siber alanda herhangi bir işlem gerçekleştirmek ve bunu diğer sistemlere aktarmak son dönemde oldukça tehlikeli hale gelmektedir. Bu noktada önceki bilişsel dönemlerde ve günümüzde önemli bir yeri olan siber güvenlik kavramı ortaya çıkar.

Siber güvenlik, özellikle artan teknolojik hareketler ve büyüyen bilişim ekosisteminde hemen hemen her alanda ihtiyaç duyulan bir gereksinim haline geldi(Lošonczi 2018). Siber güvenlik üç temel bileşen üzerine kuruludur. Bunlar; Sürdürülebilir Gizlilik (Confidentially), Bütünlük (Integrity) ve Erişilebilirlik (Avaliability)(B. Gunes 2021). Bu üç bileşendeki parametreleri temel alarak veri güvenliğini arttırmak için çeşitli şifreleme algoritmaları kullanılmaktadır. Simetrik ve asimetrik şifreleme algoritmalarından (DES, AES, RSA, Blowfish) yararlanılmaktadır.

Şifreleme, güvenli iletişimin kodlamasıdır ve modern dijital para birimleri endüstrisindeki en önemli süreçlerden biridir. Bugün kullanılan şifreleme teknikleri, çok uzun bir gelişme geçmişinin sonucudur. Eski zamanlardan beri insanlar bilgileri güvenli bir şekilde aktarmak için şifreleme kullandılar. Şifreleme ya da diğer adıyla Kriptografi yazma sanatının ortaya çıkmasıyla başladı. Medeniyetlerin gelişmesi ve insan varlıklarının ülkeler, krallıklar, klanlar vb. gruplara ayrılmasıyla, bu gruplar arasında yiyecek, enerji, içme ve diğerleri için rekabetin ortaya çıkmasına neden oldu, bu konuda bir yöntem ve yönteme sahip olmak gerekli hale geldi. Her grubun diğer gruptan uzakta

güvenli ve gizli bir şekilde iletişim kuracağı bir ortam olması gerektiği fark edildi. Böylelikle herhangi bir şekilde iletişimi örüntülemek ya da iletiyi karşı tarafa aktarılırken çeşitli semboller ya da harflere denk gelecek şekilde ilkel bir şifreleme ihtiyacı doğurdu. Fakat bu uygarlıklar arasındaki ortak görüş iletişim mesajını şifreli bir şekilde güvenli bir kanaldan karşı tarafa ulaştırmak için çeşitli şekilde yöntemler kullanarak ulaştırılmasına dayanır.

Şifreleme eski çağ uygarlıklarında ve günümüzde de sürekli gündeme gelen bir ihtiyaç olarak karşımıza çıkan bir kavramdır. İnsanoğlunun herhangi bir kişi, grup veya herhangi bir toplulukla yaptığı görüşmeyi şifreleme ihtiyacı çok eski uygarlıklara dayanmaktadır. Fakat burada şifrelemenin nereden çıktığına dair tarihçiler farklı görüşlere sahiptir. Kimilerine göre eski medeniyetlerin gözdesi olan Mısır uygarlığından çıktığını, kimileri ise orta çağda büyük bir egemenlik olan Roma uygarlığında imparatorluklar arası yazışmalarda, devletler arası görüşmelerde ihtiyaç olduğu görüşündedir (Dwiti Pandya 2015).

Şifreleme ilk çağ uygarlıklarında her ne kadar ilkel olarak kullanılsa da aslında dönemin şartlarında kodlama tekniğinin bir miktar kullanıldığı görülmektedir. Kodlama tekniğine en yakın olan ve insanlar tarafından en bilinen örnek, yaklaşık olarak 3.900 yıl önce yaşamış olan II.Khnumthab adlı Mısır zümresinden olduğu düşünülen kişinin mezar anıtında bulunduğudur. Mısır uygarlığı özellikle papirüs kağıtlarında olan mesajlaşmaları, antlaşmalarda kullanılan şifrelenmenin kullanıldığını düşünülmektedir (TonyM.D. 2009).

İlk çağ uygarlıklarında şifreleme, uygarlıklar arası iletişimle aktarıldı ve gelişmeye devam etti. Sonraki dönemlerde, şifreleme önemli yazışmalarda, antlaşmalarda ve daha çok askeri alandaki bilgilerin aktarılmasında kullanıldı. Hindistan uygarlığının devletler arası yazışmalarda ve casusların taşıdığı evraklarda M.Ö 2.YY'a kadar şifreli mesajlaşma kullanıldığı görülmektedir. Yine Yunanistan uygarlığının Fenikeliler ile yaptığı yazışmalarda ve çeşitli gizli ticaret antlaşmalarında bu ve buna benzer birçok şifreleme tekniği ile her şeyin gizli bir kanal aracılığıyla yapıldığı bilinmektedir. Aslında insanoğlunun bu yaptığı gelenek günümüz dünyasında da kişisel veya toplulukların gizlenme ve bilgiyi örtüleme ihtiyacının da somut bir göstergesidir. Şu an günümüz dünyasında da şifreleme yine bu alanda fazlaca yatırım yapılan bir

alandır. Şifreleme yıllar boyunca gelişerek ilerleyecek ve günümüze kadar olan yapıların mimari yapısını oluşturacaktı.

1.2. Literatüre katkısı

Yapılan tez çalışmasında, özellikle giderek artan güvenlik sorunlarına karşı kullanılan çeşitli şifreleme algoritmaları ve bu algoritmaların alternatifinin ne olacağı konusuna değinilmiştir. Özellikle kullanımı giderek artan bulut bilişim ekosisteminde tercih edilebilecek şifreleme algoritmalarının uygulamaları yapılarak, karşılaştırmaları olarak analiz edilmesiyle, bir tercih seçeneği yaratılması amaçlanmıştır. Literatürde şifreleme algoritmalarından hangisinin daha efektif kullanıldığı boşluğunu doldurulması hedeflenmiştir. Ayrıca bulut bilişim alanında ki siber güvenlik sorunları ve bunlara yapılan çözümler arasında şifrelemenin önemi ortaya koyulmuştur. Simetrik şifreleme türlerinden, anahtar boyutu, dosya boyutu, hız, verimlilik gibi şifreleme alanında önemli metrikler göz önüne anılarak bu çalışmadan sonraki çalışmalarda ne şekilde geliştirilebileceği ifade edilmiştir. Hızın metrik olarak önemli olan bilişim alanlarında algoritma seçimini kolaylaştırmak ve sonraki çalışmalarda ve alanlarda bunlara ışık tutması temel amaç olarak görülmüştür.

1.3. Tezin Organizasyonu

Tez çalışmasının organizasyonu şu şekilde yapıldı :

2. Bölümde Tez ile ilgili şifrelemenin gelişimi, şifreleme algoritmaları ile ilgili yapılan çalışmalar ve Bulut Bilişim güvenliğindeki şifreleme çalışmalarına ait Literatür araştırması bölümü yer almaktadır.

3. Bölümde Simetrik ve Asimetrik şifrelemelerin türlerini ve ne şekilde kullanıldıklarını anlatan Materyal ve Yöntem bölümü yer almaktadır.

4. Bölümde ise Bulut Bilişim tipleri, çeşitleri ve Bulut Bilişim mimarisi ile ilgili bilgiler verilerek Bulut Bilişimin temelleri anlatıldı.

5. Bölümde Şifreleme Algoritmalarının Performans analizleri (metin ve görsel şifreleme işlemleri) grafiksel olarak kıyaslamalı olarak sunuldu.

6. ve 7. Bölümlerinde ise Tartışma ve Sonuçlar, Sonuçlar ve gelecek çalışmalara ait Öneriler başlıklarıyla tez çalışması tamamlandı.

2. LİTERATÜR ARAŞTIRMASI

2.1. Şifrelemenin Gelişimi ile ilgili yapılan çalışmalar

1467 yılında, L.B Alberti, kriptografi alanına yeni bir soluk getirerek ilk defa kullanılan çoklu alfabeyi icat etti ve bunu yayınladı (Selleri 2020). Alberti şifresi olarak adlandırılan bu şifreleme, gönderici ve alıcı birer diske sahip olmakta ve aynı eksen üzerindeki bu disklerin karıştırılmasına dayanmaktaydı.

1499 yılında, J.Tritheim tarafından şifreleme ile mücadele için Almanya'da ilk defa kitap yazıldı. Özellikle Avrupa mahkemelerinde şifreleme ile mesajlaşma için kullanıldığı düşünülmektedir. Aslında Tritheim, Benedictine geleneğine bağlı kalarak 9.YY Diplomasisini de inceleyerek, tüm sesli harflerin yer değiştirmelerine dayanan bir şifreleme tanımladı. Örneğin tanımlanan noktalar ile ; "i" harfi için tek bir nokta, "a" harfi için iki nokta, "e" harfi için üç nokta, "o" harfi için dört nokta ve "u" harfi için beş nokta konmasına dair sistematik bir metot öne sürmüştü. Örnek bir kelime olarak "Bonifacia" olarak adlandırılan kelimesinin , "B::n.f:c.:" şeklinde şifrelenmesi metodolojisine dayandırmaktaydı. Daha sonraki yıllarda yine benzer ve aynı yöntem ticari ve diplomasi trafiğinde sıkça kullanıldı (D'Agapeyefff 2013).

1797 yılında ise, T.Jefferson, Jefferson Tekerleği (Jefferson Wheel) adlı şifreleme mekanizmasını üzerine bir buluş gerçekleştirdi. Bu buluşta demir mil üzerine monte edilerek 26 adet parçalı ahşap silindirik tekerlek üzerine inşa edildi. Alfabeye ait harfler tekerleğin kenarına tamamen rastgele olacak şekilde işlenir ve tekerlek her dönüşünde yeni bir kelime üretilir mekanizmasına dayanmaktaydı. Ayrıca gönderici bu işlemi yaptıktan sonra alıcı Jefferson Tekerleğindeki kodlanan mesajı heceleme aracılığıyla anlamlı olan kelimeyi seçip hangi kelimenin geldiğini anlayabiliyordu. Daha sonradan ise Amerika Savunma Bakanlığı (U.S Department of Defense) bu şifrelemeyi geliştirerek şirket içerisinde casus ön izlemelerinde bir teknik olarak 1923 ve 1942 yılları arasında tekrar kullandı (TonyM.D. 2009, Dooley 2018).

1930'da, Almanya hükümeti tarafından geliştirilen ENIGMA, şifrelemesi elektromanyetik temelli ticari, ekonomik ve özellikle askeri alanda kullanılan bir şifreleme ya da şifreleme cihazıydı. Alman hükümetinin asla kırılamaz diye üstüne düşündüğü ve ordu da fazlaca yeri olan enigma şifrelemesi dünyada büyük yankı

uyandırdı. II.Dünya savaşı'nın tam da hararetlendiği zamanlarda ENIGMA şifrelemesi yine yaygın olarak kullanılmaktaydı. Savaş süresince kritik bilgilerin dinlenemiyor olması bir sorundu ve İngiliz Bletchley Park tesisi bu kodu çözmeye uğraşıyordu. Çeşitli kriptoanalist ve uzmanlar şifreyi yorumladı fakat herhangi bir çözüm getiremedi. Daha sonra yine Bletchley testilerinde çalışan, 1936'da Turing makinelerine de adını veren bilim adamı A.Turing tarafından, kırılamaz denilen ENIGMA şifrelemesi "Bombe" adlı cihaz ile kırıldığı ve II. Dünya savaşının aktif zamanlarında Nazi Ordusunu yanlış bilgiler ile yönlendirilerek farklı şekillerde kullanıldığı bilinmektedir. Bu da savaşın seyrini büyük ölçüde değiştirildiği için günümüzde ve geçmiş dönemlerde bu kritik bilgilerin önemini bir kez daha ortaya kayan bir anlayış oldu (Ellis 2013).

1960'lı yıllara gelindiğinde, bilgisayar ve bilgisayar teknolojisi daha fazla ivme kazandı ve işlemler daha kolay hale geldi. Büyüyen bu gelişmeler şirketlerin milyonlara ulaşmasını kolaylaştırdı ve bilgi yayılmaya başladı. O dönemde büyüyen kurumsal şirketler bu bilgileri şifrelemenin önemini kavradı ve bilgileri şifrelemeye girişti. Fakat her kurum kendi şifreleme sistemini geliştiriyor ve ortak bir standardizasyon oluşmadı. Böyle olunca kurumlar arası herhangi bir şifrelenmiş metin diğer kurum tarafında çözümlenemiyor ve çeşitli sorunlarla karşılaşılıyordu. Bu yıllarda bu gereksinim oldukça fazla hissedildi (Kotas 2000).

1970 ve 1973 yılları arasında, Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology - NIST), standardizasyon sorununu çözmek ve uluslararası genel geçer bir standart yakalamak için NIST standart şifreleme için teklifler almaya başladı. O sırada dünyada bunun için en eşsiz aday hiç şüphesiz Uluslararası İş Makineleri(International Business Machines)'nin "Lucifer" adlı ürünüydü. Lucifer dönemlin şartlarında en güçlü şifre olarak görülüyordu. Ulusal Güvenlik Ajansı(National Security Agency) tarafından da asla kırılamaz gözüyle bakılıyordu. Lucifer şifresi temelinde "56-bit Şifreleme" olarak da adlandırılır. Çünkü şifreleme 10^{16} kadar büyük bir sayıyı temsil etmektedir. Bu da 56-bit için gereken bit sayısını ifade eder. 1976 Kasım ayının sonlarında 56 bitlik Lucifer şifresi Amerika Birleşik Devletleri'nin resmi şifreleme standardı olarak kabul edildi ve daha sonradan da adından sıkça söz ettirilen Veri Şifreleme Standardı (Data Encryption Standard) olarak adı değiştirildi (Kotas 2000).

1978'de, R.Rivest A. Shamir ve L.Adleman tarafından isimlerinin baş harflerini verdikleri, RSA olarak adlandırılan ilk açık anahtar şifreleme ve imza sistemini keşfettiler. RSA kısmi olarak kullanıldı ve bu zaman testinden başarılı bir şekilde çıktı. Güçlü bir şifreleme algoritması olarak hala çeşitli yerlerde kullanılmaya devam etmektedir. Güvenliği büyük sayıların çarpanlarına ayırmanın zorluğu prensibine dayandırır. RSA algoritmasını keşfedenler herkese algoritmayı kırmaya teşvik ettiler fakat çarpanlarına ayırarak ya da başka kriptolojik teknikler ile başarılı olan olmadı. RSA bu yönüden sertifikalı algoritmalar grubunda yer alır ve herhangi bir şekilde kırılmadıkça kullanılmaya devam edecektir (Milanov 2009).

1990'dan itibaren, Kriptografi alanında şifreleme giderek ivme kazandı ve Kuantum Kodlama (Quantum Coding) adı verilen tamamen yeni bir kodlama biçimi geliştiriyorlardı ve modern kodlamanın sağladığı koruma düzeyini bir kez daha yükseltmeyi umuyordu. Amerika Birleşik Devletleri'nde sınıflandırılmamış bilgileri kodlamak için bilgileri işlemek için, standart veri şifrelemesi olan DES, tarihte en bilinen şifreleme mekanizmasıdır. Şifrelemenin temellendiği DES 56-bitlik bir şifreleme seçeneğiyle yaklaşık 20 yıl boyunca kullanılmaya devam etti (TonyM.D. 2009, Dooley 2018).

1997 yılına gelindiğinde ise, Gelişmiş Şifreleme Standardı(Advanced Encryption Algorithm) sunuldu. AES, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından geliştirildi ve bugün başta bulut bilişim olmak üzere birçok alanda AES şifreleme standardı hala görülmektedir. DES şifrelemenin zamanla *brute-force (kaba-kuvet)* saldırılarıyla kırılması ve anahtar boyutunun düşük olması AES algoritmasının geliştirilmesini tetikledi. AES kırılması oldukça güç bir şifreleme algoritmasıdır ve 128 bitlik bir şifreleme uygulandığında kodun çözümlenmesi için yaklaşık olarak $2^{\wedge 55}$ yıl gerekir (TonyM.D. 2009, Dooley 2018).

2008 ve 2012 yılları arasında, adında sıkça söz ettiren Blok Zinciri (Block Chain) kavramı hayatımıza girdi ve günümüzde de oldukça fazla projesiyle karşımıza çıkmaktadır. Blockchain, kriptografi kullanarak ağ ve ağa bağlı her şeyi şifreleyerek kapsayarak devam etti. Aslında modern bir kayıt defteri olarak nitelendirilen Blockchainde, üzerindeki her bir blok, kendinden önceki bloğun bir kriptografik

şifrelenmiş fonksiyonunu gösterir. Çalışma mekanizması bunu içinde tutar ve her bir blok kendinden sonraki bloğu işaret eder (Don Tapscott 2016). Değiştirilemez olması, akıllı sözleşmeler (smart contracts) içermeleri ve dağıtık bir işlem defteri olması kamuya açık olarak işlem kayıtlarına erişimi mümkün kılar.

Son zamanlarda oldukça popüler olan dijital para ya da coin adları verilen birimlerinin oluşturulmasını mümkün kılmak için kriptografik yöntemler sıklıkla kullanılmaktadır. Özellikle sosyal toplulukları bu ekosistemin içine dahil etmek için çeşitli takım jetonları (token) ya da büyük kuruluşların hisse senedinin sanallaştırılmış hallerinin kripto birimleriyle, bireyleri bu sisteme katmak hedeflenmektedir. Kripto para birimleri, ortak alt anahtar şifrelemeleri veya dijital imza teknolojilerinden yararlanır. Blokchain üzerinde sürekli olarak işlem kaydı tutulan ve verilerin güvenliğini sağlamak için kullanılır. Başta Bitcoin olmak üzere altcoin adı verilen ve beyaz listesi (white paper) yayınlanmış diğer coinlerin güvenliğini sağlamak oldukça mühimdir. Özellikle buraya olan talebin çok olması ve insanların buradan para kazanma odaklı bir sektör haline getirmesi, çeşitli sahtekarları kendine çekti ve sahte token veya sahte coinler piyasaya sürerek insanların paralarını gasp etmektedir. Yine burada kişisel kullanıcılara görev düşerken, bazı projelerin hangi ağda oluşu, nerede bilgilerin tutulduğu gibi teknolojik alt yapıları da oldukça önem kazandı.

Geriye doğru bakıldığında veri şifreleme gereksinimi, çok eski çağlarda da kişi ya da toplulukların ihtiyaç duyduğu temel hizmetlerden biri oldu ve olmaya da devam etmektedir. Geçmişten günümüze kadar şifreleme ve şifreleme mekanizmalarına baktığımızda ise hiçbir sistemin tam olarak güvenli olmadığı ve şifrelemenin izin verdiği kadar güvenli olabileceği çıkarımıdır.

2.2. Şifreleme Algoritmaları ile yapılan çalışmalar

Şifreleme algoritmaları ile yapılan çalışmalar çok farklı alanlarda gerçekleştirilmektedir. Nesnelerin İnterneti, Bulut Bilişim, Web güvenlikleri ve daha birçok alanda şifreleme algoritmalarının kullanılmasıyla ilgili çalışmalar mevcuttur.

2015 yılında P.Patel ve ark. tarafından, akıllı mobil cihazların güvenliğini geliştirmek için Eliptik Eğri şifreleme algoritması ile Blowfish algoritmasını

birleştirerek yeni bir metot geliştirdiler ve bunu diğer şifreleme algoritmaları ile kıyasladılar (Payal Patel 2015).

M. Suresh ve Neema M. Blowfish algoritmasının donanımsal yapıya uyarlanması ve bu yapılan donanımsal şifrelemenin nesnelerin interneti alanında kullanılması içeren çalışmayı yayınladılar ve orjinal Blowfish ile önerilen Blowfish algoritmasını karşılaştırdılar (Manju Suresh 2016).

2014 yılında ise S. Avireddy ve ark. tarafından, "SQL Enjeksiyonu(SQL injection)" saldırılarından korunmak ve veritabanlarına herhangi yasadışı erişimi engellemek için uygulamaya özel rastgele şifreleme algoritmaları yapılarını önerdi (Srinivas Avireddy 2012). Benzer şekilde 2012 yılında A.O. Afolabi ve E.R. Adagunodo tarafından web tabanlı öğrenme sistemlerinde bağlamsal çerçeveyi ve sistem güvenliğini arttıran geliştirilmiş veri şifreleme algoritması önerildi (Afolabi and Adagunodo 2012).

N.Atikah ve ark. tarafından, AES ve RC4 algoritmalarının bir kombinasyonu önerildi. Kombinasyon yaparak şifreleme algoritmasın güçlendirmenin güzel bir yöntem olduğu savunuldu. Şifreleme algoritmasının güvenliğini ölçmek için de Çığ etkisinin (Avalanche effect) hesaplanılması gerektiğini öne sürdü (Atikah, Ashila et al. 2019).

S. Kruti ve B. Gambhava tarafından, DES algoritmasında bir iyileştirme önerildi. İyileştirme DES algoritmasının her bir turda bir operasyon uygulayarak bir anahtar daha eklenmesine dayandırdılar. Birinci anahtar K_i için ve ikinci anahtar ise f fonksiyonu ile işlem gerçekleştirdi. Önerilen geliştirilmiş DES yöntemi, şifreleme güvenlik mekanizmasını arttırdığını öne sürdüler (Shah Kruti and Gambhava 2012).

P. Singh ve K. Singh, tarafından Blowfish algoritması görsel şifrelemeler üzerinden denendi. Şifrelenmiş görüntünün histogramı daha az ve dinamik olduğu için şifrelemenin daha kolay olacağı üzerine temellendirdiler. Blowfish algoritmasının 28r+1 kombinasyonunda kırılamayacağını ve güçlü bir şifreleme algoritması olduğunu savundular (Singh and Singh 2013).

