T.C.
İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

NFC TEKNOLOJİSİ TABANLI SANAL PARA ALIŞVERİŞ MİMARİSİ TASARIMI ve GÜVENLİĞİ

Mehmet Fatih ÖZTÜRK

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

DANIŞMAN
Prof. Dr. Ahmet SERTBAŞ

Temmuz, 2016

İSTANBUL

Uygundur (05.08.2016)

Bu çalışma 01.07.2016 tarihinde aşağıdaki jüri tarafından Bilgisayar Bilimleri Anabilim Dalı Bilgisayar Mühendisliği Programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi:

Prof. Dr.Ahmet SERTBAŞ(Danışman)
İstanbul Üniversitesi
Mühendislik Fakültesi

Doç. Dr.Ataseven KURT
İstanbul Üniversitesi
Mühendislik Fakültesi

Yrd. Doç. Dr.Akhan AKBULUT
İstanbul Kültür Üniversitesi
Mühendislik Fakültesi

Yrd. Doç. Dr.Mustafa DAĞTEKİN
İstanbul Üniversitesi
Mühendislik Fakültesi

Yrd. Doç. Dr.Tolga ENSARİ
İstanbul Üniversitesi
Mühendislik Fakültesi

20.04.2016 tarihli resmi gazetede yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

ÖNSÖZ

Tezim süresince benden yardımlarını esirgemeyen danışman hocam Sayın Prof.Dr. Ahmet SERTBAŞ'a, Yrd.Doç.Dr. Muhammed Ali AYDIN'a, çalışmalarım süresince benden anlayışlarını esirgemeyen eşime ve kızım Asmin'e teşekkürü bir borç bilirim.

Temmuz, 2016 Mehmet Fatih ÖZTÜRK

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

TABLO LİSTESİ

Sayfa No

SİMGE VE KISALTMA LİSTESİ

Simgeler **Açıklama**

Mhz **:** Megahertz
Kbit **:** Kilobit
Khz **:** Kilohertz
Ghz **:** Gigahertz

Kısaltmalar **Açıklama**

NFC **:** Near Field Communication
NDEF **:** NFC Data Exchange Format
SYY **:** Site Yönetim Yazılımı
DYY **:** Daire Yönetim Yazılımı
GTS **:** Gecikme Tazminat Servisi
BGS **:** Bildirim Gönderim Servisi
VYS **:** Veritabanı Yedekleme Servisi
NKMY **:** NFC Kullanıcı Mobil Yazılımı
NOMY **:** NFC Ödeme Noktası Mobil Yazılımı
NWS **:** NFC Web Servisi
RFID **:** Radio-frequency identification
AES **:** Advanced Encryption Standard
SSL **:** Secure Sockets Layer
LF **:** Low Frequency
HF **:** High Frequency
UHF **:** Ultra High Frequency
ASP.NET **:** Active Server Page
SQL **:** Struct Query Language
HTML **:** Hyper Text Markup Language
CSS **:** Cascading Style Sheets
MD5 **:** Message Digest 5
IFF **:** Identify Friend or Foe

ÖZET

YÜKSEK LİSANS TEZİ

NFC TEKNOLOJİSİ TABANLI SANAL PARA ALIŞVERİŞ MİMARİSİ TASARIMI ve GÜVENLİĞİ

Mehmet Fatih ÖZTÜRK

İstanbul Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Prof.Dr. Ahmet SERTBAŞ

Sanal alışveriş, günlük ihtiyaçlarımızın büyük bir kısmını gidermek için son zamanlarda çok sık başvurduğumuz bir etkileşim türüdür. Sanal alışverişin yaygınlaşması ile ödeme yöntemlerinin de çeşitlenmesi ve gelişmesi kaçınılmaz olmuştur. Günümüzde alışveriş ve ödeme yöntemleri teknolojinin de ilerlemesi ile çok hızlı bir şekilde farklılaşarak gelişmiştir. Birçok farklı teknoloji ile gerçekleştirilen ödeme yöntemlerine son zamanlarda bir de NFC(Yakın Alan Haberleşmesi) tabanlı ödeme yöntemleri eklenmiştir. Bu gelişmeler ile akıllı telefonlar üzerinde sanal cüzdan mantığında uygulamalar geliştirilerek, kullanıcılar birçok fiziksel kartı taşımaktan kurtarılmıştır. Bu çalışmada; NFC tabanlı sanal alışveriş yöntemlerine, farklı saldırı türlerine karşı alınmış önlemler ile güvenli bir örnek teşkil etmesi amaçlanmıştır. Geliştirmiş olduğumuz mimari; önceki çalışmalar incelenerek oluşturulan bir hibrit model ve sonraki çalışmalara da geliştirilebilir bir altyapı sunmaktadır. Güvenli sanal alışveriş sistemimiz; apartman site yönetimlerinde kullanılmak üzere, daire sakinlerinin; NFC tabanlı çalışan mobil uygulamaları sayesinde kolayca aidat ödemelerini sağlayabilecekleri gerçek zamanlı ve güvenli bir model geliştirilerek sonuçları incelenmiştir. Performans ve güvenlik ölçümleri bu model üzerinde hesaplanmıştır ve farklı çalışmalarla mukayese edilmek suretiyle kazanımlar ortaya koyulmuştur.

Temmuz 2016, 116 sayfa.

Anahtar kelimeler: NFC, NDEF, SSL, AES, AES 128, Yakın Alan Haberleşmesi

SUMMARY

M.Sc. THESIS

NFC TECHNOLOGY BASED VIRTUAL CASH SHOPPING ARCHITECTURE DESIGN AND SECURITY

Mehmet Fatih ÖZTÜRK

İstanbul University

Institute of Graduate Studies in Science and Engineering

Department of Computer Engineering

Supervisor : Prof. Dr. Ahmet SERTBAŞ

Shopping is a sort of interaction which we recently appeal to in order to satisfy a great majority of our needs.With the proliferation of shopping, the diversification of patterns of payment has been inevitable. In our day,patterns of shopping and payment has been developed in a great variety with the advancement of technology. Recently, NFC (Near Field Communication) was included in the list of new patterns of payment which are implemented by many different technologies. With the help of these developments, applications based on the notion of "virtual purse" was developed thereby making customers free from carrying many physical cards. The architecture which we developed as an example of NFC-based shopping methodthat is secure against different types of attacks presents a hybrid model which was developed by examining previous studies and an infrastructure which can be improved by further studies. Our safe shopping system was tested on a real-time and safe model which is used in a site management system in order for occupants to easily pay dues in virtue of their NFC-based mobile applications. Besides, a great deal of beneficial data was brought out through performance and security measurements on this model.