H. K. Verma ve R. K . Singh tarafından RC6, Twofish ve Rijndael blok şifreleme algoritmaları analiz edildi. Analize göre RC6 algoritması Twofish ve Rijndael algoritmalarından daha hızlı performans gösterdi. Yine RC6 algoritmasının kaynak kullanımının Twofish ve Rinjdael algoritmalarından daha az olduğunu ve şifreleme için tercih edilmesinin daha kolay olduğunu savundular (Verma and Singh 2012).

2.3. Bulut Bilişim Güvenliği ile ilgili yapılan çalışmalar

Bulut Bilişim güvenliği ile ilgili çok sayıda mevcut simetrik algoritma ve asimetrik algoritmaların varyantları önerildi. Özellikle AES, Homomorfik ve Blowfish algoritmalarının farklı şekilde uygulanması ya da geliştirilip yeni bir yöntem adı altında geliştirmesi ile ilgili önerilen çalışmalar bulunmaktadır.

2020 yılında Dhirendra KR Shuklave ark. tarafından yine bir blok şifreleme şemasıyla, düz metini 128 bit bloğa bölen ve blokları da 16 bit'e bölen bir şifreleme yöntemi önerdi ve bu yöntemi uygulayarak DES, AES, Blowfish algoritmalarıyla kıyaslaması gerçekleştirildi(Dhirendra KR Shukla 2020).

Yine benzer şekilde U. Somani ve ark. tarafından 2010 yılında IEEE konferansında yayınlanan bildiri de bulut bilişimde veri güvenliği geliştirmek için dijital imza tabanlı yönetim ile RSA algoritmasını birlikte kullanarak bulut bilişimde güvenliğin geliştirilebileceği önerildi (Uma Somani 2010).

Halder ve Newe tarafından, güncel olarak bulut destekli IoT sistemlerde homomorfik şifreleme yoluyla güvenli zaman serisi paylaşımı önerildi (S.Halder 2022).

2014 yılında ise F. Zhao ve ark tarafından; tamamen homomorfik şifreleme üzerine dayalı, veri iletimini güvenli bir kanal üzerinden gerçekleştiren ve bunun güvenli bir şekilde depolanmasını sağlayacak homomorfik şifreleme çalışmasını gerçekleştirdiler (Liu 2014).

Thabit ve ark. tarafından bulut bilişim için NLCA adında yeni bir şifreleme algoritması önerildi ve özellikle resim şifrelemeleri ve bunlara ait histogramlar ile

performans analizini yaparak, bulut bilişim için de kullanılabilirliğini vurguladılar (Fursan Thabita 2021).

P. Kalpana ve S. Singaraju tarafından bulut bilişim için RSA algoritması kullanımı önerildi. RSA algoritması şifreleme ve deşifreleme işlemleri ile yetkisiz kullanıcıların doğrudan isteyerek ya da yanlışıkla verileri elde ederse, bu şifrelenmiş verileri çözemeyeceğini ve orjinal verileri elde edemeyeceğini savundular (Kalpana and Singaraju 2012).

M.Zhao ve Y. Geng tarafından yine bulut bilişim için Homomorfik şifreleme algoritması önerildi. Çeşitli türlerdeki homomorfik şifreleme algoritmalarını (Gentry'ye ait homomorfik şifreleme, çift anahtarlı homomorfik şifreleme, optimizasyon düşüş önlemeli homomorfik şifreleme vs.) bulut bilişim ortamlarında karşılaştırmalı olarak denediler ve kıyasladılar. Homomorfik şifrelemenin kullanıcı bilgi güvenliğini sağladığını ve bulut bilişimde aktif olarak kullanılabileceğini savundular (Liu 2014).

S.Eletriby, E. Mohamed ve H.Abdulkader tarafından, bulut bilişimde Modern şifreleme algoritmaları Amazon EC2 servisi üzerinde kıyaslamalı olarak denendi. Kapladığı alan ve hızı metrik olarak aldı ve AES,RC6, DES ve Blowfish algoritmalarının diğer modern şifreleme algoritmalarından (RC4, MARS, Two-fish, 3DES) daha iyi şifreleme algoritmaları olduğunu ve bulut bilişim sistemlerinde kullanılabileceğini savundular (El-etriby, Mohamed et al. 2012).

A.Bhardwaj ve ark. tarafından, bulut bilişimde DES, 3DES ve AES şifreleme algoritmalarını dosya boyutu, şifreleme süresi, deşifreleme süresi parametrelerini baz alarak kıyasladılar. AES algoritmasının MD5 kodlama sırasında diğer algoritmalardan daha üstün olduğunu ve hız olarak öne geçtiğini ortaya koyuldu(Bhardwaj, Subrahmanyam et al. 2016) .

3. MATERYAL VE YÖNTEM

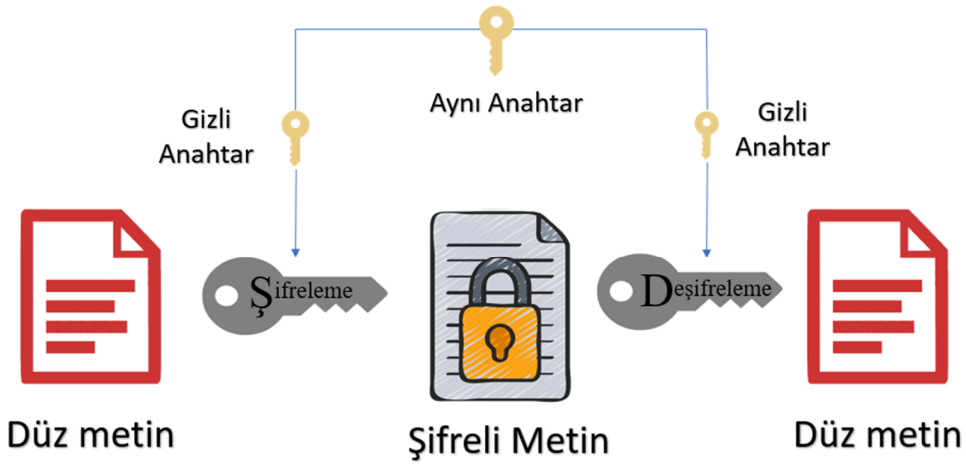
Şifrelemeler temel olarak 2 kategoride ele alınmaktadır. Bunlar Simetrik Şifreleme ve Asimetrik şifreleme algoritmalarıdır. Simetrik Şifreleme, tek bir gizli anahtar kullanılarak yapılan yapısal olarak basit ama etkili bir şifreleme türüdür. Asimetrik şifreleme ise, genel ve özel anahtar kullanılarak yapılan yine etkili bir şifreleme yöntemidir.

3.1 Simetrik Şifreleme

Simetrik şifreleme, iletişim boyunca yapılan görüşmeyi ya da iletiyi şifrelemek ve yine aynı iletişimde, karşı tarafa gönderilen şifreli iletiyi deşifre etmek için tek bir gizli anahtar içeren bir şifreleme türüdür. Simetrik şifreleme kriptografik tarihe baktığımızda yeri oldukça eskilere dayanan fakat eski ama etkili bir yöntemdir.

Herhangi bir kelime, harf ya da sayı grupları şifreli metini çözmek için gizli bir anahtar olarak kullanılabilir. İletişim kanalı boyunca gönderici ve alıcı, iletiyi şifrelerken ve şifresini çözerken bu gizli anahtara sahip olması gerekir. Eğer bu gizli anahtara sahip değilse iletiyi görüntüleyemez. Simetrik şifreleme özellikle işlem hızı parametresinin öne çıktığı yerlerde tercih edilen etkili bir algoritmadır. En bilinen örnekleri sırasıyla; AES, DES, 3DES, Blowfish, RC Algoritmaları şeklindedir (Diaa Salama Abdul. Elminaam 2008).

Simetrik şifreleme seçilen algoritmaya göre güvenlik düzeyi değişen ve şifreleme hızı değişkenlik gösteren güvenli bir şifreleme yöntemidir. Günümüzde en yaygın olarak kullanılan simetrik şifreleme, Ulusal Standartlar ve Teknoloji Enstitüsü tarafından geliştirilen Gelişmiş Şifreleme Standardı (Advanced Encryption Algorithm)'dır. AES 128, 192, 256 bitlik seçenekleriyle denk gelir ve eğer 256 bitlik anahtar uzunluğu seçilirse, 10 petaflopluk bir bilgisayarın kaba kuvvet saldırısı (brute force attacking) yoluyla anahtarı tahmin etmesi yaklaşık olarak bir milyar yıl kadar sürer. Kasım 2021 itibariyle, dünyanın en hızlı bilgisayarı Japonyada bulunmaktadır. Bu süper bilgisayar 442 petaflop hızında çalışmakta yani yaklaşık olarak 600.000 Adet Iphone 11 model telefonun çalışma gücünü tek başına gerçekleştirmektedir. Bu şekilde bile, 256-bit AES'i kırmak oldukça güçtür (Kshetri 2021).

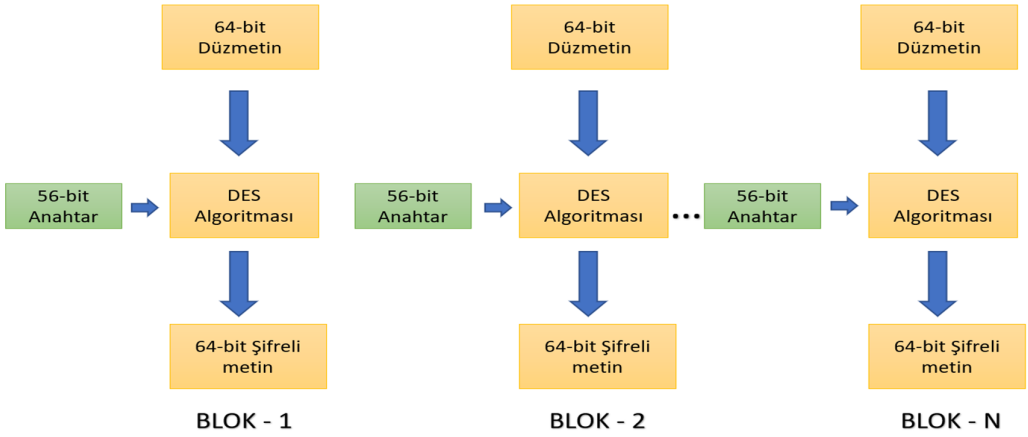


Şekil 1.1. Simetrik Şifreleme Algoritma Yapısı

Simetrik şifrelemeyle ilgili en büyük problem, gizli anahtarı alıcıya ulaştırmak için bir kanala sahip olunmasıdır. Burada şifreleme bloklar üzerinden yapıldığı için bunun karşı tarafa aktarılması gerekmektedir. Özellikle göndericinin kendisine ait metini şifrelerken yararlandığı bu seçenek simetrik şifrelemede önemli rol oynar (Canniere 2007).

3.1.1 Veri Şifreleme Standardı(Data Encryption Standard - DES)

1970'lerin başında IBM, DES'i (Veri Şifreleme Standardı) geliştirdi ve Horst Feistel tarafından tasarlanan Lucifer şifresine dayandırdı. DES, NIST'in önceki adı olan NBS'ye gönderildi. Ajansın federal kullanıma uygun bir blok şifre çağrısı ve 1977'de Amerika Birleşik Devletleri'nde bir standart haline geldi. Ancak, NSA ilk gönderilen DES ayarını değiştirdi ve karşı dirençli daha iyi S-kutuları ile sonuçlanan gönderim diferansiyel kriptanaliz yaptılar ve DES'i yapan anahtarı kısaltarak arama saldırılarına duyarlı hale getirdiler (Tezcan 2022).



Şekil 1.2. DES Algoritma Yapısı

DES, 64 bitlik bir blok boyutuna sahip Feistel tipi bir blok şifrelemedir ve 56 bitlik anahtar uzunluğuna sahiptir. 16 tura boyunca akış devam eder ve her tur işlevi aşağıdakilerden oluşur: Bir genişletme işlevi, yuvarlak anahtar XOR, S-kutularının uygulanması ve bir permütasyon işlemi uygulanması.

DES algoritmasının, çeşitli güvenlik açıklarının olması, *brute-force(kaba-kuvvet)* saldırılarıyla kırılabilir olduğunu göstermesi, 2000'li yılların başında yetersiz kalmasına yol açtı ve itibarını kaybetti. Günümüzde ise *brute-force(kaba-kuvvet)* saldırıların artık yapay zekaya dayalı bot yazılımlarıyla dinamik olarak yapıldığı ve saldırganların daha farklı yöntemler geliştirmesi nedeniyle neredeyse hiç kullanılmamaktadır.

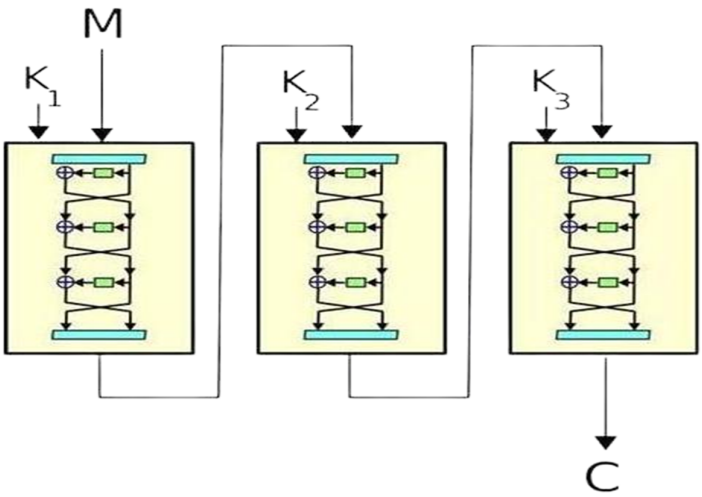
Bu sorunların neden olduğu DES algoritması, üçlü DES veya DES-3 olarak bilinen yeni bir algoritma ile düzeltildi (Aslan 2019).

3.1.2 3'lü Veri Şifreleme Standardı (Triple DES – 3DES)

Üçlü DES (3DES), 1978 yılında Uluslararası İş Makineleri tarafından geliştirilmiş olan bir şifreleme algoritmasıdır. DES'in zaman içinde kaba kuvvet saldırılarına karşı işlevsiz hale gelmesi yüzünden mevcut sistemin geliştirilmiş ve birden fazla tekrarlanmasıyla kırılmasının önüne geçmek amacıyla geliştirilmiş bir

şifreleme türüdür. 3DES, iki ana algoritma olan DES ve AES arasındaki bir geçiş döneminde tanıtıldı. 1997'de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından, DES'in yerini alabilecek şifreleme algoritmalar için resmi bir araştırma yaptığını yayınladı.

AES, 2030'ların sonlarına kadar 3DES ile birlikte kullanılması amacı ile piyasaya sürüldü. Fakat 3DES'in şifrelemedeki yavaşlıkları bazı kritik sistemlerde ve hızın parametre olarak öne çıktığı yerlerde AES'in yerini alamaması yüzünden fazla tercih edilmemesine neden olmuştur. Bununla birlikte, 3DES'in kullanımdan kaldırılması, önemli güvenlik açıklarını ortaya çıkaran ve bazı hesaplara göre çok gecikmiş olan araştırmaları muhtemelen hızlandırdı (Patil, Narayankar et al. 2016).



Şekil 1.3. 3DES Algoritma Yapısı (Wikipedia 2015)

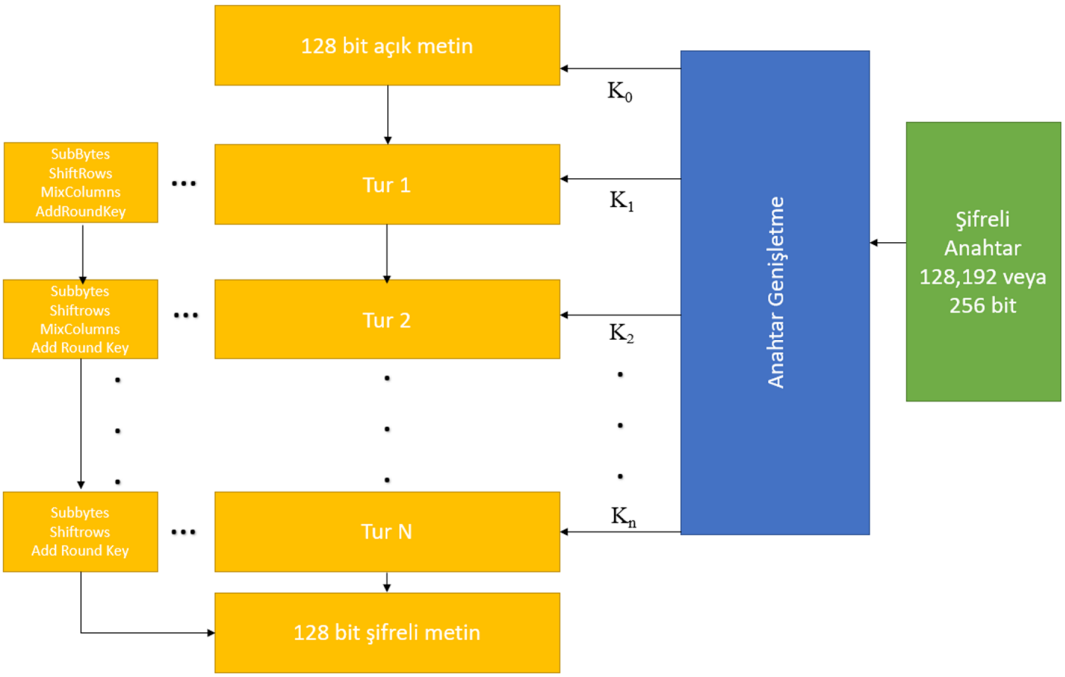
NIST, 3DES'e yönelik saldırıların analizi ve gösteriminin ardından ilk olarak 3DES'in kullanımdan kaldırılması tartışmasını başlattı. *Sweet32* güvenlik açığı, araştırmacılar K. Bhargavan ve G. Leurent tarafından kamuoyuna açıklandı. Bu araştırma, uzun aktarımlar, içerik dosyalarının değişimi veya metin enjeksiyonuna karşı savunmasız aktarımlar sırasında en yüksek olan 3DES ve diğer 64 bit blok şifreleme paketlerindeki çarpışma saldırılarına karşı bilinen bir güvenlik açığından yararlandı. Bu güvenlik açığının ortaya çıkmasından sonra NIST, 3DES'in kullanımdan kaldırılmasını önerdi ve kısa süre sonra kullanımını kısıtladı. Özellikle işlem süresinin uzun olması ve günümüzde NIST gibi bir kurumdan desteklenmemesi 3DES'in şifreleme standardı olarak popülaritesini oldukça azalttı.

3.1.3 Gelişmiş Şifreleme Standardı (Advanced Encryption Standartd - AES)

AES algoritması DES algoritmasının geliştirilmiş hali olarak nitelendirilir. DES'in kaba kuvvet saldırılarına karşı savunmasız hale gelmesiyle yeni bir standardizasyon ihtiyacı doğmuş ve DES'in yerini almış bir şifreleme algoritmasıdır. DES yetersiz kaldıktan sonra birkaç bilim adamı tarafından 2001 yılında geliştirildi. V. Rijmen ve J. Daemen tarafından tasarlandı. DES'i tamamen düzelten ve yetersizliklerini kapatan matematiksel bir blok şifreleme algoritmasıdır. 3 farklı anahtar uzunluğu vardır. Bunlar; 128, 192 ve 256 bit şeklindedir.

Koyma değiştirme ağı (Substitution–permutation network) bir dizi matematik ve mantık işlemine dayanmaktadır. AES de SP ağı olarak da bilinen bir ikame-permütasyon ağına dayanmaktadır. Girdilerin belirli çıktılarla değiştirilmesi (ikameler) ve bit karıştırmayı (permütasyonlar) içeren diğerleri de dahil olmak üzere bir dizi bağlantılı işlemden oluşur.

AES içerisinde 128- bit' lik veri blokları her biri 32- bit' ten oluşan 4 kelime olarak düşünülmektedir. AES tur mekanizmasıyla çalışmaktadır. Bit sayısı ne kadar artarsa o kadar çok güvenlik artışı meydana gelir. Örneğin 256 bit için 14 tur şifrelenmiş mesaj ulaşır. 128 bit için ise 10 tur şifrelenmiş mesaja ulaşılır. Tur sayısı bit sayısına göre paralel olarak artmaktadır. AES algoritması hem şifreleme hem de şifre çözme için şifre bir "AddRoundKey" ile başlar. Son tura ulaşmadan hemen önce bu bit sayısına göre n turdan geçer. 1) Alt Baytlara ayrılır (Sub-Bytes), 2) Satırları kaydırma işlemi (Shiftrows) uygulanır 3-) Sütunlar karılır (Mix-columns) 4-) Tur anahtarı eklenir (Add Round Key). Yalnızca son turda Mix-columns işlemi uygulanmaz. Deşifreleme işlemi de benzer şekilde bu işlemlerin tam tersi olarak uygulanır (Ajay Kakkar 2012).



Şekil 1.4. AES Algoritma Yapısı

AES ile şifreleme işlemine başlanırken 128-bit yani 4 kelimeden oluşan veri bloğu durum dizisi içerisine yazılır ve algoritma sırasındaki gerekli işlemlerin tümü bu dizi kullanılarak gerçeklenir. Şifreleme için gerekli en son işlemin de bitimiyle birlikte durum dizisinin son hali çıkış dizisine yazılır. Günümüzde özellikle bulut sistemlerde aktif olarak kullanılmaktadır.