July 2016,116 pages.

Keywords: NFC, NDEF, SSL, AES, AES 128, Near Field Communication

1. GİRİŞ

İnsanlık tarihi kadar eski olan alışveriş yöntemleri, değişen yaşam koşulları ve gelişen teknolojiyle beraber zaman içinde farklılık göstermiştir. Takas ile başlayan "alışveriş" eylemi paranın icat edilmesi ile birlikte çok daha pratik ve canlı bir hale gelmiştir. Paranın alışveriş hayatına girmesi ile insanların erişmek istedikleri mal ve hizmetlere ulaşması daha da kolaylaşmıştır. Özellikle "Takas" yönteminin kendine özgü bazı problemleri paranın icadıyla ortadan kalkmıştır.

Paranın ticaret hayatına girmesiyle birlikte, insanların farklı ihtiyaçlarından ortaya çıkan çek ve senet gibi paranın yerine geçebilen birçok kıymetli evrak kullanılmaya başlanmıştır. Bu ve benzeri gelişmeler aslında "alışveriş" kavramının özünde bulunan karşılıklı "alacak" ve "borç" edimlerinin ifasının ne şekilde gerçekleştirileceğiyle ilgilidir. Alışveriş ile ilgili gelişmeler, banka ve banka benzeri kurumların da hayatımıza girmesiyle birlikte yöntem anlamında çok daha kullanışlı hale gelmiştir.

Son yıllarda teknolojinin hızlı ve etkili gelişmeleri alışveriş yöntemlerini de çok fazla etkileyip şekillendirmiştir. Kredi kartları, EFT ve havale gibi bankacılık hizmetleri yukarıda bahsedilen "alacak" ve "borç" edimlerinin ifasını gerçek anlamda kolaylaştırmıştır. Bu gelişmeler sayesinde insanlar alışveriş için paralarını daha güvenli ortamlarda saklayıp transfer edebilmiştir. Özellikle bankacılıktaki gelişmeler "Para" kavramını sadece fiziksel bir gereç olmaktan çıkarmakla birlikte "Para"' ya sayısal bir anlam yükleyerek "Sanal Para" kavramının temellerini atmıştır. Bu çalışmalar, yakın zamanımızda daha da ilerleyerek gerçek dünyadan bağımsız yeni ve tam anlamı ile sanal para birimleri ortaya çıkarmıştır. Fiziksel karşılığı olmayan sadece alışverişe yönelik çok hızlı ve çok pratik bir şekilde kullanılan, aslında rakamsal bir ifadeden ibaret olan bu yeni para türü çok fazla rağbet görmüştür ve geleceğin alışveriş yöntemi olacak gibi görünmektedir.

Sanal para ürünleri "değer saklanmış"(stored value) veya "peşin ödenmiş"(prepaid) ürünler olarak tanımlanmaktadır. (Kabakçı, 2013) Telefon kontörleri gibi "peşin ödenmiş" veya alışveriş özendirmelerinde olduğu gibi "değer saklanmış" şeklinde

karşımıza çıkmaktadır. Sanal paranın sunduğu avantajlar gelecekteki kullanımı hakkında bizlere önemli ipuçları vermektedir. Sanal paranın avantajlarından kaynaklanan özel durumlardan dolayı güvenlik ile ilgili önemli tedbirlerin alınması da kaçınılmaz olmuştur. Sanal para mesaj transferlerinde açık ve/veya gizli anahtar şifreleme sistemleri kullanılarak büyük ölçüde güvenlik sağlanmıştır.

Sanal ya da gerçek para kullanılarak gerçekleştirilen ödemelerde önemli bir konu da; ödemenin nasıl ve hangi ortamda gerçekleşeceğidir. Bugün bunun ile ilgili birçok farklı teknolojiler ve yöntemler kullanılmaktadır, bunların birkaçı; Kredi Kartı, Nakit, İnternet, Kıymetli Evrak ve Barter (Takas)… Bu ödeme şekillerinden Kredi Kartı ve internet bankacılığı altyapısındakilerin bir kısmı son yıllarda çok daha fazla kullanılarak güvenilirliği ve popülerliği artmıştır. NFC(Near Field Communication) teknolojisi de son yıllarda gelişen bir teknoloji olması, geliştirilen özel donanımlara ve akıllı telefonlara entegre olması hasebiyle ihtiyaca özgü özel mimariler vasıtası ile ödeme şekillerinde kullanılmaya başlanmıştır. NFC teknolojisi; yakın alan haberleşme mantığı ile çalışmakta olup hızlı veri aktarımına uygun alt yapı sunmaktadır. Ödeme şekli olarak kullanılacağından veri transferinin güvenliği ayrı bir öneme sahiptir fakat NFC'nin birçok alanda kullanılacağı öngörüldüğünden herhangi bir güvenlik tedbiri varsayılan olarak alınmamıştır. NFC ile ilgili güvenlik önlemleri mimari geliştiricilerinin çalışmalarına havale edilmiştir.

Alışveriş işlemlerinde ödemelerin yapılma şeklinin süreç içinde çok değiştiğini belirtmiştik, bu sürecin önemli bir aşaması olan mobil cihazların ortaya çıkması da ödeme şekillerinde önemli yeniliklere sebep olmuştur. Yukarıda bahsedildiği üzere NFC teknolojisin de mobil cihazlarla bütünleşmesi NFC ile ödeme yapma fikrini güçlendirmiştir ve geliştiricileri bu yönde çalışmalar yapmaya yönlendirmiştir.