3.1.4 Rivest Cipher(RC) Algoritmaları

3.1.4.1. Rivest Cipher 2(ARC2) Algoritması

RC2, R. Rivest tarafından 1987 yılında bulunmuştur. RSA'in de mucitlerinden biri olan Rivest, RSA algoritmasını daha güvenli hale getirmek için çeşitli şifreleme yöntemleri üzerinde çalıştı ve RC Algoritmaları ve sonrası geliştirilecek olan diğer versiyonlarına öncülük etti.

RC2 gizli anahtarlı şifreleme yapan blok şifreleme algoritmalarından biridir. DES Algoritmasının yerini alması amacıyla geliştirildi. Giriş ve çıkış blok boyutları, her biri için 64 bittir. Anahtar boyutları 1 ile 128 bayt arasında değişebilen anahtar

uzunluğuna sahiptir. Ancak mevcut uygulama da 8 byte olarak kullanmaktadır(Rivest 1998).

RC2, 64 bitlik bir blok şifreleme kullanarak değişken anahtar boyutu kullanır. Yine feistel ağı üzerinde geliştirdiği bir şifreleme türüdür. Toplamda 18 tur boyunca işleme devam eder. 16 karıştırma turu(mixing rounds) ve 2 adet rastgele serpiştirilmiş ezme turları(interleaved mashing rounds) bulunmaktadır(Gonsai and Raval 2014).

Algoritma 16 bit mikroişlemcilere uygulanması amacıyla geliştirildi. IBM Kişisel Bilgisayarlarına göre şifreleme işlemi DES algoritmasına gore iki kat daha hızlı çalışmaktadır. Fakat burada anahtar seçimi ve kaç bayt olduğununda fazlaca değişkenlik gösterdiği ve anahtar seçim işlemin algoritma için büyük bir önem taşıdığı vurgulandı.

3.1.4.2. Rivest Cipher 4 Algoritması

RC4 algoritması Kablolu Eşdeğer Gizlilik (Wired Equivalent Privacy) ve Wi-Fi Korumalı Erişim (Wi-Fi Protected Access) kullanan RC2'dan sonra geliştirilmiş simetrik bir şifreleme türüdür. Bura kullandığı WEP ve WPA denilen kavramlar yönlendiricilerde sıklıkla kullanılan şifreleme protokelleridir. Özellikle web ağlarında kullanılmak amacıyla geliştirildi. Güçlü bir şifreleme gerçekleştirmek için genel olarak 16 bayt anahtar seçeneği kullanılır. Ancak dışa aktarma kısıtlamaları problem olduğundan kısa anahtar uzunlukları da yaygın olarak kullanılan seçenekler arasındadır. Bu algoritma her seferinde bir baytı veya bir seferde daha büyük baytları şifreler. Bir anahtar girişi, giriş anahtarı bilgisi olmadan tahmin edilemeyen 8 bitlik bir akış numarası üreten sözde rasgele bit oluşturucudur. Oluşturucunun çıkışına anahtar akışı denir ve X- kullanılarak düz metin akış şifresiyle her seferinde bir bayt birleştirilir (Gonsai and Raval 2014).

RC4 ilk olarak 2003 ve 2013 yıllarında RC4'te ciddi güvenlik açıkları bulunana kadar SSL/TLS ve WEP gibi birçok uygulamada kullanıldı. RC4 WEP'te kullanıldığından, saldırganlar onu istedikleri sıklıkta kırma pratiği yapma şansına sahip oldular. 2013 yılında RC4'te, 2011'de keşfedilen bir şifreli blok zincirleme sorunu için bir geçici çözüm olarak kullanılırken başka bir güvenlik açığı keşfedildi. Şifreli blok zincirleme, RC4'ün kullanmadığı blok şifreleri tarafından kullanılan bir işlem modudur.

Bir grup güvenlik araştırmacısı, önceki RC4 saldırısında gerekli olan işlem gücünde yalnızca küçük bir artışla RC4'ü aşmanın bir yolunu buldu. Bu ve daha sonra bulunan daha küçük güvenlik açıkları nedeniyle, RC4 şifreleme algoritması artık kullanılması önerilen bir şifreleme değildir (Eli Biham 2008).

3.1.4.3. Rivest Cipher 6 Algoritması

Kriptografide RC6, RC5'ten türetilen simetrik bir anahtar blok şifresidir. Gelişmiş Şifreleme Standardı (AES) yarışmasının gereksinimlerini karşılamak için Ron Rivest, Matt Robshaw, Ray Sidney ve Yiqun Lisa Yin tarafından tasarlandı. Algoritma beş finalistten biriydi ve ayrıca NESSIE ve CRYPTREC projelerine de sunuldu. RSA Security tarafından patentli tescilli bir algoritmadır(Akif 2012). Genel olarak RC6, RC5'in güvenliğini artıran bir gelişmedir. Döneminde en çok kıyaslandığı algoritma AES algoritması oldu. Patentli bir algoritma olmasına karşın, geleneksel şifreleme mekanizmaları üzerine kurulması ve AES algoritmasının oldukça yüksek güvenilirliği AES ile olan şifreleme yarışmasını kaybetmesine yol açtı(Ye Yuan 2018).

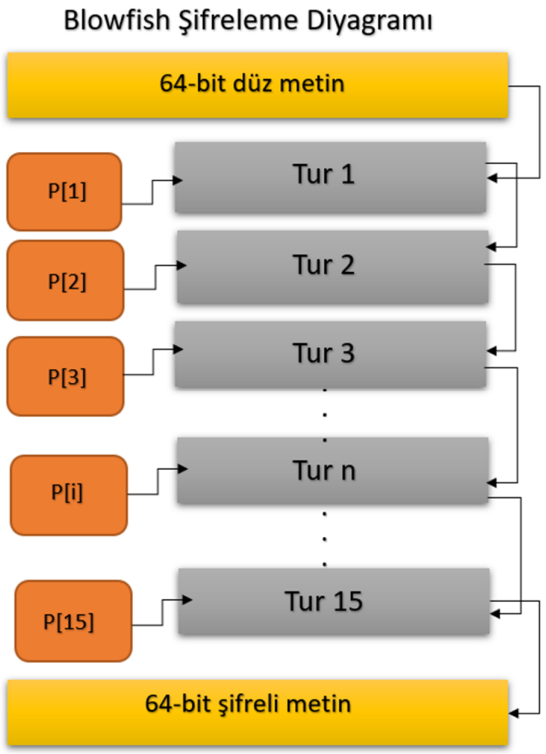
Uygun RC6, 128 bitlik bir blok boyutuna sahiptir ve 128, 192 ve 256 bitlik anahtar boyutlarını destekler, ancak RC5 gibi, çok çeşitli kelime uzunluklarını, anahtar boyutlarını ve tur sayısını desteklemek için parametrelendirilebilir. RC6, veriye bağlı döndürmeler, modüler toplama ve XOR işlemleri kullanarak yapı olarak RC5'e çok benzer; aslında, RC6, iki paralel RC5 şifreleme sürecini iç içe geçmiş olarak görülebilir. Bununla birlikte, RC6, dönüşü yalnızca en az anlamlı birkaç bite değil, bir kelimedeki her bit'e bağımlı kılmak için RC5'te bulunmayan ekstra bir çarpma işlemi kullanır.

3.1.5 Blowfish Algoritması

Blowfish algoritması 64 bitlik blok boyutuna sahiptir. Diğer simetrik şifreleme türlerinde yaygın olarak kullanılan Feistel ağını kullanır. 32 bit ile 448 bit arasında değişen anahtar uzunluklarına sahiptir. 1993 yılında B.Schneier tarafından geliştirildi. Blowfish ilk olarak diğer algoritmaların çıkış noktası olan DES algoritmasının artık isterleri karşılayamamasından dolayı yola çıkıldı ve o yüzdne geliştirildi. Blowfish algoritması döneminde şifreleme teknikleri bir sır gibi saklandığı zamanda bile herhangi bir patent hizmeti olmadan kamuya açık şekilde çıkış yaparak adından oldukça söz

ettirdi. Hatta bu konuyla ilgili B.Schneier şu şekilde bahsetti : " Blowfish, patentsizdir ve tüm ülkelerde bu şekilde yer alacaktır. Algoritma genel kamusal alanda bulunmakta olup, herkes tarafından özgürce kullanılabilir" (Alabaichi, Ahmad et al. 2013). Herkese açık olması ve özellikle patentsiz olması Blowfish ve Blowfish'in geliştirilmiş çeşitli varyasyonlarının iyileşmesine olanak sağladı.

Blowfish algoritmasının en dikkat çekici özelliği anahtar bağımlı olarak değişen S-kutuları (S-boxes) ve onlara karşılık gelen karıştırılmış anahtar düzlemidir. Şekil 1.5'de 16 adımdan oluşan Blowfish algoritmasının akış diyagramı verildi.



Şekil 1.5. Blowfish Algoritma Yapısı

Blowfish algoritması; başlangıçta toplama, tablolar arası arama ve XORlama işlemlerini içermektedir. Tablo şunları içerir: 4 adet S-kutusu (S-boxes) ve P dizisi (P-array). DES'te kullanılan F fonksiyonu yapısı gibi bir yapısı vardır. Fakat DES'i basitleştirerek daha stabil ve güvenli şekilde kullanmak için etkin bir algoritmadır.

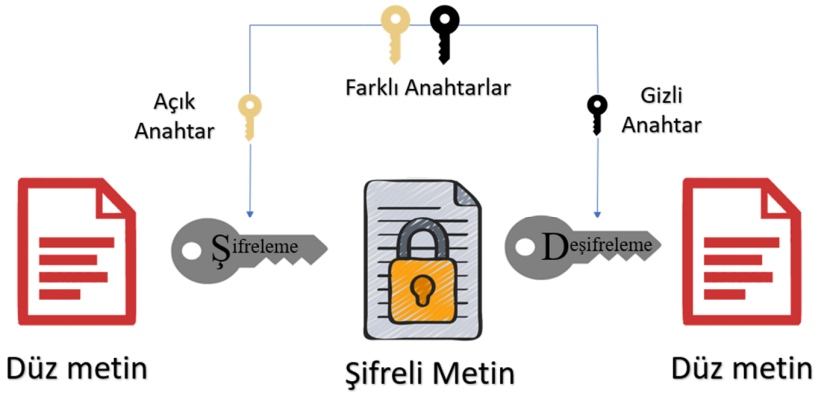
Blowfish algoritmasının mevcut sistemlere entegrasyonunda alt anahtar oluşturma ve veri şifreleme gibi farklı adımları bulunmaktadır. Blowfish bununla birlikte anahtarda şu uygulamaları barındırır: Anahtar uzun süre sabit kalabilir ve iletişim bağlantısı şifrelenmelerinde kullanılabilir ya da anahtar sık sık değişebilir ve paket değiştirme şifrelenmelerinde kullanılabilir(Mandal 2012).

İletişim bağlantısı şifreleme, bir ağ boyunca ilerleyen bir iletişimin her aşamada veya düğümde şifrelendiği ve şifresinin çözüldüğü bir tekniktir. Trafik analizini önlemek ve insan hatasını önlemek için kullanılır (Zhang 2012).

Paket değiştirme şifreleme ise, hedef taraftaki paket işleme cihazındaki uçtan uca kimlik doğrulamaya ek olarak, paket aktarım yolundaki her bir ara paket işleme cihazındaki bağlantıdan bağlantı kimlik doğrulaması kullanılır ve bu şifreleme yoluyla yapılır (Y.Zhou 2021). 32 bitlik 18 adet alt anahtar bulunmaktadır ve bu alt anahtarlar P dizisinde toplanır ve P1, P2, P3....P18'e kadar devam edecek şekilde numaralandırılır. F fonksiyonu için 4 adet S-kutuları (yer değiştirme kutuları) kullanılır. Veriler, fonksiyonun 16 defa kullanılmasıyla şifrelenir. Bu turlar boyunca sürekli benzer işlem uygulanır ve veriye göre değişkenlik gösteren S-kutuları ile yer değiştirmeler yapılır ve algoritma tamamlanmış olur.

3.2 Asimetrik Şifreleme

Asimetrik şifreleme algoritmaları simetrik şifreleme algoritmalarından anahtar farklılığı yönünden ayrılmaktadır. Asimetrik şifreleme algoritmalarında açık (public) ve özel (private) anahtar olmak üzere iki adet anahtar kullanmaktadır. Asimetrik algoritmalara ayrıca açık anahtarlı algoritmalar da denmektedir. Asimetrik algoritmalar da gönderici ve alıcı arasında iletiyi şifrelemek ve şifreyi çözmek için iki ayrı anahtar bulunmaktadır.

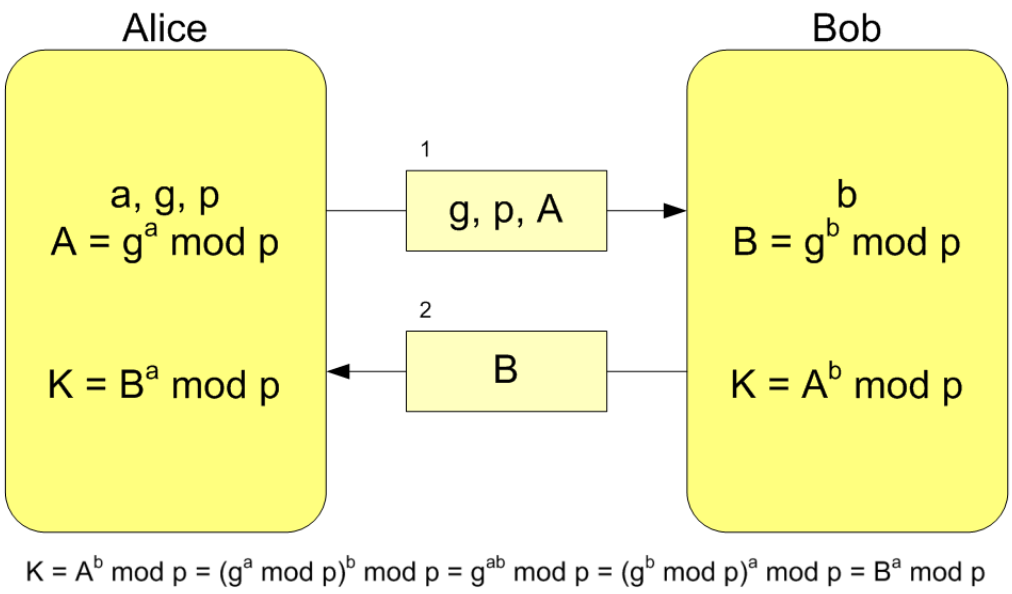


Şekil 1.6. Asimetrik Şifreleme Algoritma Yapısı

Açık anahtar şu anlama gelmektedir: Şifreleme anahtarı genel kullanıma açıktır. Yani şu şekilde ilerlemektedir. Public anahtar bilinebilir fakat private anahtar bilinemez. Bu herkese özel eşsiz (unique) bir anahtardır. Public anahtardan yola çıkarak private anahtara geçiş yapmak mümkün değildir. Şifrelenmiş bir iletiyi görmek için şifreyi çözmek için gerekli olan anahtara sahip olmak asimetrik şifreleme algoritmalarında şarttır (Joseph, Krishna et al. 2015).

3.2.1 Diffiee – Helman Algoritması

Diffiee – Helman (D - H) Algoritması, Whitfield Diffiee ve Martin Hellman'ın algoritmaya adlarını verdikleri ilk asimetrik şifreleme algoritması olarak bilinmektedir. 1976 yılında yayınlanan "New Directions in Cryptography" isimli makalelerinde yer aldı ve bulunan bu algoritma anahtarların değişimi prensibine dayanmaktadır (T. Yerlikaya 2006). Güvensiz bir iletişim hattı kullanmasıyla dikkat çeken D-H, ortak bir hat üzerinden yine ortak bir gizli anahtar üretilmesini sağlar. Bu üretilen gizli anahtar iki taraf arasındaki iletişimi şifreler ve çeşitli saldırılardan korumayı amaçlar. Mantıksal olarak bakıldığında oldukça basit duran bu algoritma 1980'li yıllarda oldukça popüler olmuştur (Dan Boneh August 17, 2015).



Şekil 1.7. Diffie-Hellman Algoritma Yapısı(Wikipedia 2014)

Diffie-Hellman ortak gizli anahtar oluşturma sistemi ayrık logaritma problemi temeli üzerinde şekillendi ve güvenirliği çok büyük asal sayıları seçmeye dayanmaktadır. Eğer p yeteri kadar büyük bir asal sayı olursa, bu ayrık logaritma problemini zorlaştırır ve çözmek çok mümkün değildir.

D-H algoritmasında kısa bir şekilde ortak anahtar yaratma adımlarını inceleyecek olursak:

• A kişisi gönderici olarak nitelendirelim ve A, $0 \leq a \leq p-2$ eşitsizliğini sağlayan ve rastgele olan bir a sayısı seçilir. Burada $c = g^a \pmod p$'yı hesaplar ve bunu B değişkenine gönderir.

• B kişisini alıcı olarak nitelendirelim ve B, benzer şekilde, $0 \leq b \leq p-2$ eşitsizliğini sağlayan ve rastgele olan bir b sayısı seçilir. Burada $d = g^b \pmod p$'yı hesaplar ve bunu A değişkenine gönderir.

• A değişkeni, ortak anahtar olan k değerini ise şu şekilde hesaplar: $k = d^a = (g^b)^a$

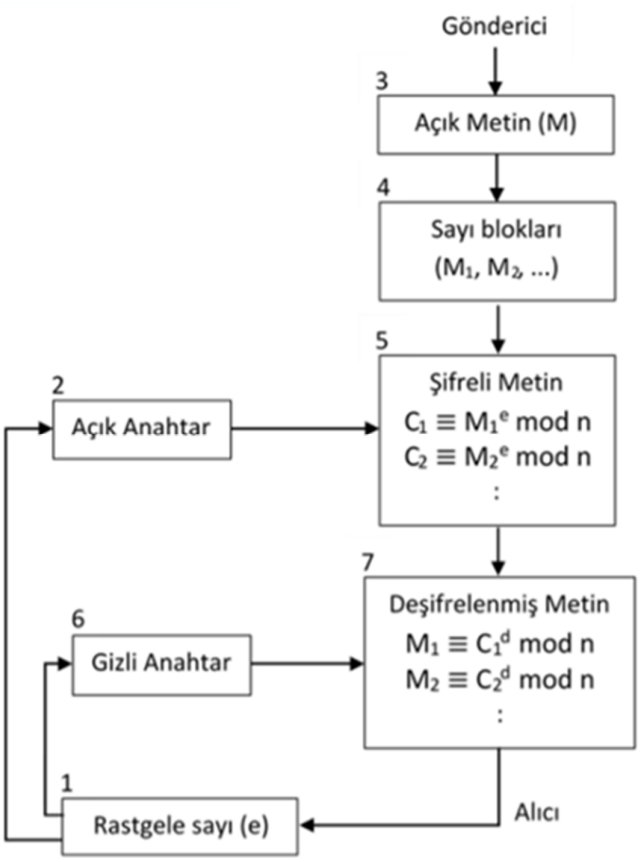
• B değişkeni, ortak anahtar olan k değerini ise şekilde hesaplar: $k = c^b = (g^a)^b$

Böylelikle A ve B aralarında ortak bir anahtar olan k için anlaşmış olurlar (T. Yerlikaya 2006).

3.2.2 RSA Algoritması

RSA Algoritması (Rivest-Shamir-Adleman Algorithm) asimetrik bir şifreleme algoritması olan RSA, 1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından geliştirilmiş ve algoritma ismini onu geliştiren kişilerden aldı. Algoritma üzerinde geliştirmeler yaptıktan sonra asimetrik şifreleme algoritmalarına uygun olacak şekilde geliştirildi. RSA şifreleme algoritması açık anahtar şifreleme düzenine sahip bir şifreleme algoritmasıdır.

En önemli adımları sırasıyla; Anahtar oluşturma (Key generation), Şifreleme işlemi (Encryption process), Deşifreleme işlemi (Decryption process) şeklindedir (Sheba Diamond Thabah 2019). RSA şifrelemesi, simetrik şifreleme ve diğer şifreleme türlerinden bu yana günümüze bu kadar uygulanan en güçlü ve popüler kripto sistemlerden biridir (Sani 2017).



Şekil 1.8. RSA Algoritma Yapısı(A. Beskirli 2019)

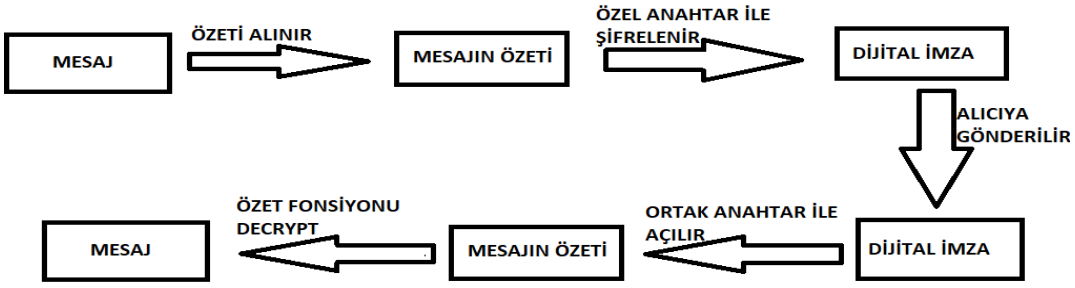
RSA temel mantığı şu şekilde ilerlemektedir: Herhangi bir tam sayıyı çarpanlarına ayırmaktansa bu tam sayıyı, yine onun gibi sayılarla çarpmaya göre daha zor olacağını savunmaktadır. Birbirlerinden farklı iki asal ve özellik büyük sayıyı çarparak, oluşan değeri pivot değer olarak kullanma mantığına dayanır. Bu belirlenen pivot değer eğer çarpanlarına ayrılabilen kolay bir değer ise özel anahtar (private key) bilinebilirliği ve tahmin edilmesi kolaylaşır. İşte tam da burada anahtar boyutunu iki ya da üç katına çıkarmanın özel anahtar bilinmesinin önüne geçip şifrelemeyi güçlendirdiği savunulmaktadır.