NFC, RFID spesifikasyonunu (tanımları, özellikleri vb.) temel alır. 13.56 Mhz radyo frekansında çalışır ve bu frekanstaki RFID etiketlerini okuyabilir. NFC'nin RFID'dan en büyük farkı hem okuma hem yazma yapabilmesidir. 4 cm'lik bir mesafede saniyede 424 kbit hızında iletişim sağlayabilir. Araştırmalar NFC uyumlu mobil cihazların NFC yığıt (stack) uygulamalarında çeşitli açıklar ve sorunlar olduğunu göstermiştir. NFC yığıtındaki bu kusurlar kullanıcıya ait bilgilerin ele geçirilmesi ya da cihazın uzaktan kontrol edilebilmesi sonucuna yol açabileceği gösterilmiştir. (Quinlan, 2013)

NFC, birçok alanda kullanılmaktadır, dünyadaki örnekleri açısından aşağıda listelenmiştir. (Michael Roland, 2011)

- Fransa; Ulaşım, ödeme, akıllı poster, öğrenci kimlikleri, müze ve sergilerde rehberlik uygulamaları
- İspanya; Ulaşım uygulamaları
- Hollanda; Stadyum ve sinemalarda bilet uygulamaları,
- Belçika; Ödeme uygulamaları
- Avusturya; Ulaşım ve ödeme uygulamaları
- Almanya; Ulaşım, müze ve sergilerde rehberlik uygulamaları
- İngiltere; Stadyumlarda biletleme, ulaşım, öğrenciler için servis kullanımı ve kişisel sağlık servisi uygulamaları
- Finlandiya; Ulaşım uygulamaları
- İtalya; Kayak merkezlerine giriş kontrolü uygulaması

NFC teknolojisinin 2016 sonuna kadar dünya çapında yaygınlaşarak 448 milyon kullanıcıya ulaşması ve 617 milyar dolarlık mobil ödeme işleminin bu cihazlarla gerçekleşmesi beklenmektedir. (Shen, 2012)

NFC teknolojisinin kullanıldıkları sistemlerin karşı karşıya olduğu ataklar ve bu ataklara dair literatürde çalışmalar yapılmıştır. (Michael Roland, 2011) Bu kaynaklarda belirtilen ataklar aşağıdaki gibidir.

- Hattın dinlenmesi
- Veri bozma
- Veri değiştirme
- Veri ekleme
- Ortadaki adam saldırısı

Literatürde NFC ve güvenlik tabanlı yapılan bazı çalışmalar şöyledir;

Karşılıklı haberleşen cihazlarda NFC kullanımını etkinleştirecek bir tuş kombinasyonu kullanılması bununla birlikte simetrik ve asimetrik şifreleme yöntemlerini kullanarak Android JellyBean cihazlara yönelik elektronik cüzdan alt yapısında bir çalışma yapılmıştır. (Quinlan, 2013) Çalışmadaki şifreleme ve tuş kombinasyonu önlemleri önemlidir fakat cihazın çalınması durumunda bir çözüm üretilmiş değildir.

NDEF mesaj paketleri üzerinde bazı işaretleme teknikleri kullanılarak kayıt değiştirme saldırılarının önüne geçmeyi hedefleyen bir çalışma yapılmıştır. (Michael Roland,

2011)Bu çalışma da ortam dinleme ve kayıt değiştirme saldırılarına karşı etkili olmuştur fakat cihazların komple kopyalanması, cihazın çalınması, NDEF üzerindeki değişikliğin saldırgan tarafından fark edilmesi durumunda bir çözüm sunmamıştır.

Bir başka çalışmada da 3 adımlı bir kimlik onayı yapısı kurularak ortadaki adam saldırı türlerinin önüne geçilmesi hedeflenmiştir (Deepa S Pillai, 2014). Gayet başarılı bir yöntem olarak kabul edilebilir fakat diğer çalışmalar da olduğu gibi ortamın kopyalanması veya çalınması durumunda yine bir önlem alınmamıştır.

Literatürde güvenlik anlamında birçok saldırı türüne karşı güvenli olarak geliştirilmiş; "NFC uyumlu araba anahtarları için çok katmanlı güvenlik mimarisi" çalışması kullanmış olduğu şifre talebi ile güvenliği gerçek anlamda ön plana çıkarmıştır. (Suman Chaudhary, 2014) Anahtarın web servis gibi farklı bir platform üzerinden taşınmıyor olması sistem için önemli bir tehlike oluşturmaktadır.

"NFC tabanlı bütünleşik mobil ödeme, bilet ve kupon çözümü" (Helena Rodrigues, 2014) temasında geliştirilen bir çalışmada da birçok güvenlik önlemi alınmıştır fakat tuş kombinasyonu, şifre sorma gibi bazı saldırı türleri için gerekli olan önlemler kullanılmadığından sistemi tam anlamı ile sorunsuz kabul etmek mümkün değil. Haberleşmenin farklı bir port üzerinden yapılıyor olması sistemin önemli artılarındandır.

Mobil ödemeler için geliştirilmiş iki mimaride de sertifika ve QR kod kullanılarak güvenlik sağlanmaya çalışılmıştır. (Chang, 2014) , (Pardis Pourghomi, 2014)Bu iki sistem sorunlu kullanıcıların bloke edilmesi, bulut ortamı ile SSL haberleşme, tuş kombinasyonu ve cihazın çalınması gibi durumları göz önünde bulundurmadığından bazı saldırı türlerine karşı zaaf bulundurmaktadır.

Performans ve kullanım kolaylığı açısından şifre talebi kullanılmadığından gayet başarılı olan bu mobil cüzdan uygulama çalışmasında (Wei, 2013) da güvenlik anlamında yine şifre kullanılmamasından kaynaklanan birçok zaaf barınmaktadır.

Özel donanımlarla yapılan deneysel bir çalışma olan EMV-TLS uygulaması (Urien, 2015) da sim kartın pin bilgisini kullanarak sağladığı güvenlik, çalışma arşivimiz açısından önemlidir fakat bu sistemin uygulanabilirliği ve çok sübjektif olması aynı

zamanda yukarıdaki çalışmalarda bahsi geçen birçok güvenlik önleminin göz ardı edilmesi sistemi çok tercih edilebilir kılmamaktadır.

Yukarıda kısaca özetlenip referansları verilen çalışmalarda birbirinden farklı güvenlik önlemleri alınmış olup birçok konuda çalışmamıza fikir ve model anlamında önemli katkılar sunmuştur. Çalışmaların amaçları genellikle; sorunsuz bir sistem oluşturmaktan ziyade güvenlik anlamında NFC ile haberleşmeye tek güvenlik açığı başlığında katkı sunmak olmuştur. Bizim çalışmamızda, yukarıda özetlenen ve literatürdeki başka çalışmalar incelendikten sonra muhtemel saldırı türleri ve güvenlik açıkları tespit edilmiştir ardından bu açıklar ile ilgili alınması gereken tedbirler belirlenmiştir. Yapılan bu ön çalışmanın ardından ortaya güvenli bir model çıkarmak hedeflenmiştir. Aldığımız güvenlik tedbirleri ve uygulamalar göz önünde bulundurulduğunda literatürdeki çalışmalara bir hibrit model sunmak kaydı ile katkı sağlanmıştır.

Geliştirmiş olduğumuz sistemin literatürdeki yerinin NFC ile güvenli haberleşmeye bir hibrit model olmasını öngördük. İleri sürülen tezin uygulanmasına da örnek ateşkil etmesi açısından gerçek bir sanal ödeme sistemi geliştirilmiştir.

Site yönetimlerinin site sakinlerinden aylık olarak tahsil ettikleri aidatların takibi ve diğer bütün muhasebe işlemlerinin yönetimini kolaylaştırmak üzere geliştirilmiş olduğumuz Site Yönetim Yazılımı(SYY) ‘nın bağlı olduğu bulut ortamına entegre olmak üzere yeni mobil tabanlı yazılımlar geliştirilmiştir. Geliştirilen bu mobil yazılımlar NFC ile haberleşme altyapısını kullanarak site sakinlerine güvenli bir aidat ödeme imkanı sunmuştur. Geliştirilen mimari; SSL, NFC, AES 128 ile şifreleme ve ilerleyen kısımlarda detaylıca anlatılan birçok güvenlik önlemi ile kullanıcıların sorunsuz ve güvenli bir ortam üzerinde ödemelerini yapmasına katkı sunmaktadır.

NFC tabanlı güvenli aidat ödeme sistemimizin bütün modülleri, güvenlik tedbirleri ve detaylı açıklamaları ilerleyen kısımlarda literatürde önceden yapılmış olan çalışmalar ile kıyaslanarak hibrit model etiketi ile sunulmaktadır. Sonuç olarak geliştirmiş olduğumuz sistem güvenlik anlamında önerdiğimiz bütün tedbirlerin uygulanılmış haline bir örnek teşkil etmektedir ve ileri sürülen tezin uygulanabilirliği görülmekle birlikte gerekli ölçümler de yapılarak ilerde yapılacak çalışmaların hizmetine sunulmuştur.

2. GENEL KISIMLAR

2.1. RFID TEKNOLOJISI

RFID; İngilizce olarak "Radio Frequency IDentification" sözcüklerinin baş harflerinden oluşan ve "Radyo Frekansları Tanıma Teknolojisi" anlamına gelen bir sözcüktür. RFID teknolojisi radyo dalgaları ile bilginin temassız bir şekilde alınmasına dayanır.

Almanya'da 1935 yılında İskoç fizikçi Robert Alexander tarafından keşfedilmiş olan radar sistemi kullanılıyordu. Bu radar sistemi ile bölgeye gelen uçakların dost ya da düşman uçakları olup olmadığını anlamak istediler. Almanlar, pilotlarının uçakları döndürmesi durumunda radardaki sinyallerinin değiştiğini fark ettiler. Bu basit metot radar personelinin gelenlerin Alman mı yoksa düşman uçakları mı olduğunu anlamalarına yarayan aslında ilk pasif RFID sistemiydi. Radarın geliştiricilerinden olan Watson-Watt'ın önderliğinde İngilizler de ilk aktif tanımlama sistemi olan IFF yani; dost mu düşman mı ayrımını yapan sistemi geliştirdiler. Sisteme göre tüm İngiliz uçaklarına yerden gelen radar sinyallerine tepki veren bir aktarıcı koydular. Bu aktarıcı temel olarak bir radar dalgası gönderildiğinde sistem uyanıp ya sinyali geri gönderiyordu ya da yeni bir sinyal üretiyordu. Bu sistemin geliştirilmesi ise RFID adını almıştır. RFID sisteminin bileşenleri temel olarak Etiket, Okuyucu ve Değerlendirme Sistemi olmak üzere 3'tür. (Bank For International Settlements, 1996)

RFID sistemler genel olarak bir etiket ve bir okuyucudan oluşur. Okuyucunun anteni elektromanyetik dalgalar gönderir ve etiketteki anten bu dalgaları algılayarak içindeki bilgileri okuyucuya gönderir. Okuyucunun etiketten aldığı radyo dalgaları şeklindeki bilgiyi dijital bilgiye dönüştürmesiyle işlem tamamlanır. Bu sistemler amaca göre farklı frekanslarda çalışır. Çalışma frekansları ise etiket ve okuyucunun birbirlerini algılayabilmeleri için gereken mesafeyi belirler. (Özdemir S. , 2011)

Bir RFID sistemini temel olarak,

- Etiket
- Okuyucu
- Değerlendirme Sistemi

oluşturur.

1. **Etiket**

İçerisinde bilgi taşıyan ve alıcı/verici anten, bir yonga çip ve gerekli güç kaynağından oluşan kartlar, posterler, şeklinde bulunabilen bir yapıdır.

2. **Okuyucu**

Etiketleri okumak için tasarlanan, farklı güç ve frekanslarda çalışan yapılardır.

3. **Değerlendirme Sistemi**

Bilgisayar ağları ve veritabanı sistemlerinin tümüne verilen addır.

Tablo 2.1: RFID Haberleşme Standartları.

RFID Frekans Türü	**Frekans Aralığı**	**Okuma Mesafesi**
Düşük Frekans(LF)	125-135 Khz	50cm
Yüksek Frekans(HF)	13,6 Mhz	1 – 1,5m
Çok Yüksek Frekans (UHF)	800 -1000 Mhz	5-7 m
Mikrodalga	2,4 Ghz	3m +

2.1.1. RFID Frekansları

2.1.1.1. Alçak Frekans

Normal aralık olarak 30 KHz-300 KHz aralığı olarak tanımlanmasına rağmen, genel olarak kullanımı 125KHz ile 134Khz arasındadır. Kısa okuma mesafesine sahiptir, normal şartlarda yarım metreden de azdır. Daha yavaş bir okuma hızı vardır. Normal şartlarda yüksek frekanslar daha yüksek mesafeler ve okuma hızları demektir. Veri transferi direkt olarak bant genişliği ile orantılıdır. Daha az emilim oranı ki bant genişliği frekans ile ters orantılıdır. Bu nedenle LF sinyalleri atmosfer ve içinden geçtiği malzemeler tarafından daha az emilirler. Bu nedenle metal ve su ile birlikte kullanılabilirler. (Kabakçı, 2013)

2.1.1.2. Yüksek Frekans

HF'in genel olarak kullandığı bant aralığı 3Mhz ile 30Mhz arasındadır. Yakın alan teknolojisinde ise 13.56MHz kullanılmaktadır. HF' in ortalama okuma mesafesi maksimum 3 m' dir. Kısa dalga boyları yüzünden, LF kadar sıvı ve metal gibi malzemeler ile dost değildir. LF'den daha yüksek frekans sayesinde daha yüksek veri aktarım hızlarına sahiptir. Bu özellikler ile genel kullanım alanları bina giriş kontrol sistemleri, bagaj takibi gibi nesne takibi uygulamaları, kütüphaneler örnek olarak verilebilir. (Kabakçı, 2013)

2.1.1.3. Ultra Yüksek Frekans

UHF bant genişliği genel olarak 300 Mhz ile 3 Ghz arasındadır. Ancak 860-960 Mhz arası en sık kullanılan frekans aralığıdır. Haberleşme ve okuma hızı LF ve HF teknolojilerine göre oldukça yüksektir. Otoyol ücretlendirme, stok yönetimi, malzeme takibi gibi uygulamarda kullanılabilir (Kabakçı, 2013).