Fakat bununla birlikte RSA'in düzeltilmesi gereken sorunları olduğunu düşünen araştırmacılarda vardır. A.Chmielowiec, RSA'in mevcut formülüzasyonunda neye göre rastgele olarak verildiği hakkında bilgi verilmediğini ve bunun düzeltilmesini gerektiğini savundu (Chmielowiec 2010).

Farklı görüşler olmak ile birlikte, RSA asimetrik şifreleme algoritmaları arasında oldukça popüler bir algoritmadır. RSA algoritmasının kırılabilmesi kolay gibi gözükse de oldukça güçtür. Ortadaki Adam (Man in the middle) saldırılarıyla veya farklı saldırı yöntemleriyle yakaladığı açık anahtara ait olan bir gizli anahtar bulabilmesi gerekmektedir. Eğer bu kişi özel anahtarı yakalarsa karşıdaki kişinin mesajını okuyabilir, alıcı kişiymiş gibi karşı tarafa mesajlar atabilir. Bu işlemi matematiksel olarak yapmanın yolu ise n'in asal çarpanlarına ayrılması ve p ve q değerlerini hesaplayarak mümkün olmaktadır. P, q ve açık üs e kullanılarak d değeri hesaplanabilmektedir. Fakat RSA'i güvenli kılan ve güvendiği kısım ise n modülünün çarpanlarına zor ayrılmasıdır. RSA sisteminin güvenlik mekanizması çok büyük sayıların asal çarpanlarına ayrılmasının zorluğu varsayımına dayanmaktadır. N değeri ne kadar büyük olursa algoritma mekanizması o kadar kuvvetli olacak ve bu şifrenin kırılması o kadar zorlaşacaktır (Günden 2010). Günümüzde kişisel bilgisayarlar veya kuantum bilgisayar gibi hesaplama eşiği yüksek bilgisayarda bile oldukça zaman almaktadır.

3.2.3 Dijital İmza Algoritması (Digital Signature Algorithm - DSA)

Dijital İmza Algoritması (Digital Signature Algorithm veya DSA) 1991 yılında Ulusal Standartlar ve Teknoloji Enstitüsü(NIST) tarafından dijital imza algoritması olarak tasarlandı. RSA algoritmasına benzer şekilde ortak anahtar şifreleme yöntemlerini kullanır. Bu, verilere eklediğimiz tek yönlü özet (hash) değiştirerek verilerin değiştirilme prensibine dayanan bir algoritmadır.

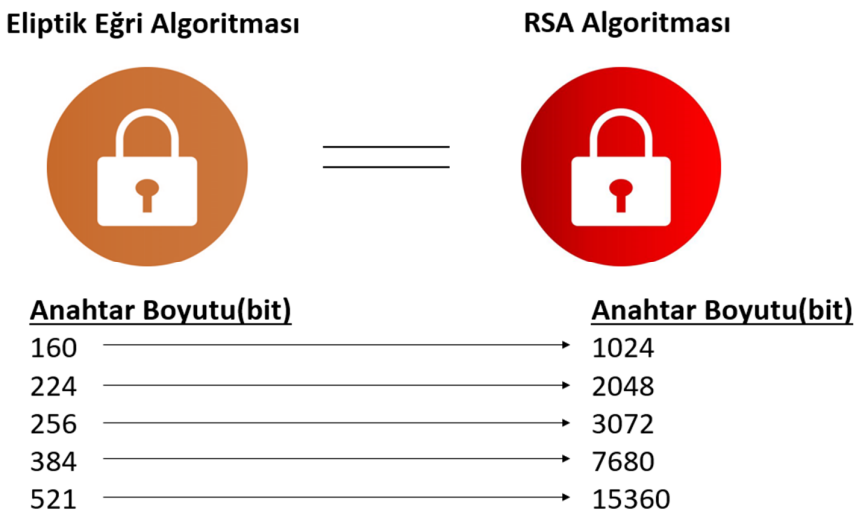


Şekil 1.9. Dijital İmza Algoritma Yapısı (Özdemir 2020)

Şekil 1.9'da görüldüğü gibi öncelikle mesaj özeti alınır daha sonra bu mesaj özeti şifrelenir. Dijital olarak imza kullanılır ve bu dijital imza ile birlitke karşı taraftaki alıcıya gönderilir. Bu imza ortak anahtar ile açılabilir şekildedir. Mesaj özeti alınır ve tek yönlü özet (hash) üzerinden deşifreleme işlemi yapılır ve ana mesaja ulaşılır.

3.2.4 Eliptik Eğri Şifreleme Algoritması (Elliptic Curve Algorithm - ECC)

Eliptik Eğri Şifreleme (Elliptic Curve Cryptography), bir logaritmik problem üzerine kurulmuş asimetrik şifreleme algoritmasıdır. ECC algoritması, ECC kod baytlarının uzunluğuna bağlıdır ve buna göre güçlü ya da güçsüz bir şifreleme yaptığından söz edilir (Zhang 2012). ECC algoritması aynı kategoride olduğu için sürekli asimetrik bir şifreleme algoritması olan RSA ile kıyaslanır. RSA deki yüksek anahtar boyutuna karşın, ECC de oldukça küçük anahtarlar vardır. Örneğin 1024 bit RSA anahtar uzunluğuna sahip bir anahtarın ECC de ki karşılığı yalnızca 160 bit uzunluktadır. Kısa anahtarlarda yüksek şekilde güvenlik sunan RSA anahtar uzunluğunun daha fazla olduğu yerlerde ise tercih edilmemektedir(A. Yücelen 2017).



Şekil 2.1. Eliptik Eğri Algoritması ve RSA Algoritması Anahtar Boyutu Kıyaslaması

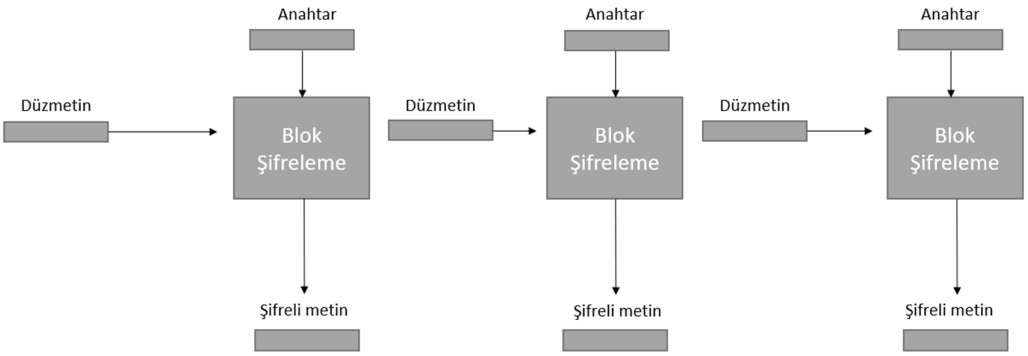
ECC, küçük anahtar kullanımına sahip olduğu diğer şifreleme algoritmalarına göre hız ve sertifika bilgisi hızı yer alır. Özellikle işlem gücü,makine üzerindeki saklama alanı ve buna bağlı olarak makinenin güç tüketiminin önemli olduğu koşullarda ECC tercih edilir. Özellikle son zamanlarda akıllı kartlar, cep telefonları, sayısal postalama işaretleri gibi zorunlu ortamlara tam olarak uygun olduğudur(T. Yerlikaya 2006).

3.3 Şifreleme için Gizlilik Modları

Blok şifreleme için çeşitli çalışma modları bulunmaktadır. Bunlar tercih edilen algoritmaya göre ve duruma göre değiştirilebilir modlardır. Gizlilik ve bütünlüğü korumak için bu modlar özellikle tercih edilmektedir.

3.3.1 Elektronik Kod Kitabı (Electronic Code Book - ECB)

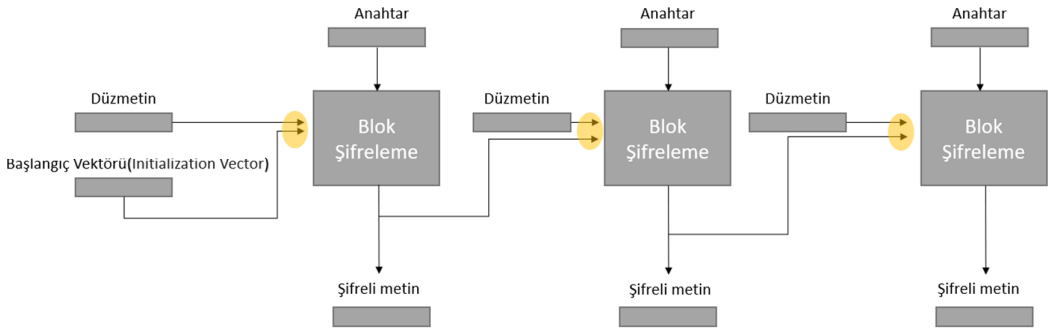
Bir blok şifreleme mekanizması, n bitin katı olan mesajları ayrı ayrı şifrelemektedir. ECB en temel şifreleme modlarından biridir. ECB diğer şifreleme modlarına göre güvenlik yönünden daha zayıftır. Her biri birbirinden bağımsız şifrelenen ilkel bir yöntemdir. Bu yüzden ECB her yerde kullanılması gereken bir gizlilik modu olarak görülmemelidir (Rogaway 2011).



Şekil 2.2. Elektronik Kod Kitabı Modu Akış Diyagramı

3.3.2 Şifre Blok Zincirleme(Cipher Block Chaining- CBC)

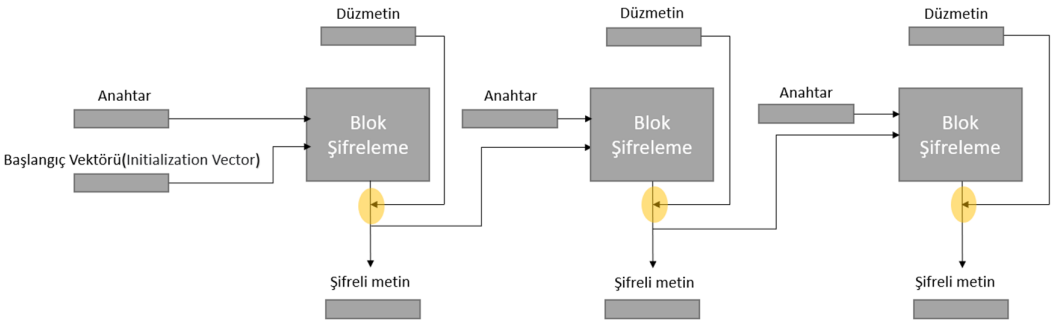
Şifre Blok Zincirleme, IV tabanlı bir şifreleme olan bir gizlilik modudur. Rastgele IV seçilerek şifreyi kuvvetlendirmeyi amaçlar. XOR işlemi yapılarak bir önceki blok ve sonraki blok arasında geçiş yapılır. Her bloktan gelen şifrelenmiş metinin XOR'lu hali ile elde edilir(Rogaway 2011).



Şekil 2.3. Şifre Blok Zincirleme Modu Akış Diyagramı

3.3.3 Şifreli Geri Bildirim Modu (Cipher Feedback Mode - CFB)

IV tabanlı bir şifreleme şeması olan CFB gizlilik modu, rastgele bir IV varsayarak rastgele bitlerden ayırt edilemezliği ve tahmin edilemezliği sağlar. IV tahmin edilebilirse veya şifrelenmemiş bir kod tarafından yapılmışsa, gizlilik sağlanmaz. CFB gizlilik modunda bloktan elde edilen şifrelenmiş sonuç, bir sonraki bloklar ile işleme sokulur ve genel akış tamamlanmış olur (Rogaway 2011).

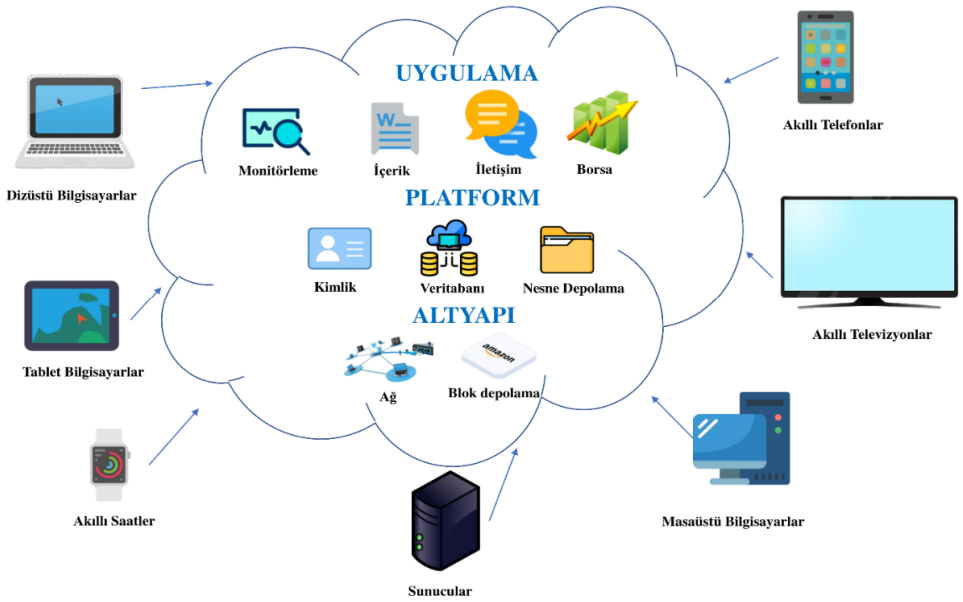


Şekil 2.4. Şifreli Geri Bildirim Modu Akış Diyagramı

4. BULUT BİLİŞİM

Bulut bilişim en kısa ve sade tanımıyla, Bilişim Teknolojilerine ait kaynaklara ihtiyacı olan kişiler veya kurumların talepleri doğrultusunda talep edilen BT kaynaklarını internet üzerinden çeşitli bulut servis sağlayıcıları tarafından ücret karşılığında ulaştırılmasıdır (M.G.Avram 2014).

Özellikle fiziksel sunucuları almak, felaket senaryoları için çeşitli lokasyonlarda veri merkezleri kurmak yerine bu hizmetler internet üzerinden servis edilir.



Şekil 2.5. Bulut Bilişim Yapısı

Günümüzde birçok cihaz bulut sistemler ile entegre olarak çalışmaya başladı. Bugünün dünyasında artık her şey internete bağlanabilen ve doğrudan internet üzerinden haberleşen araçlar ile fazlaca etkileşimdedir. Bu cihazlar, çeşitli verileri okur, yazar ve depolayabilir. Bu ve bunun gibi birçok işlemi ortaklaşa yapabilen ya da yöneten sistemler bulut bilişimi beraberinde getirdi. Bulut kavramını şu an ve daha öncesinde öncülüğünü Amazon şirketi yaptı. 2006 yılında bulut kavramının ve servislerin ilk kullanımı kabul edilip, neredeyse her yıl yeni servis ve ortam geliştirmeleriyle dinamik olarak gelişen bir alandır. Şu an mevcut olarak 200+ amazon

servisi bulunmaktadır(Amazon 2018). Bunlar işlem gücü veya veri depolaması için kullanılabilen farklı servis ve servis gruplarıdır.

Bulut kavramı birden çok kavram ile anlatılabilir. Bunun için genel geçer bir tanım olmamakla beraber, Bulut Servis Sağlayıcılarının her biri kendine göre en kısa tanımlarla bulut sistemini açıkladılar.

Amazon, bulut bilişim için BT kaynaklarının internet aracılığıyla , gelen isteklere göre ve kullandığın kadar öde prensibiyle ücretlendirerek hizmet verilmesi olarak ifade etmektedir(Amazon 2018). Microsoft ise, Bulut kavramının her bir ağı benzersiz bir fonksiyonelliğe sahip küresel bir sunucu ağını tanımlamak için kullanılan bir terim olduğunu belirtmektedir. Bulut kavramının fiziksel bir varlık olmadığını, aksine dünya üzerinde birbirine bağlandığını ve tek bir ekosistem çatısı altında birleştirilmesi amaçlanan geniş bir uzak sunucu ağı şeklinde tanımlar (Microsoft 2018).

ABD Ulusal Standartlar ve Teknoloji Enstitüsü, Bilgi Teknolojisi laboratuvarı tarafından bulut bilişim şu şekilde açıklanır: Her yerde kullanılabilen, oldukça kullanışlı, istendiği zaman ağ erişimine açık, yapılandırılabilir ve sürdürülebilir bir işlem havuzu olarak nitelendirilir (Grance 2011, Birgul Kutlu 2016). S.Blabeva ve T. Wozniak tarafından bulut bilişim için şu ifadeler ile kullanıldı: Bulut bilişim, BT altyapılarının ve uygulamaların bulut servis sağlayıcı tarafından hizmet olarak sağlanmasıdır. Bunlar ölçeklenebilir olarak sunulur (Stanoevska-Slabeva and Wozniak 2010).

Bugüne gelindiğinde, özellikle yeni kurulan şirketler veya kurumsal olarak giderek büyüyen şirketlerin, artık çok miktarda yönetilmesi gereken karmaşık sistemleri tek bir elden kullanmak isteme ihtiyacı doğdu. Özellikle start-up firmaları yönünden fazlaca bir sermaye olmadan bir proje kapsamında belirli hizmetler ve temel altyapıyı sağladığı için günümüzde oldukça tercih edilen ve işleri kolaylaştıran bir modeldir.

Genel olarak bakıldığında bulut için; kullanıcı merkezli olduğu, görev odaklı çalıştığı, akıllı ve programlanabilir bir ortam olduğunu söylemek mümkündür (Mirashe and Kalyankar 2010).

Bulut bilişim mobil cihazlar, akıllı saatler veya taşınabilir ve internet bağlantısı olan günümüz cihazları gibi önemli dijital cihazlara etkileşim gücü veren altyapı hizmetini sunar. Nesnelerin İnterneti, Büyük Veri ve Yapay Zeka gibi yükselen çalışma alanlarını hızlandırır, yönetir ve depolar. Bundan dolayı bu alanlardaki mevcut endüstri dinamiklerini hızlandırmak, dijital dönüşüm yolundaki en büyük engelleri ortadan kaldırır ve al, uygula ve yönet modeliyle bunu birleştirir (Sunyaev 2020).

Bulut bilişim faydaları şu şekilde listelenebilir:

- Dağıtık olarak farklı noktalardaki fiziksel sunucu ya da veri merkezlerini alarak bu hizmetleri yönetmesi,
- Sunucu ya da veri merkezlerinin yedeklemelerini sağlaması,
- Felaket senaryolarının önüne geçmesi ve engel olabilecek çözümleri listelemesi,
- Kullanıcı ya da şirketlere hizmeti aldığı bulut servis sağlayıcının imkanı doğrultusunda bir kullanıcı ara yüzü sağlaması,
- Birbirinden tamamen aykırı noktalarda sunucuları bir bütün olarak görüp birbirleri üzerinden çeşitli uygulamalar veya servisler ile iletişime geçtiğini görüntüleme imkanı bulmak,
- Yüksek ölçekli servislerde hız olarak normal sunucu ya da internet ağlarından daha hızlı olması,
- Donanım imkanları veya herhangi bir altyapı hizmeti olmadan yapay zeka, makine öğrenmesi gibi özel faaliyetlerde de hizmet verebilmesi

Liste farklı servisler ve kullanım doğrultusunda farklılaşabilir fakat genel olarak bulut bilişimin temel faydaları bu şekildedir.

Bulut bilişim için güncel bir örnek olarak şu verilebilir : Günümüzde oldukça popüler olan e-ticaret uygulamaları mevcut olarak büyük kitlelerce kullanılmaktadır. Bu uygulamalara günde milyonlarca, aylarda ise milyarlarca istek gelmektedir. Bulut bilişime ait özel bir servisle, belirli bölgelerde olmak şartıyla bir ürün eğer belirli bir limitten fazla gösterim alıyorsa, bunu servis tekrar tekrar çağırıp sunucuyu yormaktansa bulut bilişimin ön bellek servisi sunarak kullanıcıları yavaşlıktan ve arka taraftaki e-ticaret sistemindeki teknik kadroyu büyük bir zahmetten kurtarmaktadır. Direk ön

bellekten gelen herhangi bir ürün, ürün görseli çeşitli ülkelerde aynı anda dağıtılmakta ve sunucular arası adeta bir dosya transferi gibi servisler olmadan haberleşebilmektedir.

Bununla birlikte bulut ortamlarında bulut hizmet sağlayıcının imkanları ölçüsünde sayısız servis ve alan bulunmaktadır. Tüm ücretlendirmeleri görmek ve yine bunları yönetmek için bile ayrı servis hizmetleri bulunmaktadır. Kullanıcı veya şirket isterse herhangi bir ücret aşımı yaşamadan bilgilendirilir, buna göre aksiyon alması gereken yerlerde talimat verebilir.

Aslında manuel olarak gözüken bu sistemlerde arka tarafta bir yapa zeka mekanizması çalışmaktadır. Örneğin çok trafikli bir işlem hacmi olan bir uygulamada sunucular çok fazla yüke maruz kalır. Bulut ortamına verilen talimatlarla sizin yerinize paranızı yönetir ve size en uygun geçici bir sunucu satın alır. Buradaki yükü dağıttıktan sonra tekrardan eski haline dönüş yaparak en etkin bir şekilde kullanmaya çalışır.