2.1.1.4. Mikrodalga

Mikrodalga genel olarak 1 GHz ile 300 GHz arası olarak tanımlanmaktadır. Ancak genel olarak 2.44GHz ile 5.80Ghz de yüksek veri transfer oranı olan frekanslar kullanılmaktadır. Yüksek frekanstan kaynaklanan emilim ile ilgili problemler için genelde aktif ve yarı aktif etiketler kullanılarak bu sorun bir avantaja dönüştürülmektedir. (Kabakçı, 2013)

2.1.2. RFID Etiketleri

2.1.2.1. Aktif Etiket

Aktif etiketler enerji ihtiyacını etiket içindeki bataryadan karşılar. Batarya etiket içinde olduğundan, etiket sürekli olarak RF yayını yaparak çevredeki okuyuculara bulunduğu yeri bildirir. Aktif etiketler bu nedenle hantal görünümdedir, aktif etiketler belli periyotlarda batarya değişikliği gerektiğinden bakım gerektirir. Yegane avantajları algılanma mesafelerinin uzun oluşudur. (Kabakçı, 2013)

2.1.2.2. Yarı Aktif Etiket

Yarı aktif etiket, batarya ömrünü uzatmak amacı ile, aktif etiketin yalnızca okuyucu tarafından uyarılması halinde çalışan biçimidir. Aktif etikete benzer avantaj ve dezavantajlara sahiptir. (Kabakçı, 2013)

2.1.2.3. Pasif Etiket

İçinde batarya olmayan, bu nedenle boyut olarak küçük, bakım gerektirmeyen ve ekonomik ömrü en az 10 yıl olan etiketlerdir. Önemli bir üstünlüğü de aktif ve yarı aktif etiketlerden çok daha ucuz olmasındadır. Pasif etiket enerji ihtiyacını okuyucu tarafından oluşturulan endüktif veya kapasitif kuplaj ile sağlar. (Kabakçı, 2013)

2.2. NFC TEKNOLOJISI

2.2.1.NFC Tanımı

Yakın Alan Haberleşmesi (Near Field Comminication)'ın kısaltılmış şekli olarak bilinen NFC; uygun donanımlara sahip cihazların temassız olarak haberleşmesini sağlayan teknolojidir. Veri aktarım hızı ve birçok uygulamaya kolayca entegre olabilmesinden dolayı popülaritesi her geçen gün çok daha fazla artmaktadır.

NFC teknolojisinin noktadan noktaya veri alışveriş kabiliyeti olduğu gibi uçlardan birinin içinde sadece veri saklayabilen pasif bir etiketle de farklı uygulamalar geliştirilebilir. NFC teknolojisi kişisel ve kurumsal bir çok ihtiyaca cevap vermektedir.

NFC 13.56 Mhz frekans bandında çalışan ve saniyede 424 kilobite kadar veri transferi yapabilen 4 cm civarında kısa mesafeli radyo iletişim teknolojisidir. Global bir konsorsiyum olan NFC Forum tarafından standartları ortaya konulmuş ve desteklenen bir teknoloji olduğundan ve uygulamalara entegrasyonu kolay olarak gerçekleşebildiğinden birçok alanda ve uygulamada tercih edilmektedir. Veri haberleşme mesafesinin kısa olması da NFC' yi ayrıca güvenilir kılmaktadır.

Yakın alan haberleşmesi teknolojisi için, radyo frekanslı kimlik tanıma teknolojisinin yüksek frekans (HF-high frequency) ve kısa mesafede kullanılan bir alt kümesidir denilebilir. Çünkü RFID ile metrelerce uzağa veri alışverişi yapılabilirken NFC ile ancak 20 santimetreye kadar olan uzaklıklarda veri alışverişi yapılabilir. RFID sistemlerinin çalışma frekansı 125-134 KHz mertebelerinden yani düşük frekanslardan başlar. NFC sistemlerinin çalışma frekansı ise 13.56 MHz'dir. Çalışma frekansı ve buna bağlı olarak oluşan mesafe farkları kullanım alanlarında da farklılıklar yaratır. RFID'nin yukarıda yazdığım kullanım alanları NFC teknolojisi için geçerli değildir. NFC teknolojisi ödeme, bilet, servis sorgulama ve veri paylaşımı için kullanılır. Ödeme gibi güvenlik gerektiren bir alanda kullanılması da NFC teknolojisinin RFID sistemlerden daha gelişmiş olduğunun bir kanıtıdır. (Özdemir S. , 2011)

2004 yılında Nokia, Philips ve Sony firmaları tarafından kurulan NFC Forum tarafından ortaya koyulan NFC, başlangıçta sadece akıllı poster mantığında tek taraflı bir haberleşme sunmakta iken 2006 yılında iki yönlü haberleşmenin de mümkün

olabileceği şekilde gelişmeler yaşanmıştır. Akıllı telefonların gelişmesi ile birlikte birçok farklı uygulamalarda kullanılmak ile günümüzde artık rahatlıkla kullanılabilir bir hal almıştır.

NFC Standartları ISO/IEC, ETSI, ve ECMA tarafından yayımlanmaktadır. NFC data transfer hızı saniyede kilo bit hızlarında ölçülmüştür. NFC Standartları çeşitli data hızlarını desteklesede, mevcut data transfer hızları 106 kbps, 212 kbps ve 424 kbps' dir (Bank For International Settlements, 1996).