Bunlar ve bunun gibi hizmetleri olan bulut bilişim, yeni dünya düzeninde daha fazla etkin olmaya ve gelişmeye devam edecektir. Yeni teknolojilerin; özellikle metaverse gibi sanal dünya kavramlarının yakında her biri için ayrı servisler ile bulut bilişim ile entegre olacağı ve sonrasında yapay dünya adı verilen *meta* kavramı ile iç içe olacağını öngörülmektedir.

4.1 Bulut Bilişim Tarihçesi

1963'te İleri Savunma Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency), Massachusetts Teknoloji Enstitüsü (Massachusetts Institute of Technology) MAC Projesi için 2 milyon $ bütçe ayırdı. Bu verilen bütçe kaynakları çoğaltmak için tasarlanan bir projenin eseriydi. Verilen bütçe, MIT'nin bir bilgisayarın aynı anda iki veya daha fazla kişi tarafından kullanılmasına imkan veriyordu. Bu şekilde ikili programlama (pair-programming) adımlarını gerçekleştirmek isteniyordu.

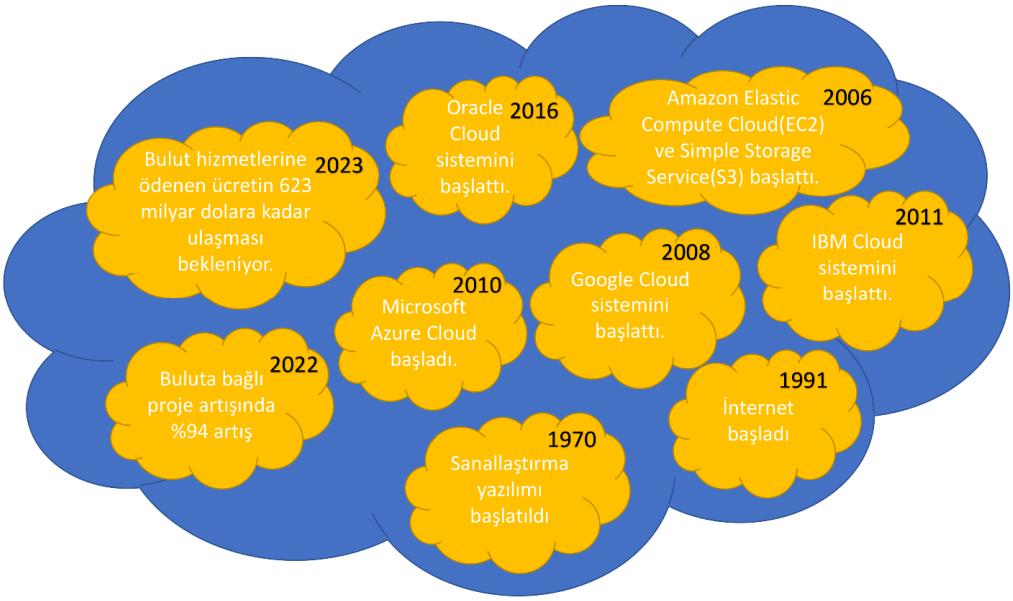
Bunu aynı anda yapan arkaik bilgisayar olarak da adlandırılan bir sistem geliştirildi ve günümüzdeki bulut kavramanın en ilkel yapısı olarak görüldü. İki veya daha fazla kişinin erişebildiği bu bilgisayar sistemi fiziksel alanı paylaşmak ve bunu sanallaştırmanın bir yolu olduğu fikrini gündeme getirdi. Aslında tam da burada

“Sanallaştırmak ya da Sanallaştırma” denilen yeni bir teknolojinin ilk temelleri atıldı. Fakat o zaman ki sanallaştırma sadece birden fazla paylaşıma izin veren kısıtlı bir anlam ifade ederken 1980 ve sonrasında kapsamı genişlemiş ve günümüze kadar başta bilgisayar sistemleri olmak üzere tüm alanlar içinde genişleyerek devam etti (Swati I. Bairagi 2015).

1969'da J. C. R. Licklider, İnternet'in gelişmemiş bir versiyonu olan İleri Araştırma Projeleri Ajansı Ağı (Advanced Research Projects Agency Network)‘nın geliştirilmesine yardımcı oldu. JCR bilgisayar bilimcisiydi ve gezegendeki herkesin bilgisayarlar aracılığıyla birbirine bağlanacağından bahsetti. İnternet olarak da bilinen “Galaksiler Arası Bilgisayar Ağı”, buluta erişim için gereklidir. ARPANET aldığı devlet destekleri ve JCR’nin özverili çalışmalarıyla ağ giderek genişledi ve 70 yıllarda adından oldukça sık söz ettirdi.

1970-1970 arası, Sanallaştırmanın kapsamı dar ve tam vurgulanamayan anlamı, 1970'lerde değişmeye başladı ve tamamen işlevsel bir işletim sistemine sahip gerçek bir bilgisayar gibi davranan sanal bir makinenin oluşturulmasını dayandırıldı.
Sanallaştırma teriminin kapsamı giderek büyüyerek bir hizmet aracına dönüştü ve fiziksel sunucuların üzerine sanal sunucular kurularak hem yerden, hem maliyetten tasarruf edildi. Ayrıca internet ile birlikte paralel olarak gelişti ve 1990-2000 yılları arasında günümüzdeki bulut bilişim alt yapısının temelini oluşturan önemli bir kavram olarak ortaya çıktı.

1990 ve sonrası, bulut bilişim tamda bu yıllarda hala soyut olarak gelişmeye devam ediyordu. Sanallaştırma kavramının üzerinde inşaa edilmiş fakat havada bir kavramdı. Aslında o zaman kullanılan teknik alt yapı bulut mimarisinin daha basit verisyonlarıydı fakat kimse buna bulut ya da başka bir isimle nitelendirmiyordu. Son kullanıcı ile sağlayıcı arasındaki boşluğu ifade etmek için kullanıldı. Bulut bilişim o zamanki teknolojik altyapılar düşünüldüğünde yeni bir soluk getirmiş olup yeni bir mekanizma olduğu ve işleri oldukça kolaylaştırdığı konusunda hem fikir olundu.



Şekil 2.6. Bulut Bilişim Tarihçesi

1991'de İnternet'in keşfiyle tamamen haberleşme ve uygulamaların popülerliliği artmış birbirleri ile bir şekilde iletişime geçmesi zorunlu olan alanlar oluştu. Bu yaşanan gelişmeler ise bulut ekosistemini geliştiren ve destekleyen büyük firmaların; Salesforce, Amazon, Microsoft vs. bu alana AR-GE yatırımları yapmaları ve giderek büyüyen bu sektörün öncülerinden olmalarını sağladı.

1999 yıllarına gelindiğinde, Salesforce bulut bilişimi kendi sistemlerine entegre etti ve dünyada büyük yankı uyandırdı. Özellikle CRM alanında verdiği faaliyetleri son kullanıcıya ulaştırdı ve bunları internet aracılığıyla gerçekleştirdi. Dünyada artık internet kullanımı oldukça arttı ve dünyanın neresinde olursa olsun bu uygulamaya erişilebilir olduğu kanıtlandı. Bu da yine hem zaman yönünden oldukça büyük tasarruf sağlamış olup, hem de maliyet açısından herhangi bir yere gidip kurulum yapmadan mevcut uygulamayı kullanmanın bütçesel katkılarının olumlu olduğu gözlemlendi.

2000 ve 2006 yılları arası, 2000 li yıllarda son kullanıcıya internet üzerinden verilen hizmetlerin çeşitliliği oldukça arttı. İvmelenen bu sektörde herkes yerini alıyor ve çoğu alt yapısını internet üzerine kurmaya başlıyordu. Daha sonra adından sıkça söz ettirecek olan Amazon, web tabanlı perakende hizmetlerini tanıttı. Web tabanlı perakende hizmetleri giderek gelişti ve onlara büyük esneklik yarattı. Artık mevcut bilgisayarlar, sunucuları çok daha efektif kullanıyor ve geri dönüşleri alıyordu.

2006 yılına gelindiğinde, sonraki dönemler için devrim niteliğinde olan, Amazon Web Hizmetleri piyasaya sürüldü. Amazon bununla birlikte web sitelerine ve Amazon müşterilerine çeşitli hizmetleri sunmaya başladı. Bulut bilişim adının daha vurgulu telaffuz edildiği bu yıllarda Amazon'un ilk servislerinden olan "Amazon S3 Bulut Depolama" adında yeni bir servis tanıttı. Bu servis adın da anlaşılabileceği gibi basit bir depolama hizmetini çevrimiçi olarak veriyordu. Hemen ardından ise "Amazon Elastik Bilgi İşlem Bulutu (Amazon Elastic Compute Cloud – Amazon EC2) " adında ikinci bir servis tanıttı. Bu hizmet ise sanal bilgisayarlar kiralanmasını ve kullanıcı ya da şirketlerin kendi mevcut programlarını ya da uygulamalarını çalıştırmalarına olanak sağladı. Ayrıca "Amazon Mechanical Turk" adlı Amazon Web Services sitelerinden biri, depolama, hesaplama ve "insan zekası" dahil olmak üzere çeşitli bulut tabanlı hizmetleri sunuyordu(Surbiryala and Rong 2019).

2008 ve Google, Bulut sektöründe yerini almak isteyen ve güçlü bir altyapısı olan Google, "Google Dokümanı hizmetleri" adında bir servis tanıttı. Bunlar iki ayrı tipte servislerdi. Google yenilik olarak elektronik E-tablo hizmetini sunmuştu. Bu e-tablo hizmetlerinde belgelere bir şeyler yazılabilir, kayıt edilebilir ve düzenlenebilirdi. Tabi yine bunu da kullandığın kadar öde prensibiyle yapan Google, aslında e-tablo alanını kiralama işlemi gerçekleştiriyordu. Zaten bunun hemen öncesinde sektörün buraya doğru kaydığını ve geliştiğini gören Google, piyasayı yakalamak ve geç kalmamak için "Google E-Tablolar" hizmetini başka firmadan satın aldı. Daha sonra Writely'yi satın alarak bu belgeleri aktarılmasına olanak sağladı. Bu gelişmeler devam ederken Bulut tiplerinde bir seçim söz konusuydu. Özel bulut (Private cloud) teknolojisi 2008 yıllarında başladı fakat henüz yeterince gelişemedi. Genel bulut (Public cloud) sistemleri çok cazip gelse de kullanıcı ya da şirketlere güvenlik açıklarının olabileceği endişesi ile fazla kullanılmıyordu. Bu yüzden private cloud teknolojisi public cloud teknolojisinden daha fazla kullanılmaktaydı. Bu yıllarda private cloud talebini gören bulut hizmet sağlayıcıları olan AWS, Microsoft, OpenStack gibi büyük şirketler private cloud alanına olan yatırımını ve çeşitliliğini geliştirdi.

2010-2011 yılları ve sonrası, sektörde ağırlığı olan iki büyük rakip firma olan Microsoft ve IBM firmaları da bulut bilişim alanında yerini almak için geliştirmelere devam etti. İlk olarak 2010 yılında Microsoft, Azure Bulut Sistemini tanıttı. Hemen

ardından 2011 yılında IBM, Bulut Sistemini tanıttı. Aslında IBM bir kültürel düşünme projesi olan Akıllı Gezegen(Smart Planet) projesini desteklemek için IBM Akıllı Bulut(IBM Smart Cloud) hizmetini duyurdu. Bu yıllarda Microsoft şirketi sosyal medya hesaplarında, televizyonda ve birçok farklı alanda bulut sistemlerinin reklamlarını yapmaya başladı. Bu da aslında her bulut servis sağlayıcısının kendi hizmetinin önceliklendirmesi kapsamında gelişiyordu. Hemen ardından sektörün kızıştığını ve hamle yapması gerektiğini düşünen diğer büyük bir şiket olan Apple, "ICloud" hizmetini duyurdu. Bu hizmetle kullanıcıların kendilerine ait yazı, resim, müzik, video ve sunu gibi farklı çeşitteki bilgileri belirli bir limit dahilinde depolayabileceğini tanıttı. Bu gelişmelerle birlikte 2008 de Private cloud ve Public cloud arasına sonradan katılacak olan Hibrit bulut (Hybrid cloud) kavramı duyuruldu. 2011 yıllarında tanıtılan bu teknolojide, private cloud ve public cloud aralarında yük taşıyabilecek ve istendiğinde public cloud'a istendiğinde private cloud'a yönlendirilebilecekti.

2014 yılına gelindiğinde, bulut bilişim giderek şekillenmeye başladı. En temel özelliklerini geliştirdi ve artık çoğu şirket ya da kullanıcı tarafından kullanılmaya başladı. Fakat herkesin endişe ettiği konu güvenlik meselesiydi. Bulut güvenliği'nin sağlanması, bulut hizmetini kullanan müşteriler için hızla büyüyen bir hizmet haline geldi. Bulut güvenliği son birkaç yılda önemli ölçüde ilerledi ve artık geleneksel BT güvenlik sistemleriyle karşılaştırılabilir koruma sağladığı düşünüldü. Tüm bunlar ile birlikte, güvenlik çoğu bulut kullanıcısının başta gelen endişesidir.

2016 yılına gelindiğinde, Oracle sektör içerisindeki yerini korumak ve daha önceden tanıttığı, bulut bilişimdeki üç temel öğeyi kapsayan; IaaS (Hizmet Olarak Altyapı), PaaS (Hizmet Olarak Platform) ve SaaS (Hizmet Olarak Yazılım) 'ı içeren "Oracle Bulut Altyapısı" adındaki sistemi tanıttı. Diğer bulutlara göre çeşitli avantajlar ve dezavantajları bulunduran bu hizmetler ile dünya üzerinde bulut sistemlerini önceliklendirme yarışı farklı bir boyut aldı. Bulut bilişim özellikçe yazılım geliştiriciler tarafından sıkça kullanılmaya başlandı. Önceden geliştiricilere çeşitli ortam sağlarken artık yönünü geliştiricileri bulut bilişim sistemleri üzerinde geliştirme yapmaya ve iç içe hizmetleri kullanılmasına doğru itti. Buradaki kar potansiyelini gören bulut hizmet sağlayıcıları çok sayıda hizmet seçeneğini sunarak geliştiricilerin bulut bilişim sistemleriyle entegre çalışan uygulamalar geliştirmelerine olanak sağladı.

2017 yılında ise, Uygulamaları sanallaştırmak için hafif (lightweight) bir teknoloji olarak konteynerlar, bulut bilişim sistemi üzerindeki uygulamaları yönetmek için oldukça başarılı oldu(Pahl, Brogi et al. 2017). Bu alanda da benzer şekilde üreticiler farklı teknolojiler hizmete sundu. Konteyner olarak en bilinen örneklerden biri 2014 yılında Google tarafından geliştirilen "Kubernetes" teknolojisidir. Açık kaynak olarak tanıtılan bu ürün ile uygulamaları yönetmek oldukça kolaylaştı ve piyasa tarafından kabul edildi. Docker ile birlikte ikisini de yanyana görmek mümkündür. Kubernetes en kısa özeti ile, bulut bilişim sistemindeki uygulama dağıtımlarını yapmak, bu uygulamaları ölçeklendirmek ve uygulama yönetimi otomatikleştirmek için tasarlanmış bir kapsayıcı düzenleme sistemidir. Daha sonradan farklı üreticiler tarafından çeşitli konteynar modelleri ortaya çıktı. Örneğin ; IBM tarafından "RedHat OpenShift" , Microsoft tarafından "Azure Container Service" gibi.

2019 ve sonrası için bulut bilişim, 2019 yılında tüm insan hayatını etkileyen COVID-19 virüsü ile birlikte pandemi ve karantina süreçleri neredeye tüm işlemleri evden yapmaya itti. Bununla birlikte internete olan talep, çeşitli yeni ürünlerin ve konseptlerin ortaya çıkmasına ve fiziksel kullanımın herhangi bir neden ile sekteye uğrayacağını gösterdi. Özellikle pandemi sürecinde e-ticaret alışverişlerinin ve yoğunluğunu hesaba katarak bu alanın hala büyüyecek bir alan olduğunu kolaylıkla söyleyebiliriz. Bununla birlikte her şeyin sanal olması daha önceki yıllarda da endişe konusu olan bulut bilişim sistemlerinin güvenliği, bu güvenliğin yönetilmesi konularını da tekrardan gündeme taşıdı.

4.2 Bulut Bilişim Özellikleri

Bulut bilişim için temel özellikler aşağıdaki başlıklarda verilmiştir.

4.2.1 Dış Kaynak Kullanımı

Kullanıcıların kendi ortamlarında bulunan fiziksel donanımları kullanmak yerine bu donanımın yönetilmesi ve kullandırılması sorumluluğu bulut hizmet sağlayıcılarına aittir.

4.2.2 Ölçeklenebilirlik

Bulut bilişim içerisinde çalışan uygulamalar normalde yüksek düzeyde ölçeklenebilir şekildedir. Bulut hizmet sağlayıcıdan kaynakları talep eden başvuru sahibi bu kaynakları manuel olarak ekleyebilir veya kaldırabilir veya uygulama otomatik olarak ölçeklenecek şekilde yapılandırılabilir. Örneğin bir sistemde uygulama yüksek kullanıcı talebiyle karşılaştığı zaman mevcut olan ek kaynaklara kadar ölçeklenebilir ve daha sonra kullanıcı talebi azaldığında başvuru ölçeğini azaltabilir şekilde mekanizması vardır (Swain 2015).

4.2.3 Erişilebilirlik

Dünyada internetin kesintisiz veya stabil olarak bulunduğu her konumdan sürekli olarak hesaplama, depolama, sunuculama, çözümleme işlemlerine bulut bilişim sayesinde erişilebilmektedir.

4.2.4 Sanallaştırma

Bulut bilişim sistemlerindeki donanım kaynakları çoğunlukla sanaldır. Bu yüzden verimliliği artırmak için bu sanal kaynaklar birden fazla kullanıcı tarafından paylaşılırlar. Tek bir fiziksel sunucu üzerinde birden fazla sanal sunucu kurulabileceği gibi sanal sunucular da tek bir sanal sunucu merkezine bağlanabilir.

4.2.5 Kullandığın Kadar Öde

Bulut bilişimin esneklik özelliğini ön plana çıkaran en önemli unsurlarından biri de esnek ödeme sistemidir. Buna göre bulut hizmet sağlayıcından alınan servis veya servisin türüne ve ne kadar süreyle kullanıldığına bağlı olarak aylık olarak faturalandırılması gerçekleştirilir. Eğer ücretsiz bir servis kullanılıyorsa kullanılan bulut hizmet sağlayıcıya bağlı olmak şartıyla herhangi bir ücret ödemesi gerçekleştirilmez.

4.2.6 Yardımcı Bilgi İşlem

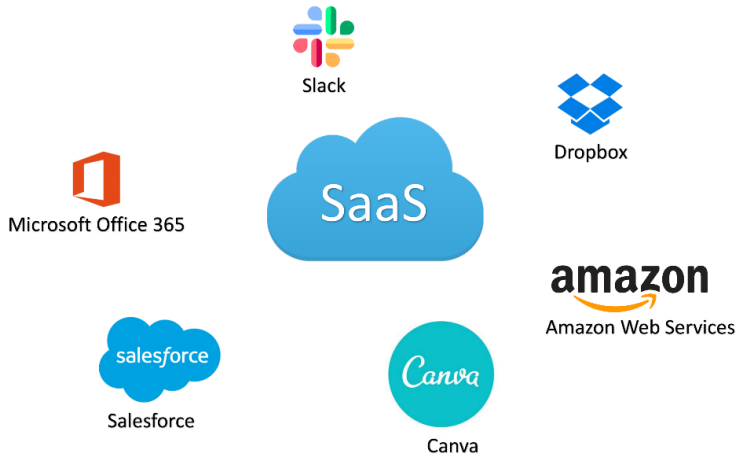
Yardımcı Bilgi İşlem, bulut bilişimin bir alt kümesidir ve kullanıcıların ihtiyaçlarına göre ölçeklendirmesini ve küçültmesini sağlar. Müşteriler, kullanıcılar veya işletmeler, veri depolama alanı, bilgi işlem yetenekleri, uygulama hizmetleri, sanal sunucular ve hatta CPU'lar, monitörler ve giriş cihazları gibi donanım kiralama gibi olanaklar elde eder (Borko Furht 2010).

4.3 Bulut Bilişim Servis Modelleri

Bulut bilişim hizmetleri temel olarak üç hizmet modeline ayrılır. Bunlar: SaaS (Hizmet Olarak Yazılım), IaaS (Hizmet olarak Altyapı), ve PaaS (Hizmet Olarak Platform). Bulut modellerinin kendi avantajları vardır ve avantajlar farklı türde olup çeşitli kurumların ihtiyaçlarını karşılayabilir.

4.3.1 Hizmet Olarak Yazılım(Software as a Service)

Hizmet olarak Yazılım veya teknik adıyla SaaS, Bulut tabanlı web uygulamalarına her yerden etkin ve hızlı erişim sağlayan bir modeldir. Bulut bilişim hizmeti sağlayıcıları tüm bilgi işlem yığınını kontrol edebilmekte ve bunlara bir web tarayıcısı kullanarak erişebilmektedir. Bu uygulamalar bulut üzerinde çalışır ve bunları kullandıkça öde ilkesiyle lisanslanabilir ve kullanılabilir bir yapıya sahiptir. Öte yandan, bazı hizmetler ve bazı hizmetler kota dahilinde ücretsizdir. AWS Storage, Alibaba Cloud vs. gibi ürünlerin sınırlı şekilde kullanıma açık birçok servisi bulunmaktadır (Bairagi and Bang 2015).

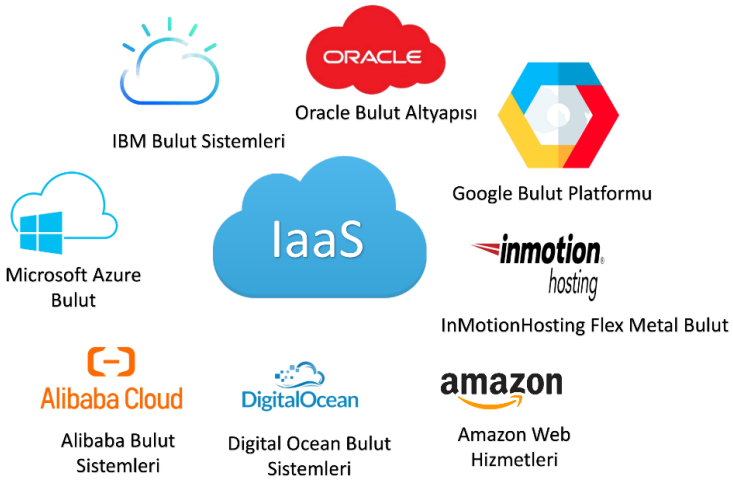


Şekil 2.7. SaaS Hizmetleri

SaaS, mevcut bilgi işlem altyapınız üzerinde herhangi bir kurulum veya indirme gerektirmez. *Plug and play(Tak-çalıştır)* ilkesi ile hareket etmektedir. Uygulama, satıcı tarafından bakımı yapılan ve desteklenen her bilgisayara yüklenebilmektedir. En çok bilinen SaaS örnekleri olarak Google G Suite, Microsoft Office 365, Dropbox vb. söylenebilir.

4.3.2 Altyapı Olarak Yazılım(Infrastructure as a Service)

Altyapı olarak Yazılım veya teknik adıyla IaaS, Hizmet Olarak Platform (PaaS) ve Hizmet Olarak Yazılım (SaaS) dahil olmak üzere hizmet katmanlarından biri olarak bulut ekosisteminde başladı. Müşteriler, sunucularına ve depolama alanına doğrudan erişmek için uygulama *dashboard(anaekranı)* ve çeşitli API'leri kullanır. IaaS ile daha fazla ölçeklenebilirlik imkanı vardır.

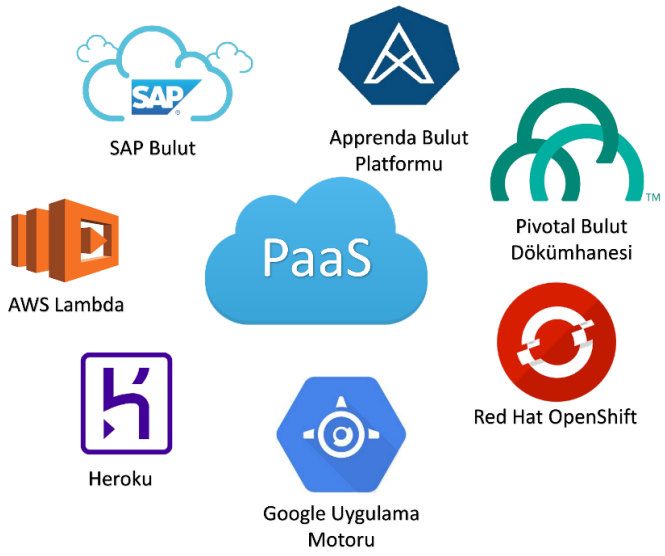


Şekil 2.8. IaaS Hizmetleri

IaaS kullanıcıları, geleneksel bir veri merkezinin aynı altyapı teknolojisi hizmetlerine çok fazla kaynağa yatırım yapmak zorunda kalmadan erişmek gibi bir hizmet olarak Altyapının birçok avantajından yararlanır. Sunucuların otomatik dağıtımına, işlem gücüne, depolamaya ve ağ oluşturmaya izin veren esnek bir bulut bilgi işlem modelidir. Özellikle altyapı desteği bulamayan ve farklı nedenler yüzünden planlamalarında aksamalar yaşayan kişisel kullanıcılar veya farklı şirketlerin daha fazla zaman ve ücret kaybetmesinin önüne geçmektedir.

4.3.3 Platform Olarak Yazılım(Platform as a Service)

PaaS, esas olarak kuruluşlar için farklı uygulamaları geliştirebilecek, test edilebilecek ve düzenlenebilecek bir bulut sistem tabanıdır. PaaS'yi uygulamak, kurumsal yazılım geliştirme sürecini basitleştirmektedir. PaaS tarafından sağlanan sanal çalışma zamanı ortamı, uygulamaları geliştirmek ve test etmek için uygun bir alan sağlar.



Şekil 2.9. PaaS Hizmetleri

Sunucular, depolama ve ağ oluşturma şeklinde sunulan kaynakların tamamı, şirket veya bulut servis sağlayıcı tarafından yönetilebilmektedir. Google App Engine ve AWS Elastic Beanstalk, PaaS'nin iki tipik örneğidir. PaaS de benzer şekilde ücretlendirilmiş lisans üzerine dayanmaktadır. Yapılacak işin boyutu ve gereksinimlerinize bağlı olarak size esnek fiyatlandırma seçenekleri sunmaktadır. Bu da yine bulut bilişimin kullandığın kadar öde ücret politikasıyla örtüşmektedir.

4.4 Bulut Bilişim Türleri

Bulut bilişim tip olarak 4 ana kategoride toplandı. Bunlar; Genel Bulut (Public Cloud), Özel Bulut (Private Cloud), Hibrit Bulut (Hybrid Cloud), Topluluk Bulut (Community Cloud) şeklindedir.

4.4.1 Genel Bulut (Public Cloud)

Bulut altyapısı, bulut hizmeti sağlayıcısına aittir. Bulut altyapısı bulut hizmet sağlayıcı bünyesinde bulunmaktadır. Kişisel kullanım için uygun bir çözüm olan, verilerin ortak tutulduğu, standart olarak kabul edilen internet üzerinden genel kullanıma açık bulut bilişim modelidir.

Bulut servis sağlayıcısı bulutun sahibidir ve bulut altyapısı genel amaçlar için genellikle ücretsiz erişimli veya kullanım başına ücretlendirilerek internet üzerinden herkese açıktır. Kişisel kullanımın yanı sıra küçük ve orta ölçekli işletmeler için herhangi bir altyapı yatırımına gerek kalmadan hizmet alınmasını sağlayan, düşük maliyetli çözümlerdir (Öz 2013, B. KeziaRani 2015).

4.4.2 Özel Bulut(Private Cloud)

Özel bir buluttaki bulut altyapısı, yalnızca bir kuruluş için çalıştırılır. Kuruluşun kendisi tarafından ya da 3.parti bir kişi / kurum tarafından yönetilebilir. Kuruluşlar özel bulutlara sahip olabilir veya kiralayabilir.

Bununla birlikte, altyapı ve güvenlik kontrolleri, hizmet sağlayıcılar ve kullanıcılar tarafından optimize edildi. Bir kuruluş tercih edebilir verilerini uzakta barındıramayacaklarına inandıklarında özel bir bulut kullanmak için, kaynaklarının otomasyonunu ve kullanımını iyileştirmek için bir bulutun yardımını ararlar.

4.4.3 Hibrit Bulut(Hybrid Cloud)

Hibrit bulut, çeşitli platformlar arasında düzenleme ile şirket içi altyapı, özel bulut hizmetleri ve Amazon Web Services (AWS) veya Microsoft Azure gibi bir genel buluttan oluşan karma bir bilgi işlem, depolama ve hizmetler ortamını ifade eder. Veri merkezinizde genel bulutlar, şirket içi bilgi işlem ve özel bulutların bir kombinasyonunu kullanmak, hibrit bir bulut altyapınız olduğu anlamına gelir.

Bununla birlikte Hibrit bulutun öne çıktığı ve kullanılmasının en büyük avantajı çevikliktir. Hızla uyum sağlama ve yön değiştirme ihtiyacı, dijital bir işletmenin temel ilkesidir. Bulut servis sağlayıcıdan hizmet alan kuruluş, rekabet avantajı için ihtiyaç duyduğu çevikliği elde etmek için genel bulutları, özel bulutları ve şirket içi kaynakları birleştirmek ve bunları daha efektif kullanmak isteyebilir.

4.4.4 Topluluk Bulut(Community Cloud)

Topluluk bulut bilişim, özel bulutun hibrit biçimli bir versiyonudur. Topluluk bulutu, genel bulut ve özel bulut arasında kalmış tüketici profiline hitap etmektedir. Özel buluta benzer fakat altyapı ve hesaplama için ayrılan kaynaklar özel olarak tutulur. Eğer iki şirket ortak olarak gizli bir şekilde kullanıyorsa kaynakları onlara özeldir ve tek bir organizasyon adı altında birleşerek bu hizmeti kullanırlar (Goyal 2014).

Başka bir tabirle Topluluk bulut bilişim, farklı türdeki bulut çözümlerinin sunduğu hizmetleri entegre ederek iş sektörlerinin belirli sorunlarını çözen dağıtık bir hizmet sunan altyapı sunar. Ortak ilgi alanlarına sahip, güvenlik ve uyumluluk konusunda herhangi bir sorun yaşamayan iki ticari kuruluş veya şirketlerin benzer hedeflerini tek çatı altında toplayarak kolay ve hızlı bir şekilde altyapı sunar.

Topluluk bulut bilişim de maliyet tüm kullanıcılar arasında eşit olarak paylaşıldığı için kullanıcılarının kendi işlerini ve maliyetini belirlemesini kolaylaştırır. Diğer yandan public cloud'a göre maliyeti fazladır. Sabit miktardaki bant genişliği ve veri depolama alanları tüm topluluk arasında paylaşılır (Goyal 2014).

5. ŞİFRELEME ALGORİTMALARININ PERFORMANS DEĞERLENDİRMELERİ VE UYGULAMALARI

5.1 Uygulamalar için Deneysel Ortam

Performans değerlendirme çalışması için yapılan analizde; DES, 3DES, AES, Blowfish ve RC şifreleme algoritmaları kullanılarak farklı dosya tiplerinde uygulanmıştır. DES, 3DES, AES, Blowfish ve RC algoritmaları Java 11 sürümünde implemente edilmiş ve 32 GB Ram, i7-8650U CPU 2.11 GHz işlemciye sahip, üzerinde Windows 10 20H2 versiyonu bulunan işletim sisteminde denenmiştir. Listelenen simetrik algoritmalar 2MB ile 200 MB arasındaki farklı kategorideki pdf uzantılı kitaplar üzerinde test edilmiştir. Ayrıca belirtilen algoritmaların farklı çözünürlükteki görseller üzerinde şifrelenmesi test edilip analiz tamamlanmıştır.

5.2 Uygulamaların Çalıştırılması

DES, 3DES, AES, Blowfish ve RC algoritmalarını şifrelemeler için uygulamak adına Java programlama dili kullanılmıştır. Java programlama dili şifreleme yöntemlerini uygulamak için hazır kütüphaneleri olan security ve crypto'dan yararlanılmıştır. Key oluşturmaları, IV vektör oluşturmaları için her biri tüm algoritmalar için ayrı ayrı uygulanmıştır.

Düz metin şifreleme işlemleri açık kaynak Z-books'ta bulunan kitap olan pdf uzantılı farklı dosyalar üzerinde, görsel şifrelemeler ise yine açık kaynak olarak Kaggle da bulunan çeşitli görseller üzerinde, DES, 3DES, AES, Blowfish ve RC algoritmalarına göre şifreleme ve şifre çözme işlemleri gerçekleştirilmiştir. Her iki şifrelemede de şifrelenmiş metin veya görsel, yine aynı konumda yer alan .pdf ya da .png uzantılı dosyaya yeni bir dosya şeklinde yazılmıştır. Oluşturulan şifreli metin ya da şifreli görsel, yeni bir kaynak olarak uygulamaya gösterilip yine o pdf ya da png uzantılı dosya üzerinde şifre çözme işlemleri hesaplanmıştır.

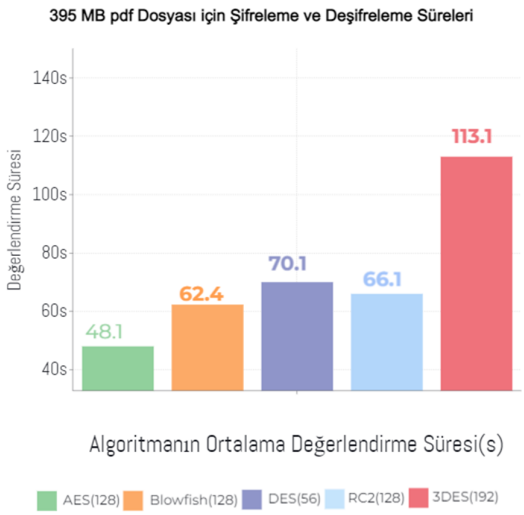
5.3 Yapılan Uygulamalara ait Bulgular

Pdf metinleri için uygulamalar sırasıyla; 395 MB, 215 MB, 98 MB, 50 MB, 25 MB, 12 MB, 3.5 MB, 2MB ve 575 KB gibi farklı boyuttaki metin dosyalarını kıyaslama metedolojisi ile, metin şifreleme ve şifre çözme becerileri AES, Blowfish, DES, RC2 ve 3DES algoritmaları için analiz edilmiştir. Analizde kullanılan metinler Z - Books adresinden açık kaynak kitapların pdf uzantılı halleridir. Uygulanan şifreleme algoritmaları Şifre Blok Zincirleme (Cipher Block Chain - CBC) gizlilik modu ile uygulanmıştır. Burada CBC modunun seçilmesinin nedeni, şifrelemenin sıralı olarak yapılması ve deşifreleme işleminin de paralel olarak yürütülmek istenmesinden kaynaklanmıştır. Diğer bir sebep ise, varsayılan modun tahmin edilebilir bir şifreleme mekanizmasına sahip olması ve ECB modunun tahmin edilemez rastgele bir başlangıç vektörü yaratmasıdır. Ayrıca, yapılan şifreleme analizlerinde CBC modunda PKCS5Padding ile şifreleme methodu ile ilerlenmiştir. Buna göre; isteğe bağlı olarak girilen metinin veri uzunlukları kabul edilmiştir. Fakat dolgu(padding) 8 baytın katlarına kadar doldurulmuştur. Normalde ise bu mod CBC modu için default No Padding şeklindedir.

Görseller için uygulamalar sırasıyla; 12 MB, 7 MB, 5.5 MB, 2.6 MB, 1MB ve 397 KB görselleri kıyaslama metedolojisi ile, görsel şifreleme ve şifre çözme becerileri AES, Blowfish, DES, RC2 ve 3 DES algoritmaları için analiz edilmiştir. Analizde kullanılan görseller Kaggle'dan alınan açık kaynak görsellerin png ve jpeg uzantılı halleridir. Java, kripto kütüphanesi görsel şifreleme için pdf metinde kullanılan CBC modunu desteklemediğinden, uygulanan şifreleme algoritmalarında pdf metinleri şifrelemeden farklı olarak, herhangi bir gizlilik modu kullanılmamıştır. Görseller için herhangi bir padding seçilmemiştir ve varsayılan kullanım şekli NonPadding olarak kullanılmıştır. Bunun nedeni ise, Java crypto kütüphanesinin CBC moduyla şifreleme yapıldığında bazı şifreleme algoritmalarında(RC2, DES) sorun yaşatmasıdır. Tüm algoritmaları aynı kulvarda değerlendirmek ve aynı yöntemi uygulamak için varsayılan modu ile uygulanmıştır.

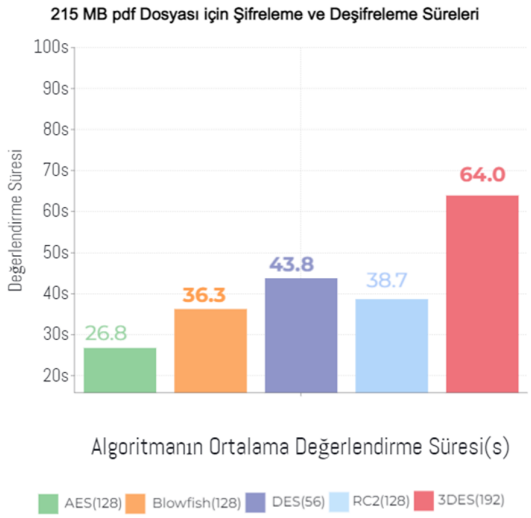
5.3.1 Metin şifreleme için yapılan analizler

Buradaki bölümde, analizde kullanılan şifreleme algoritmalarının, Algoritma Ortalama Değerlendirme Süreleri saniye cinsinden grafiksel olarak analiz edilmiştir.



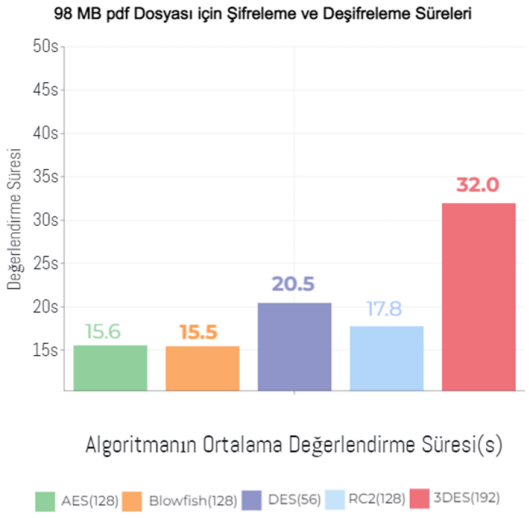
Şekil 3.1. 395 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.1'e bakıldığında 395 MB bir pdf metni için, 3DES algoritmasının en yavaş şifreleme algoritması olduğu görülmüştür. 3DES algoritması 113.1 s değerlendirme süresine sahiptir. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 395 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür. AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir.



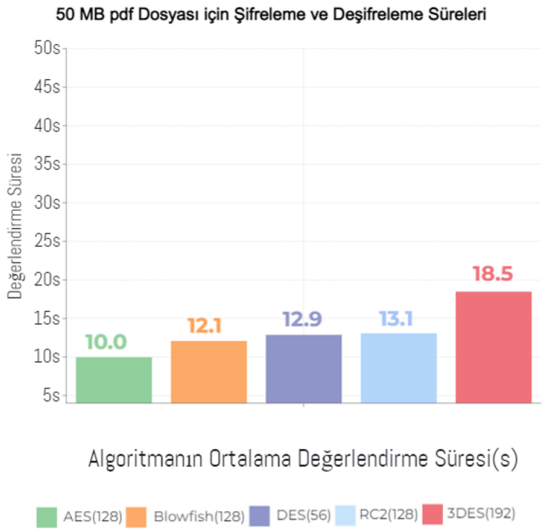
Şekil 3.2. 215 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.2'ye bakıldığında 215 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu görülmüştür. 3DES algoritması 64 s gibi bir değerlendirme süresine sahiptir. Yine aynı şekilde grafiğe bakıldığında AES algoritmasının da 395 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür. Burada AES algoritması 26.8 s gibi bir değerlendirme süresi göstermiştir. Şekil 3.1 ve Şekil 3.2'ye bakıldığında yüksek boyutlu şifreleme pdf metinlerinde 3DES algoritması en hızlı şifreleme algoritması olan AES algoritmasının neredeyse 2.5 katı kadar yüksek bir değerlendirme süresine sahiptir.



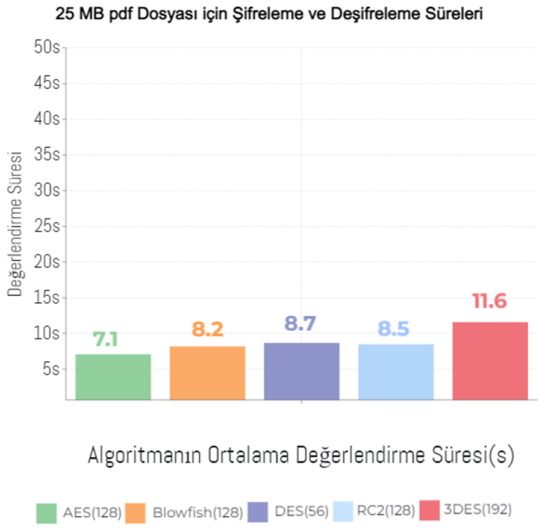
Şekil 3.3. 98 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.3'e bakıldığında 98 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu görülmüştür. Burada 3DES algoritması 32 s değerlendirme süresine sahip olduğu ortaya çıkmıştır. 98 MB pdf metnini şifrelemek için diğer grafiklerden farklı olarak, şekildeki grafiği de göz önünde bulundurarak Blowfish algoritmasının 98 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 15.5 s'ye eşittir. Dosya boyutları azaldıkça algoritmalar arasındaki değerlendirme süreleri farkları giderek azaldığı gözlemlenmiştir.