NFC ile mobil ödeme uygulamaları son kullanıcılara çok büyük avantajlar sağlar, yanlarında farklı bankaların kartlarını taşımak yerine zaten sürekli yanlarında olan cep telefonlarıyla alışverişlerini güvenli bir şekilde gerçekleştirebilirler.

NFC etiketlerinin SIM kartlara entegre olabilmesiyle ödeme sistemleri cihazdan bağımsız olarak da kullanılabiliyor. Yani NFC özelliği olan bir telefon zorunluluğu ortadan kalkıyor. Yine de lider cep telefonu üreticilerinin yeni nesil telefonları NFC özelliği ile piyasaya sürmesi SIM karta entegre yakın alan haberleşmesi teknolojisinin çok da fazla yaygınlaşmayacağını gösterir nitelikte. (Özdemir S. , 2011)

NFC iletişimi sırasında, NFC uyumlu cihaz diğer kart okuyucuları ve akıllı posterlerde bulunan etiketler ile etkileşime geçen radyo frekans sinyalleri gönderir. Etiket tarafından alınan bu sinyal akım oluşturur ve iki uygun cihaz arasında iletişimi sağlar. Tipik olarak bir etiket pasif bir cihazdır ve yalnızca okuyuculara bilgi gönderir. Akıllı telefonlar gibi aktif cihaz ise hem bilgi alan hem bilgi gönderen cihazlardır. (Kabakçı, 2013)

NFC: Bu üç harf çok yakında GSM ve ADSL kadar tanınmış olacak (Destot M. , 2009)

2.2.2. NFC Türleri

NFC teknolojisi 4 farklı etiket tipine, 4 farklı sinyalleşme teknolojisine ve belirli NFC cihazların yaptığı 4 farklı çalışma moduna sahiptir. NFC cihazlarının birbirleriyle haberleşmesinde kullanılan 3 sinyalleşme teknolojisi mevcuttur. Çalışma modlarının her biri bu tezde açıklanmaktadır. Okuyucu ve etiket haberleştiği anda ilk olarak kullanılan protokol belirlenir. (Kabakçı, 2013)

2.2.2.1. NFC - A

NFC-A RFID A tipi iletişim teknolojisine karşılık gelir. A tipi iletişimde, gecikme kodlaması olarak da bilinen, Miller kodlaması %100 genlik modülasyonu ile kullanılır. Kurulum aşamasında genliği yüzde 0' dan yüzde 100' e değişen sinyal gönderilir. A tipi iletişimde veri hızı 106 kbps' dir.

2.2.2.2. NFC - B

RFID-B tipi iletişime karşılık gelen NFC-B iletişim teknolojisi A tipi iletişim teknolojisine benzemektedir. Miller kodlaması yerine Manchester kodlaması yapılır. Genlik modülasyonu %10' dur. %10' un anlamı %90' nın low, %100' ün ise high sinyali için kullanıldığını gösterir. Alçak sinyalden yüksek sinyale geçişler 0, yüksekten düşük sinyale geçişler 1 ile temsil edilir.

2.2.2.3. NFC - F

NFC-F FeliCa olarak bilinen daha hızlı RFID iletişimi temsil etmektedir. FeliCa Japonya da kullanılan NFC' ye benzer, fakat daha hızlı çalışan bir temassız iletişim sistemidir. Ödeme sistemlerinde kullanılan çok popüler bir teknolojidir.

2.2.2.4. NFC SD ve Sim Kartlar

NFC mobil ödeme sistemlerini kullanmak isteyen fakat herhangi bir NFC uyumlu cep telefonu olmayan kullanıcılar için hali hazırda NFC SD ve SIM kartlar mevcut olarak hizmet vermektedir. Bazı şirketler her iki kartı birden de telefon çipleri içerisinde tasarlamaktadır.

2.2.2.5. Felıca Teknolojisi

FeliCa Japonya da popüler olarak temassız ödeme sistemlerinde kullanılan RFID' nin bir türüdür. FeliCa, NFC' ye benzer ve NFC uyumlu cihazlar ile birlikte çalışabilir. Temel olarak alışveriş ve bilet uygulamalarında kullanılılan FeliCa kartları pasif cihazlardır ve kendisinin herhangi bir güç kaynağı yoktur. Kart okuyucular ile arasındaki mesafe yaklaşık olarak 10 cm' dir. FeliCa teknolojisi 13.56 Mhz frekans bandında çalışmakta olup, Manchester kodlamasını kullanmaktadır.

2.2.3. NFC Çalışma Modları

NFC cihazları okuma/yazma, P2P ve kart emülasyon modu olmak üzere 3 modda çalışır. Farklı çalışma modları ISO/IEC 18092, NFC IP-1 ve ISO/IEC 14443 temassız akıllı kart standartlarında bahsedilmektedir.

- **Okuma/Yazma modunda,** NFC cihaz akıllı poster üzerinde yazma ve okuma yapabilir. Bu mod ISO/IEC 14443 ve FeliCa şemalarında açıklanmaktadır.
- **P2P modunda,** iki NFC cihazı veri alışverişinde bulunabilir. Bu mod ISO/IEC 18092 standartlarında açıklanmaktadır.
- **Kart Emülasyon modunda,** NFC cihazları geleneksel temassız akıllı kartlar gibi harici bir okuyucu olarak davranır. Bu mod mobil ödeme ve biletleme sistemlerinde kullanılmaktadır. (Bank For International Settlements, 1996)

Veri paylaşımı NFC teknolojisinin P2P(Peer to Peer) modu kullanılarak gerçekleştirilir. Klasik bluetooth gibi çalışır ve iki cep telefonu arasında müzik, ses dosyası, kartvizit, ajanda bilgileri vb. verileri aktarmada kullanılır. Bluetooth'la kıyaslandığında iki telefonu birbirine yaklaştırıp veri alışverişine başlama süresi oldukça kısadır. Ayrıca güvenlik bakımından bluetooth'a göre çok üstündür. Fakat ne yazık ki sadece çok kısa

mesafelerde çalışabilmesi ve veri hızının düşük olması sebepleriyle çok fazla tercih edilen bir uygulama değildir. Aşağıdaki tabloda NFC, Bluetooth V4.0 ve Bluetooth V2.1 arasında bazı özellikleri bakımından bir kıyaslama yapılmıştır. (Özdemir S.)

Bluetooth ve Wi-Fi NFC gibi yüzey üzerinde yakın alan teknolojisini kullanır. Bu üç iletişim şeklide akıllı telefonlar gibi dijital cihazlar arasında kablosuz veri iletişimi ve veri haberleşmesine imkan verir. Ancak Bluetooth ve Wi-Fi radyo iletişimini kullanırken, NFC elektromanyetik radyo alanlarını kullanmaktadır. NFC, RFID teknolojisinin bir parçasıdır.