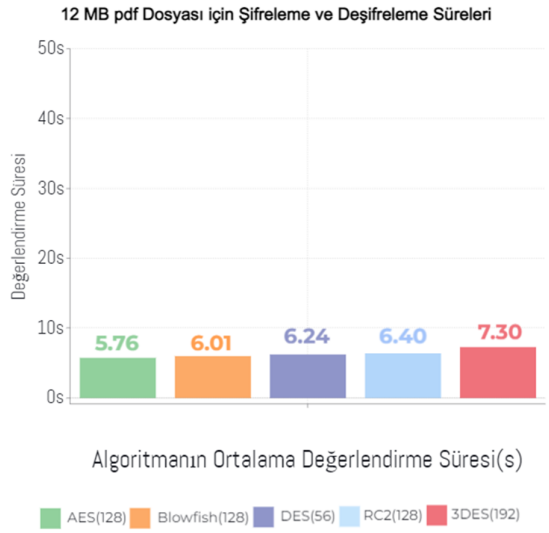
Şekil 3.4. 50 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.4'e bakıldığında 50 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu görülmüştür ve bu süre 18.5 s dir. 50 MB pdf metnini şifrelemek için diğer şekillerle (Şekil 3.1 ve Şekil 3.3) paralel olarak, AES algoritmasının 50 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 10 s dir. AES algoritmasını sırasıyla; Blowfsih, DES, RC2 ve 3DES algoritması takip etti. Diğer şekillerden farklı olarak burada RC2 algoritması DES algoritmasından daha etkili bir performans göstermiştir.



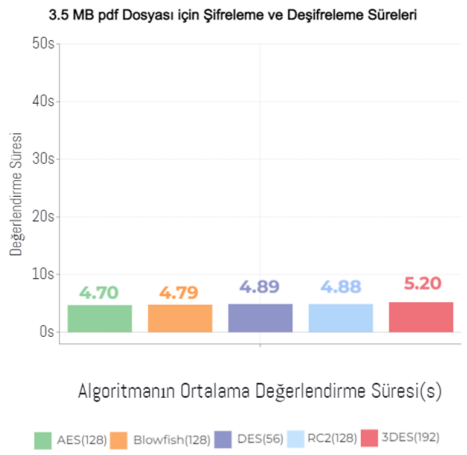
Şekil 3.5. 25 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.5'e bakıldığında ise 25 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu gözlemlenmiştir ve bu süre 11.6 s şeklindedir. 25 MB pdf metnini şifrelemek için diğer şekillerle (3.1 - 3.5) paralel olarak, AES algoritmasının 25 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 7.1 s dir. 50 ve 25 MB dosya boyutlarında ki grafiklerde dosya boyutları azaldıkça Şekil 3.1'de ki grafikten farklı olarak değerlendirme süreleri oldukça yakınsamıştır. Fakat dosya boyutu düşmesine karşın yine AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir.



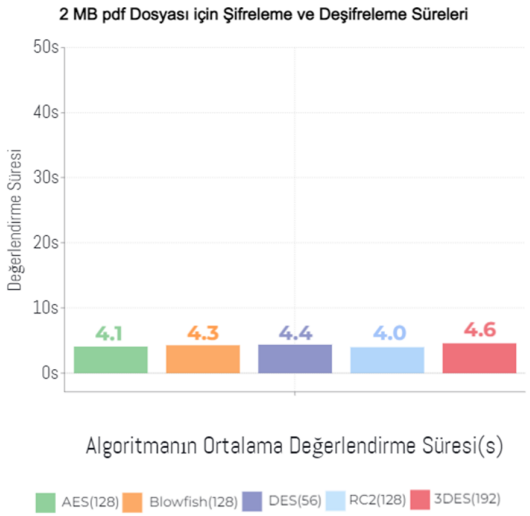
Şekil 3.6. 12 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.6'ya bakıldığında 12 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu tespit edilmiştir ve bu süre 7.3 s dir. 12 MB pdf metnini şifrelemek için diğer şekillerle (3.1 - 3.6) paralel olarak, yine benzer şekilde AES algoritmasının 12 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 5.7 s olarak gözlemlenmiştir. AES algoritmasını sırasıyla; Blowfish, DES, RC2 ve 3DES algoritması takip etti.Yine Şekil 3.4'te gösterilen 50 MB pdf metni şifreleme ile paralel olarak DES algoritması burada da RC2 algoritmasının önüne geçmiştir .Burada diğer grafiklerden farklı olarak ondalıklı kısımdan sonra iki basamak şeklinde gösterilmiştir. Çünkü algoritmalar birbirlerine o kadar çok yakınsadı ki artık virgülden sonraki kısım bizim için belirleyici unsur haline gelmiştir.



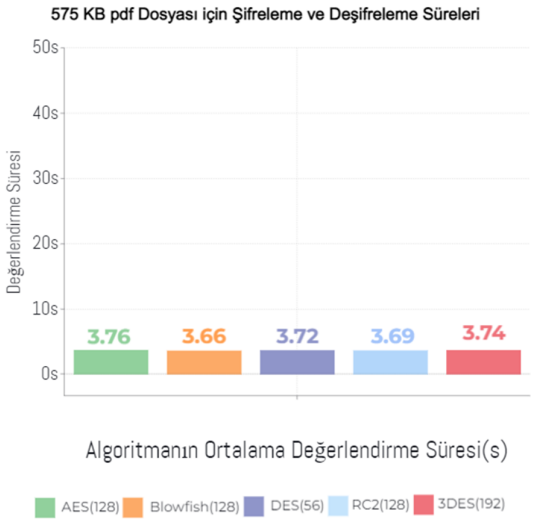
Şekil 3.7. 3.5 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.7'ye bakıldığında 3.5 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu ve bu sürenin 5.20 s olarak gözlemlenmiştir. 12 MB pdf metnini şifrelemek için diğer şekillerle (3.1 - 3.7) paralel olarak, yine benzer şekilde AES algoritmasının 3.5 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 4.70 s dir. AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir. Bu grafikte algoritmalar arası süre farkının oldukça az olduğu gözlemlenmiştir. Şekil 3.6 ile paralel olarak aynı neden ile burada da ondalıklı kısımdan sonraki iki basamak dikkate alınmıştır.



Şekil 3.8. 2 MB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.8'e bakıldığında 2 MB bir pdf metni için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu gözlemlenmiştir ve bu süre 4.6 s dir. 2 MB pdf metnini şifrelemek için diğer şekillerden farklı olarak, RC2 algoritmasının 2 MB pdf metnini şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 4s dir. RC2 algoritmasını sırasıyla; AES, Blowfish, DES ve 3DES algoritması takip etmiştir.

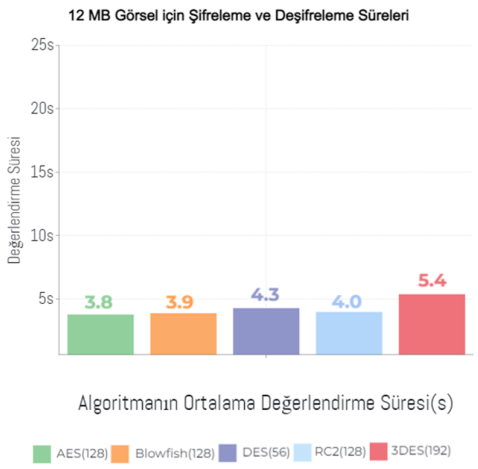


Şekil 3.9. 575 KB pdf metni için Şifreleme ve Deşifreleme süresi

Şekil 3.9'a bakıldığında 575 KB bir pdf metni için, diğer şekillerden farklı olduğu gözlemlenmiştir. Buna göre 575 KB metni en yavaş şifrelen şifreleme algoritması ise AES algoritmasıdır. Burada dosya boyutunun normal dosya boyutlarından daha az olması ve diğer şifreleme algoritmalarının da benzer performans eşiğini yaklaşması nedeniyle böyle bir sonuç görmek son derece doğaldır. Son durumda Blowfish algoritması 575 KB metini şifrelemek için en hızlı algoritmadır ve bu süre 3.66 s olarak ölçülmüştür. Blowfish algoritmasını sırasıyla; RC2, DES, 3DES ve AES algoritması takip etmiştir.

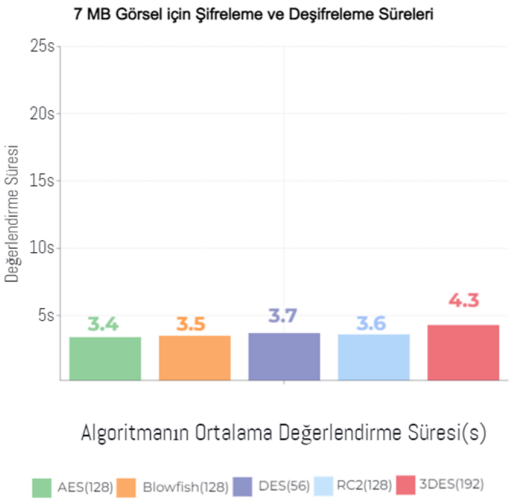
5.3.2 Görsel şifreleme için yapılan analizler

Bu bölümde ise, analizde kullanılan şifreleme algoritmalarının, Algoritma Ortalama Değerlendirme Süreleri görsel metinler üzerinde sınanıp, yine benzer şekilde saniye cinsinden grafiksel olarak analiz edilmiştir.



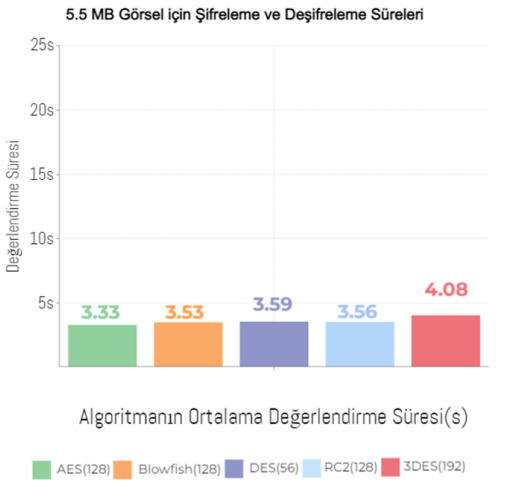
Şekil 4.1. 12 MB görsel için Şifreleme ve Deşifreleme süresi

Şekil 4.1'e bakıldığında 12 MB bir görsel için, 3DES algoritmasının en yavaş şifreleme algoritması olduğu gözlemlenmiştir ve bu süre 5.4 s dir. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 12 MB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 3.8 s olarak tespit edilmiştir. Pdf metni şifrelemeden farklı olarak görsel şifrelemede yüksek boyutlu şifrelemeden başlayarak algoritmalar arası değerlendirme süreleri, birbirlerine oldukça yakınsamıştır.



Şekil 4.2. 7 MB görsel için Şifreleme ve Deşifreleme süresi

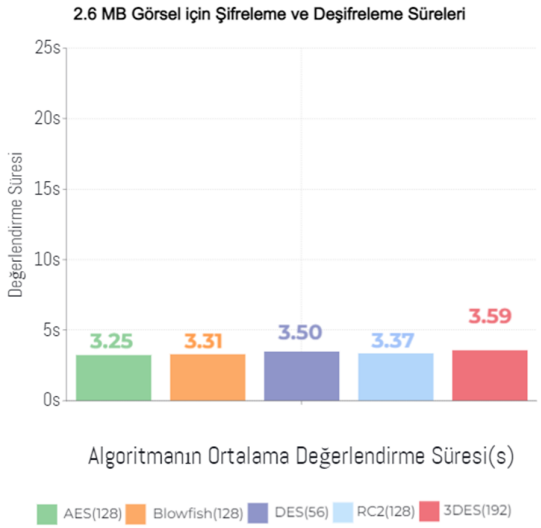
Şekil 4.2'ye bakıldığında 7 MB bir görsel için, 3DES algoritmasının en yavaş şifreleme algoritması olduğuve bu sürenin 4.3 s olarak hesaplanmıştır. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 7 MB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 3.4 s dir. AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir.



Şekil 4.3. 5.5 MB görsel için Şifreleme ve Deşifreleme süresi

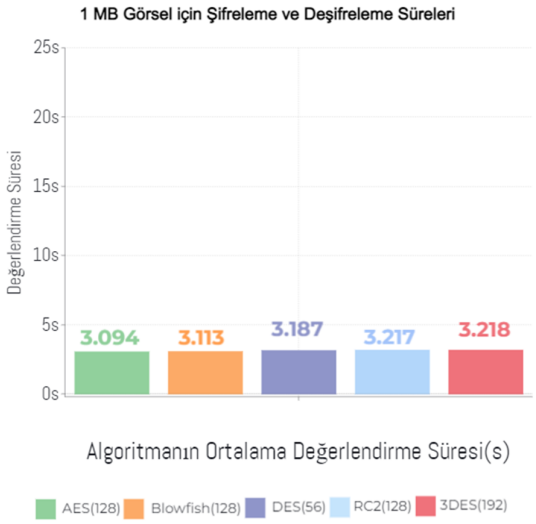
Şekil 4.3'e baktığımızda 5.5 MB bir görsel için, 3DES algoritmasının en yavaş şifreleme algoritması olduğu ortaya çıkmıştır ve bu süre 4.08 s olarak ölçülmüştür. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 5.5 MB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu süre 3.33

s gibi ufak bir değerdir. AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir.



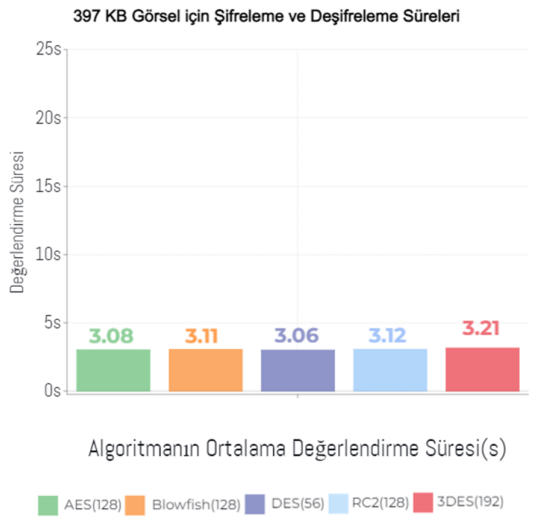
Şekil 4.4. 2.6 MB görsel için Şifreleme ve Deşifreleme süresi

Şekil 4.4'e bakıldığında 2.6 MB bir görsel için, yine 3DES algoritmasının en yavaş şifreleme algoritması olduğu görülmüştür ve bu süre 3.59 s olarak hesaplanmıştır. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 5.5 MB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve 3.25 s şeklindedir. Diğer şekiller ile benzer şekilde AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir.



Şekil 4.5. 1 MB görsel için Şifreleme ve Deşifreleme süresi

Şekil 4.5'e bakıldığında 1 MB bir görsel için, 3DES algoritmasının en yavaş şifreleme algoritması olduğu gözlemlenmiştir ve bu süre 3.218 s olarak tespit edilmiştir. Yine aynı şekilde grafiğe bakarak AES algoritmasının da 1 MB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve 3.094 s dir. Diğer şekiller ile benzer şekilde AES algoritmasını sırasıyla; Blowfish, RC2, DES ve 3DES algoritması takip etmiştir. Buradaki şekilde diğer şekillerden farklı olarak şu gözlemlenmiştir. 1 MB bir görsel için çoğu algoritmanın Algoritma Ortalama değerlendirme süreleri birbirine fazlasıyla yakınsamıştır. Burada diğer şekillerden farklı olarak ondalıklı kısımdan sonra 3 basamak dikkate alınmıştır. Algoritmaların 1 MB dosya boyutunda oldukça yakınsadıkları için böyle bir gereksinim ortaya çıkmıştır.



Şekil 4.6. 397 KB görsel için Şifreleme ve Deşifreleme süresi

Şekil 4.6'ya bakıldığında 397 KB bir görsel için, 3DES algoritmasının en yavaş şifreleme algoritması olduğu ortaya koyulmuştur ve bu süre 3.21 s şeklindedir. Diğer şekillerden farklı olarak, grafiğe bakarak DES algoritmasının da 397 KB bir görseli şifrelemek ve şifresini çözmek için en hızlı algoritma olduğunu söylemek mümkündür ve bu 3.06 s olarak hesaplanmıştır. Diğer şekillerden farklı olarak DES algoritmasını sırasıyla; AES, Blowfish, RC2 ve 3DES algoritması takip etmiştir. Buradaki yine Şekil 4.5 de ki ile paralel olarak görsel boyutu küçüldüğünden dolayı Algoritmaları, ortalama değerlendirme sürelerinin birbirine oldukça fazla yakınsadığı gözlemlenmiştir. Yüksek görsel boyutlarında ise bu farkın daha fazla olduğu açıktır.

6. ARAŞTIRMA SONUÇLARI VE TARTIŞMA

Algoritmalarının performanslarının açık bir şekilde karşılaştırılması ve analiz edilebilimesi için etkinlik (throughput) metriğinden yararlanılmıştır. Bir şifreleme algoritmasının etkinliği şu formül ile formulize edilmiştir:

Etkinlik = Toplam PDF metini boyutu (MB cinsinden) / Algoritma Ortalama Toplam Değerlendirme Süresi(ms)

Bir şifreleme algoritmasının etkinlik değeri arttıkça buna bağlı olarak, şifreleme ve şifre çözmesi süresine göre ilgili şifreleme algoritmasının güç tüketimi azalacaktır.

Çizelge 1.1. Çeşitli pdf Metinlerine ait farklı Şifreleme Algoritmalarının Değerlendirme Süreleri

pdf Dosyası Adı	Pdf dosya boyutu byte cinsinden	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
CompleteAtlasoftheWorld.pdf	395.693 MB	48105	62482	70100	66199	113100
SignsSymbolsAnIllustrated Guide.pdf	215.077 MB	26828	36387	43810	38756	64012
Heartstopper.pdf	98.378 MB	15694	15523	20502	17818	32047
The History Book.pdf	50.507 MB	10001	12109	12976	13198	18585
English Vocabulary in Use.pdf	25.296 MB	7189	8275	8702	8553	11643
Python Basics.pdf	11.925 MB	5766	6016	6241	6408	7309
Thinking,Fast and Slow.pdf	3.590 MB	4706	4799	4892	4885	5202
Tutunamayanlar.pdf	2.160 MB	4174	4394	4464	4007	4674
The Art of Creative Thinking.pdf	575 KB	3765	3664	3725	3638	3745

Buradaki metin şifreleme ve şifre çözme işlemleri çalışmasında AES, Blowfish, DES, RC2, 3DES algoritmaları Çizelge 1.1 de görüldüğü, farklı pdf dosyaları üzerinden analiz edilmiştir. Çizelge incelendiğinde 3DES algoritması genel olarak büyük dosyalardan başlayarak, neredeyse küçük dosya boyutlarına kadar daha uzun bir algoritma hesaplama süresi karmaşasına sahip olduğu açıkça görülmüştür. Buna karşın, AES algoritması ise yine büyük dosya boyutlarından başlayarak küçük dosya boyutlarına inildiğinde bile en hızlı algoritma olarak saptanmıştır.

Hesaplama da en büyük parametrelerden biri de toplam değerlendirme süresidir. Algoritmaların etkinliğini ölçerken toplam değerlendirme süresinden ortalama değerlendirme süresi bulunmaktadır.

Çizelge 1.2. Farklı Şifreleme Algoritmalarının Metin Şifrelemede Toplam Algoritma Hesaplama Süreleri

Algoritma Toplam Değerlendirme Süresi	Toplam Pdf dosya boyutu byte cinsinden	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
Toplam Değerlendirme Süresi	803.241 MB	126228	153649	175412	163462	260317

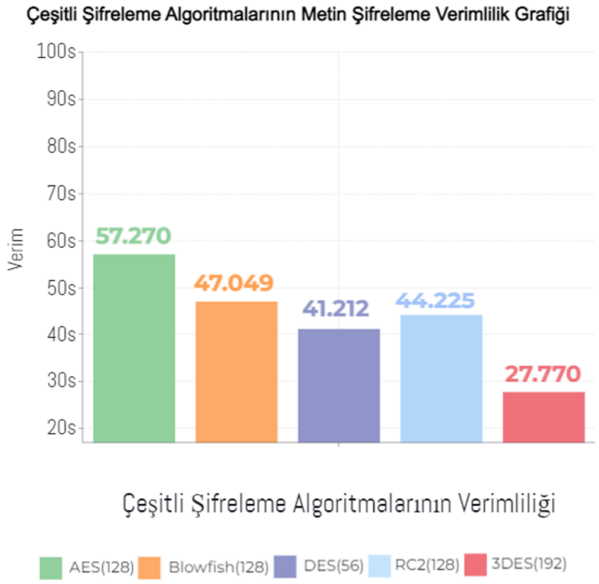
Toplam değerlendirme sürelerine bakıldığında, en az toplam değerlendirme süresine sahip şifreleme algoritması AES algoritmasıdır ve 126.228 ms olarak hesaplanmıştır. AES algoritmasını sırasıyla, Blowfish, RC2, DES ve 3DES algoritmaları takip etmiştir. 3DES algoritması ise en fazla toplam değerlendirme süresine ait şifreleme algoritmasıdır ve 260.317 ms olarak ölçülmüştür. Burada 3DES algoritmasının düz metini daha fazla işleme sokması yani DES'i 3 defa uygulaması nedeniyle 3DES algoritmasının metini en yavaş şifreleyen şifreleme algoritması olduğunu kanıtlamıştır.