Tablo 2.2: Bluetooth ve NFC karşılaştırması (Özdemir S.).

*	NFC	BLUETOOTH 4.0	BLUETOOTH 2.1
Güvenlik	Yüksek	İyi	İyi
Mesafe	<0.2m	<1m	<10m
Modlar	Aktif/Pasif	Aktif	Aktif
Güç	15mA	15mA	sınıfa göre değişken
Veri hızı	424kbps	200kbps	2.1mbps
Frekans	13.56 MHz	2,4-2,5 GHz	2,4-2,5 GHz
Bağlantı Tipi	Point to point	WPAN	WPAN
Başlatma Süresi	<0.1sn	<6sn	<1sn

ISO Standartlarında 3 tip NFC teknolojisi mevcuttur. ISO 14443 A Tipi, B Tipi ve FeliCa. Hepsi birbirine benzerdir fakat farklı şekillerde iletişim kurmaktadırlar. Her biri 13.56 Mhz frekans bandında okuyucu anten ile yakın kuplaj temassız kartlar için kullanılan standartlardır. FeliCa yaygın olarak Japonya da kullanılmaktadır.

NFC teknolojisi güvenli iletişim adına, kredi kartı bilgileri gibi hassas bilgi alışverişi sırasında, güvenli bir kanaldan iletişim yapmaktadır. Kullanıcılar özel verilerini şifre kullanarak cep telefonlarındaki anti-virus yazılımları ile koruyabilmektedirler. Böylece veri hırsızarının önüne geçilmeye çalışılmaktadır. (Kabakçı, 2013)

NFC Teknoloji Standartları ;

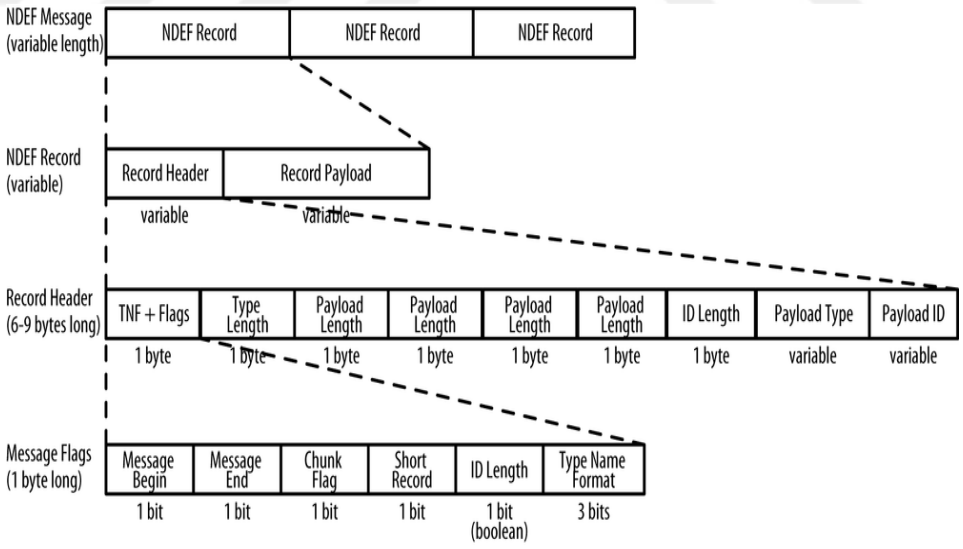
- ISO/IEC 14443, NFC taglarında bilgi saklanması için kullanılan ID kartlar için geliştirilmiş standarttır. NFC cihazları tarafından kullanılan RFID iletişimi için geliştirilmiştir.
- ISO/IEC 18000-3, NFC' nin de kullandığı A ve B tipi kartlarında 13.56 Mhz frekans bandında çalışan tüm kablosuz iletişim standartlarını kapsar.

2.2.4. NDEF (NFC Data Exchange Format)

NDEF formatı çeşitli RFID protokolleri ve NFC etiketlerini tek bir formatta kapsamak ve temsil etmek için kullanılan basit bir ikili mesaj formatıdır. (Quinlan, 2013)

Bir NDEF kaydı aşağıdakileri içerir (Destot M. , 2009):

1. Birden çok başlık alanı (header field) ve payload içerir.
2. Bir başlık ise aşağıdaki flag'leri içerir:
    - Message Begin (Mesaj başlangıcı-MB)
    - Message End (Mesaj bitimi-ME)
    - Chunk Flag (CF): Kaydın payload'ının bir sonraki kayıtta devam edeceğini belirtir.
    - SR (Short Record-Kısa kayıt)
    - ID length present (IL-Seçimli ID alanı ve ona karşılık gelen uzunluk alanının sunulduğunu belirtir)
    - Type Name Format (Tip adı formatı): Verilerin hangi tipte olduğunu belirtir.



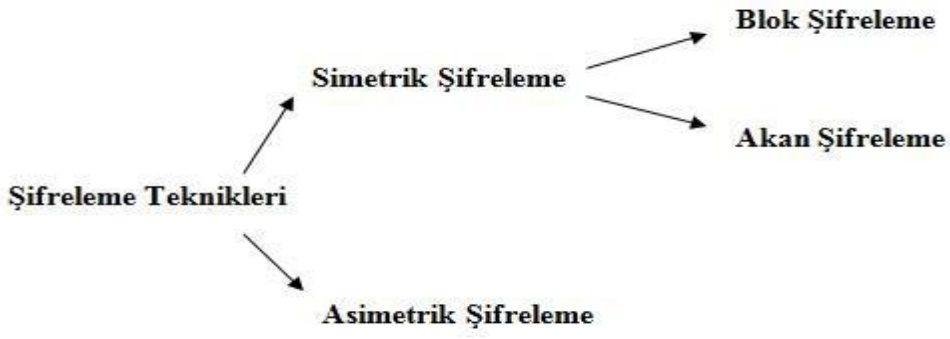
Şekil 2.1: NDEF Yapısı

2.3. ŞİFRELEME YÖNTEMLERİ

Şifreleme, verilerin herkese açık ortamlarda iletilirken istenmeyen kişiler tarafından kullanılmasını veya değiştirilmesini önlemek amaçlı kullanılır. Şifreleme işlemi önceleri sadece askeri amaçlı kullanılmaktaydı. Ancak günümüzde gelişen teknoloji ile veri güvenliği önemli bir sorun haline gelmiştir. Bu yüzden kriptografinin alanı genişlemiş ve şifreleme, veri haberleşmesinde yaygın olarak kullanılır hale gelmiştir. Şifreleme işleminde düz metin, şifreleme işlemine tabi tutulur ve bu işlem sonucunda elde edilen şifrelenmiş veri alıcı tarafa yollanır. Alıcı taraf şifrelenmiş veriyi şifre çözme işlemi ile düz metin haline çevirir . Bu yolla haberleşme kanalında esas veri anlaşılmaz bir halde gönderilir ve verinin başkaları tarafından elde edilmesi ve değiştirilmesi engellenmiş olur. (Kula)

Şekil 2.2: Şifreleme ve şifre çözme işlemleri diyagramı.