Çizelge 1.3. Farklı Şifreleme Algoritmalarının Metin Şifrelemede Ortalama Algoritma Hesaplama Süreleri ve Verimlilikleri

Algoritma Ortalama Değerlendirme Süresi	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
Ortalama Değerlendirme Süresi	14025.33	17072.11	19490.22	18162.44	28924.11
Verimlilik(Toplam Pdf Boyutu / Ortalama Değerlendirme Süresi)	**57.270**	47.049	41.212	44.225	**27.770**

Çizelge 1.3'e bakıldığında şifreleme algoritmalarının verimlilikleri görülmektedir. Buna göre diğer çizelgelerde de olduğu gibi, AES algoritması verimlilik (throughput) değeri en fazla olan şifreleme algoritmasıdır ve 57.270 ms olarak ölçülmüştür. AES algoritmasını yine sırasıyla, Blowfish 47.049 ms, RC2 44.225 ms, DES 41.212 ms ve 3DES 27.770 ms ile algoritması takip etmiştir. Verimlilik değeri en düşük şifreleme algoritması 3DES algoritmasıdır. DES algoritması da 3DES algoritması gibi karmaşık

şifreleme mekanizmasına sahip olduğu için 3DES algoritmasını yavaş verimlilik oranında takip etmiştir. Blowfish ve RC2 arasında ise 2.824 ms lik bir fark bulunmaktadır. RC2, RC algoritmaları arasında temel bir algoritmadır. Bu yüzden çok fazla zafiyet bulunmaktadır. Bu yüzden hız parametresinin yüksek oluşu algoritmanın paralel olarak zayıflığını da beraber getirmiştir. Bu yüzden aradaki 2.824 ms lik farka rağmen, Blowfish algoritması şifreleme ve deşifreleme işlemlerindeki yalın metotları sayesinde RC2 algoritmasının önüne geçmiştir.



Şekil 4.7. Metin Şifrelemede Kullanılan Şifreleme Algoritmalarının Verimlilik Grafiği

Böylece bu çalışmada metin şifreleme ve şifre çözme işlemleri için AES, Blowfish, DES, RC2 ve 3DES şifreleme algoritmaları karşılaştırmalı olarak analiz edilmiştir. Şekil 4.7'deki grafiği incelediğimizde AES algoritmasının, uygulanan diğer şifreleme algoritmalarından daha yüksek verimliliğe sahip olduğu görülmüştür. Çalışmada 3DES algoritmasının en az verimliliğe sahip olan şifreleme algoritması olduğu ortaya koyulmuştur.

Çizelge 1.4. Çeşitli Görsellere ait Farklı Şifrele Algoritmalarının Değerlendirme Süreleri

Görsel Dosyası Adı	Görsel boyutu byte cinsinden	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
Water in the sea.jpg	12.374 MB	3868	3982	4318	4031	5410
Winter Stalactites.png	6.903 MB	3446	3563	3740	3682	4329
Wolf in the Forest.png	5.434 MB	3332	3533	3597	3569	4086
Gardens by the Bay.png	2.665 MB	3250	3319	3503	3371	3590
Simple House.png	1.001 MB	3094	3113	3187	3217	3218
Sea and Beach.png	397 KB	3085	3111	3066	3123	3214

Buradaki görsel şifreleme ve şifre çözme işlemleri çalışmasında AES, Blowfish, DES, RC2, 3DES algoritmaları yukarıdaki Çizelge 1.4 de görüldüğü, farklı png ve jpeg görselleri üzerinden kıyaslamalı olarak analiz edilmiştir. Yukarıdaki çizelge incelendiğinde 3DES algoritması genel olarak büyük dosyalardan başlayarak, neredeyse küçük dosya boyutlarına kadar daha uzun bir algoritma hesaplama süresi karmaşasına sahip olduğu açıkça görülmüştür. Fakat metin şifrelemeden farklı olarak görsel şifrelemede ki fark metin şifreleme kadar açık değildir. Diğer şifreleme algoritmaları birbirine oldukça yakın değerler göstermiştir. Buna karşın, AES algoritması ise yine büyük dosya boyutlarından başlayarak küçük dosya boyutlarına inildiğinde bile en hızlı algoritma olarak görülmüştür.

Çizelge 1.5. Farklı Şifreleme Algoritmalarının Görsel Şifrelemede Toplam Algoritma Hesaplama Süreleri

Algoritma Toplam Değerlendirme Süresi	Toplam Görsel boyutu byte cinsinden	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
Toplam Değerlendirme Süresi	28.774 MB	20075	20621	21411	20993	23487

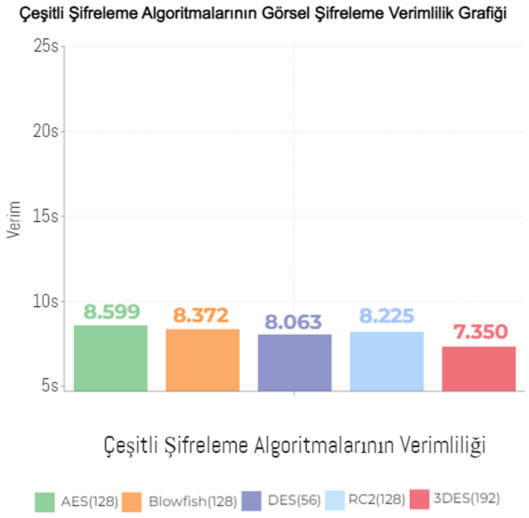
Toplam değerlendirme sürelerine bakıldığında, görsel şifreleme için en az toplam değerlendirme süresine sahip şifreleme algoritması AES algoritmasıdır ve bu süre yaklaşık 20075 ms olarak ölçülmüştür. AES algoritmasını sırasıyla, Blowfish, RC2, DES ve 3DES algoritmaları takip etmiştir. 3DES algoritması ise en fazla toplam değerlendirme süresine ait şifreleme algoritmasıdır ve 23.487 ms olarak hesaplanmıştır. Burada 3DES algoritmasının düz metini daha fazla işleme sokması yani DES'i 3 defa uygulaması 3DES algoritmasının metini en yavaş şifreleyen şifreleme algoritması

olduğunu kanıtlamıştır. Yinelemek gerekirse, 3DES ve diğer şifreleme algoritmaları arasındaki fark görsel şifrelemede oldukça aza indirgemektedir. AES algoritması ile toplam değerlendirme süresi farkı yalnızca 3.412 ms şeklindedir.

Çizelge 1.6. Farklı Şifreleme Algoritmalarının Görsel Şifrelemede Ortalama Algoritma Hesaplama Süreleri ve Verimlilikleri

Algoritma Ortalama Değerlendirme Süresi	AES(128)	BlowFish(128)	DES(56)	RC2(128)	3DES(192)
Ortalama Değerlendirme Süresi	3345.83	3436.83	3568.50	3498.33	3914.50
Verimlilik(Toplam Pdf Boyutu / Ortalama Değerlendirme Süresi)	**8.599**	8.372	8.063	8.225	**7.350**

Çizelge 1.6'ya bakıldığında şifreleme algoritmalarının verimliliklerini görülmektedir. Buna göre diğer çizelgelerde de olduğu gibi, AES algoritması verimlilik (throughput) değeri en fazla olan şifreleme algoritmasıdır ve 8.599 ms olarak ölçülmüştür. AES algoritmasını yine sırasıyla, Blowfish 8.372 ms, RC2 8.225 ms, DES 8.063 ms ve 3DES 7.350 ms algoritması takip etmiştir. Verimlilik değeri en düşük şifreleme algoritması 3DES algoritmasıdır. Fakat Blowfish, DES ve RC2 şifreleme algoritmaları arasındaki fark görsel şifrelemede oldukça yakınsamıştır. Blowfish ile, sırasıyla DES ve RC2 arasında 0.336 ms ve 0.147 ms verimlilik farkı bulunmaktadır. Benzer şekilde DES ve RC2 algoritmaları arasındaki fark sadece 0.162 ms verimlilik farkından oluşmaktadır. Görsel şifrelemede değerler birbirine her ne kadar yakın olsa da çalışma AES algoritmasının diğer şifreleme algoritmalarından üstün olduğunu ortaya koymuştur.



Şekil 4.8. Görsel Şifrelemede Kullanılan Şifreleme Algoritmalarının Verimlilik Grafiği

Böylece bu çalışmada görsel şifreleme ve şifre çözme işlemleri için AES, Blowfish, DES, RC2 ve 3DES şifreleme algoritmaları karşılaştırmalı olarak analiz edilmiştir. Şekil 4.8'deki grafiği incelediğimizde AES algoritmasının, uygulanan diğer şifreleme algoritmalarından daha yüksek verimliliğe sahip olduğu görülmüştür. Çalışmada 3DES algoritmasının en az verimliliğe sahip olan şifreleme algoritması olduğu ortaya koyulmuştur.

7. SONUÇLAR VE ÖNERİLER

Bu tez çalışmasında farklı simetrik şifreleme algoritmaları, çeşitli dosya tiplerinde uygulanarak şifrelenmiş ve şifre çözme işlemleri gerçekleştirilmiştir. Bu işlemler birbirleri ile kıyaslanarak hangi algoritmanın daha yüksek ya da daha az performans gösterdiği ortaya koyulmuştur. Buna göre hangi algoritmanın bulut bilişim sistemlerinde kullanılabileceği yönünde bir seçim imkanı yaratılmıştır. Performans analizi bulguları incelendiğinde, AES algoritmasının yüksek metin boyutlarında etkin ve hızlı bir algoritma olduğu gözlemlenmiştir. AES şifreleme algoritması bulut bilişim sistemlerinde, yine mesajlaşma uygulamalarında kullanılabilecek etkin bir şifreleme algoritması olmuştur.

3DES algoritmasının ise yüksek boyutlu metin dosyalarında algoritma değerlendirme süresi en yavaş algoritma olması sebebiyle hızın metrik olarak önemli olmadığı alanlarda kullanılabilir bir algoritmadır. Fakat eski bir şifreleme algoritma olması ve kaba kuvvet saldırıları ile kırılma özelliğinin hala bulunması nedeniyle çok fazla tercih edilmemesi gereken bir şifreleme algoritmasıdır.

Blowfish algoritmasının özellikle düşük boyutlu verilerde hızlı bir algoritma olması ve güvenlik konusunda ön plana çıkması günümüzde gömülü sistemler veya bulut sistemler gibi giderek büyüyen bu alanlarda kullanılabilecek hızlı ve etkili bir algoritma olabileceğini göstermiştir. AES algoritmasının ardından verimlilik oranı en yüksek olan Blowfish algoritması hem metin şifrelemelerinde hem de görsel şifrelemede yüksek verimlilik ortaya koymuştur.

DES ve RC2 algoritması ise, DES algoritması metin şifrelemede RC2 algoritmasından daha az verimlilik göstermiştir. Görsel şifrelemede ise DES algoritması ile yakın bir verimliliği olduğunu kanıtlamıştır.

AES algoritması ilerideki çalışmalarda, mesajlaşma sistemlerinde entegre edilip iki kişi arasındaki metin arka plandaki şifrelemeleri, hangi yöntem ile ne hızda yapacağı konusu araştırma konusu olarak belirlenmiştir. 3DES algoritması, görsel şifreleme alanında ise verimlilikler arasında çok fazla fark gözlemlenmediği için görsel şifreleme alanında da kullanılabilir bir algoritma olduğu görülmüştür. Blowfish algoritması, farklı

dosya tiplerinde ya da daha da büyük dosya şifrelemelerde denenip verimliliği gözlenip, diğer çalışmalarla kıyaslanabilecek bir algoritmadır. RC2 ve DES algoritmaları ise, iki algoritmanın temel şifreleme algoritmaları olmaları ve yine zamanla kaba kuvvet saldırıları nedeniyle güvenlik açığı oluşturduğundan dolayı günümüzde daha az tercih edilmesi gereken algoritma türlerindendir.

8. KAYNAKLAR

Beskirli, A. D. Ö., Beskirli, M. (2019). "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme." EJOSAT.

Yücelen, A., C. Çoşkun (2017). "Kriptolojide eliptik eğri algoritmasının uygulanması." Dicle Üniversitesi Mühendislik Dergisi.

Afolabi, A. O. and E. Adagunodo (2012). "Implementation of an improved data encryption algorithm in a web based learning system." International Journal of research and reviews in Computer Science **3**(1): 1407.

Kakkar, A., M. L. S. a. P. K. B. (2012). "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network." International Journal of Engineering and Technology **2**.

Akif, O. Z. (2012). "Image Encryption Technique Using Lagrange Interpolation." Ibn Al-Haitham Journal for Pure and Applied Science **25**.

Alabaichi, A., et al. (2013). Security analysis of blowfish algorithm. 2013 Second International Conference on Informatics & Applications (ICIA), IEEE.

Amazon (2018). "What is AWS ?". from https://aws.amazon.com/tr/what-is-aws/.

Aslan, K. (2019). PERFORMANCE EVALUATION OF IOT DATA SECURITY ON CLOUD COMPUTING. Department of Computer Engineering. Ankara, ANKARA YILDIRIM BEYAZIT UNIVERSITY. **MS**.

Atikah, N., et al. (2019). AES-RC4 Encryption Technique to Improve File Security. 2019 Fourth International Conference on Informatics and Computing (ICIC), IEEE.

Gunes, B., G. K., P. Bolat (2021). "Cyber security risk assessment for seaports: A case study of a container port." Computer & Security.

KeziaRani, B., A. VinayaBabu (2015). "Cloud Computing and Inter-Clouds – Types, Topologies and Research Issues." Procedia Computer Science **9**.

Bairagi, S. I. and A. O. Bang (2015). Cloud computing: History, architecture, security issues. National Conference "CONVERGENCE.

Bhardwaj, A., et al. (2016). "Security algorithms for cloud computing." Procedia Computer Science **85**: 535-542.

Kutlu, B., Z. S., Ozge Cetinel, Duygu Ece (2016). "CORPORATE REQUIREMENTS FOR CLOUD SERVICES: ADOPTERS AND NON-ADOPTERS." 3rd International Management Information Systems Conference.

Furht, B. R., Armando Escalante (2010). Handbook of Cloud Computing. Springer, Springer.

Canniere, C. D. (2007). ANALYSIS AND DESIGN OF SYMMETRIC ENCRYPTION ALGORITHMS. FACULTEIT TOEGEPASTE WETENSCHAPPEN DEPARTEMENT ELEKTROTECHNIEK, KATHOLIEKE UNIVERSITEIT LEUVEN. **MS**.

Chmielowiec, A. (2010). "Fixed points of the RSA encryption algorithm." Theoretical Computer Science **411**.

D'Agapeyefff, A. (2013). CODES AND CIPHERS : A HISTORY OF CRYPTOGRAPHY. British Library Cataloguing-in-Publication Data.

Boneh, D., V. S. (August 17, 2015). Principles of Modern Cryptography. Stannford University.

KR Shukla, D., V. K. R. D., Munesh C Trivedi (2020). "Encryption algorithm in cloud computing." Materials Today: Proceedings **1869-1875**.

Abdul, D. Elminaam, H. M. A. K. a. M. M. H. (2008). "Performance Evaluation of Symmetric Encryption Algorithms." International Journal of Computer Science and Network Security **8**.

Tapscott, D., A. T. (2016). "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World." Penguin.

Dooley, J. F. (2018). "History of Cryptography and Cryptanalysis." Springer.

Pandya, D., R. K., Narayan, Sneha Thakkar, Tanvi Madhekar, B S Thakare (2015). "Brief History of Encryption." International Journal of Computer Applications **131-9**.

El-etriby, S., et al. (2012). Modern encryption techniques for cloud computing. ICCIT.

Biham, E., Y. C. (2008). "Efficient Reconstruction of RC4 Keys fromInternal States." Computer Science Department Technion.

Ellis, S. R. (2013). Enigma Machine. Computer and Information Security Handbook (Third Edition), Science Direct.

Thabita, F., S., Sudhir Jagtap Dr (2021). "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing." Global Transitions Proceedings **2**.

Gonsai, D. A. M. and L. M. Raval (2014). "Evaluation of Common Encryption Algorithm and Scope of Advanced Algorithm for Simulated Wireless Network." Int. Journal of Computer Trends and Technology **11**(1): 7-12.

Goyal, S. (2014). "Public vs private vs hybrid vs community-cloud computing: a critical review." International Journal of Computer Network and Information Security **6**(3): 20-29.

Grance, M. (2011). "The NIST Definition of Cloud Computing." National Institute of Standards and Technology : Information Technology Laboratory.

Günden, Ü. (2010). ŞİFRELEME ALGORİTMALARININ PERFORMANS ANALİZİ. Computer Engineering. SAKARYA UNIVERSITY
Institute Of Science, SAKARYA UNIVERSITY **MS**.

Joseph, D. P., et al. (2015). "Cognitive analytics and comparison of symmetric and asymmetric cryptography algorithms." Int. J. Adv. Res. Comput. Sci **6**(3): 51-56.

Kalpana, P. and S. Singaraju (2012). "Data security in cloud computing using RSA algorithm." International Journal of research in computer and communication technology, IJRCCT, ISSN: 2278-5841.

Kotas, W. A. (2000). "A Brief Hist A Brief History of Cr y of Cryptography." TRACE : Tennessee Research and Creative Exchange.

Kshetri, N., and Voas, J. (2021). "Major Computing Technologies of the Past 75 Years." IEEE Computer Society.

Liu, F. Z. C. L. C. F. (2014). A cloud computing security solution based on fully homomorphic encryption. 16th International Conference on Advanced Communication Technology, IEEE.

Lošonczi, P. (2018). "Importance of Dealing with Cybersecurity Challenges and Cybercrime in the Senior Population." SECURITY DIMENSIONS.

Avram, M.G. (2014). "Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective." **12**.

Mandal, P. C. (2012). "Superiority of blowfish Algorithm." International Journal of Advanced Research in Computer Science and Software Engineering **2**.

Suresh, M., N. M. (2016). Hardware implementation of blowfish algorithm for the secure data transmission in Internet of Things Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology(RAEREST 2016), Procedia Technology **248-255**.

Microsoft (2018). "What is the cloud?". from https://azure.microsoft.com/en-us/overview/what-is-the-cloud/.

Milanov, E. (2009). "The RSA algorithm." RSA laboratories: 1-11.

Mirashe, S. P. and N. V. Kalyankar (2010). "Cloud computing." arXiv preprint arXiv:1003.4074.

Öz, A. (2013). BULUT BİLİŞİM VERİ GÜVENLİĞİ. GAZİ ÜNİVERSİTESİ BİLİŞİM ENSTİTÜSÜ, GAZI UNIVERSITY. **MS**.

Özdemir, Ö. (2020). "DSA Şifreleme." 2020, from https://www.sibervatan.org/makale/dsa-sifreleme/35.

Pahl, C., et al. (2017). "Cloud container technologies: a state-of-the-art review." IEEE Transactions on Cloud Computing **7**(3): 677-692.

Patil, P., et al. (2016). "A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish." Procedia Computer Science **78**: 617-624.

Patel, P., R. P., Nimisha Patel (2015). "Integrated ECC and Blowfish for Smartphone Security." Procedia Computer Science **210-216**.

Rivest, R. (1998). A Description of the RC2 (r) Encryption Algorithm.

Rogaway, P. (2011). "Evaluation of some blockcipher modes of operation." Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan.

Halder, S., T. N. (2022). "Enabling secure time-series data sharing via homomorphic encryption in cloud-assisted IIoT." Future Generation Computer Systems

Sani, N. A. A. K., Hailiza (2017). "RSA cryptography and multi prime RSA cryptography." Mathematical Sciences Exploration for the Universal Preservation.

Selleri, S. (2020). "The roots of modern cryptography: Leon Battista Alberti's" De Cifris"." URSI Radio Science Bulletin **2020**(375): 55-63.

Kruti, S. R. and B. Gambhava (2012). "New approach of data encryption standard algorithm." International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307.

Thabah, S., M. S., Rekib Uddin Ahmed, Prabir Saha (2019). Fast and Area Efficient Implementation of RSA Algorithm. ICRTAC 2019, India.

Singh, P. and K. Singh (2013). "Image encryption and decryption using blowfish algorithm in MATLAB." International Journal of Scientific & Engineering Research **4**(7): 150-154.

Avireddy S., V. P. N. G. R. S. K. P. T. S. G. (2012). Random4: An Application Specific Randomized Encryption Algorithm to Prevent SQL Injection. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE.

Slabeva, K. and T. Wozniak (2010). Cloud basics–an introduction to cloud computing. Grid and cloud computing, Springer**:** 47-61.

Sunyaev, A. (2020). Cloud computing. Internet computing, Springer**:** 195-236.

Surbiryala, J. and C. Rong (2019). Cloud computing: History and overview. 2019 IEEE Cloud Summit, IEEE.

Swain, D. P. B. P. S. S. S. M. S. (2015). "Cloud Computing Features, Issues, and Challenges: A Big Picture." IEEE.

Bairagi, S., A. O. B. (2015). "Cloud Computing: History, Architecture, Security Issues." CONVERGENCE 2015.

Yerlikaya, T., E. B., N.Buluş (2006). "ASİMETRİK ŞİFRELEME ALGORİTMALARINDA ANAHTAR DEĞİŞİM SİSTEMLERİ." 13. Güvenlik Sistemleri.

Tezcan, C. (2022). "Key lengths revisited: GPU-based brute force cryptanalysis of DES, 3DES, and PRESENT." Journal of Systems Architecture **124**.

Tony, M.D. (2009). "A Brief History of Cryptography." Inquiries Journal **1**.

Somani, M. K. L., Manish Mundra (2010). "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing." IEEE.

Verma, H. K. and R. K. Singh (2012). "Performance analysis of RC6, Twofish and Rijndael block cipher algorithms." International Journal of Computer Applications **42**(16): 1-7.

Wikipedia (2014). "Diffie-Hellman anahtar değişimi." from https://tr.wikipedia.org/wiki/Diffie-Hellman_anahtar_de%C4%9Fi%C5%9Fimi.

Wikipedia (2015). "Üçlü DES." from https://tr.wikipedia.org/wiki/%C3%9C%C3%A7l%C3%BC_DES.

Zohu, Y. (2021). "Research on Application of Packet Encryption Technology in Information Security Algorithm." Journal of Physics: Conference Series.

Yuan Y., Y. Y., Liji Wu, Xiangmin Zhang (2018). A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation. 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC).

Zhang, L. Z.-a. T.-k. (2012). "Identification of NAND flash ECC algorithms in mobile devices." Digital Investigation **9**.