Şifreleme sistemleri işleyişi bakımından temel olarak iki ana başlıkta incelenebilir. Bu sistemler simetrik şifreleme ve asimetrik şifreleme sistemleridir.



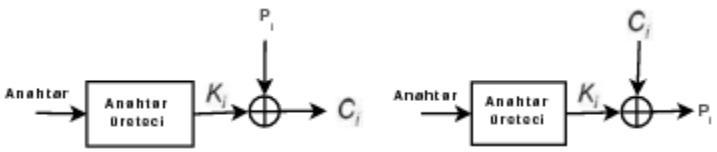
Şekil 2.3: Şifreleme Teknikleri.

2.3.1. Simetrik Şifreleme

Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemleri için tek bir gizli anahtar kullanmaktadır. Bu durum veri şifreleme için matematiksel açıdan daha az problem çıkaran bir yaklaşımdır ve çok kullanılan bir yöntemdir. Bu tip algoritmalarda şifreleme işlemi gerçekleştirildikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermek gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı bir şekilde şifreleme ve şifre çözme işlemlerini gerçekleştirebilmektedir

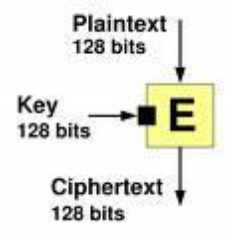
Simetrik Şifrelemede hem şifreleme hem de şifre çözme işlemlerinde aynı anahtar kullanılır. Simetrik şifreleme algoritması; açık metni ve gizli anahtarı veri girişi olarak alıp, çıktı olarak şifreli metni üretir. Algoritmadaki amaç şifreli metnin açık metne dönüşümünün gizli anahtar kullanılarak sağlanmasıdır dolayısıyla gizli anahtarın bilinmediği durumlarda dönüşüm gerçekleşemez. Açık metine erişim sadece gizli anahtar bilindiği durumlarda mümkün olmalıdır. Simetrik şifreleme teknikleri blok şifreleme ve akan(dize) şifreleme olmak üzere ikiye ayrılır. (Vural, 2006)

Dizi şifreleme sistemlerinde şifreleme işleminde anahtar üretilir ve verinin her bir biti ile anahtarın her bir biti exorlanır. Verinin her bir biti sırayla şifrelenir. Alıcı taraf şifrelenmiş veriye yine anahtar ile e-xor işlemi uygular ve düz veriyi elde eder. Dizi şifreleme sistemlerinin işleyişinin blok diyagramı şekilde verilmiştir (Doğan, 2006).



Şekil 2.4: Dizi Şifreleme.

Blok şifreleme sistemlerinde ise veri belirli uzunluktaki veri blokları halinde şifrelenir. Şifreleme için karmaşık işlemler ve algoritmalar kullanılır. Blok şifrelemeye örnek olarak 128 bitlik veri bloğunun aynı uzunluktaki anahtar ile şifrelenerek yine aynı uzunlukta şifrelenmiş veri elde edilmesinin blok diyagramı Şekil 4'de verilmiştir.



Şekil 2.5: Blok Şifreleme.

2.3.1.1. AES Şifreleme Tekniği

Gelişmiş şifreleme standardı (AES) veriyi 128 bitlik paçalar halinde şifreleyen bir blok şifreleme algoritmasıdır. Kullandığı anahtar uzunluğuna göre AES-128, AES-192 ve AES-256 olmak üzere üç çeşittir (Fips). Bu tezde AES'in 128 bit uzunluğunda anahtar kullandığı çeşidi üzerine çalışılmıştır.

AES-128 10 çevrimdir. İlk olarak 128 bitlik anahtar on çevrimde farklı şekliyle kullanılması amacıyla genişletilir (Fips). Daha sonra Tur Anahtarını Ekleme adımı gerçekleşir. Bu aşamadan sonra 10 çevrim gerçekleşir. Her çevrim sırasıyla Bayt Değiştirme, Satırları kaydırma, Sütunları karıştırma ve Tur Anahtarını Ekleme işlemlerinden oluşur. Son çevirm olan onuncu çevrimde Sütunları Karıştırma adımı uygulanmaz (Kula).

AES algoritması kendini tekrarlayan bir yapıdadır. Kullanılan anahtar boyutuna göre bu tekrarların bir başka deyişle çevrimlerin sayısı değişir. Bu çevrim sayıları 128 bitlik anahtar kullanımı için 10, 192 bitlik anahtar kullanımı için 12 ve 256 bitlik anahtar kullanımı için 14'tür. AES çevrimi sırasıyla yukarıda anlatılan dört adımdan oluşur. (Doğan, 2006)

AES Şifrelemede yapılan işlemler aşağıda kısaca verilmiştir. (Kula)

- Bayt Değiştirme

  İlk olarak 128 bitlik veri 8'er bitlik 16 parçaya ayrılır ve 4x4 boyutundaki durum matrisi oluşturulur. Tüm işlemler bu durum matrisi üzerinden gerçekleşmektedir. Bayt değiştirme adımında her 8 bitlik parçaya matematiksel

bir dönüşüm uygulanır. Bu dönüşüm iki aşamada gerçekleşir. İlk olarak indirgeme kullanılarak çarpmaya göre ters alma işlemi uygulanır. Burdan elde edilen sonuç bir geçiş matrisi ile çarpılarak sabit bir matris ile toplanır [1]. Bu işlemlerin sonucunda bayt değiştirme adımı sonucu elde edilir. Bu dönüşümler 8 bitlik 16 veriye seri olarak tekrarlandığında 128 bitlik veri bu adımdan geçmiş olur.

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

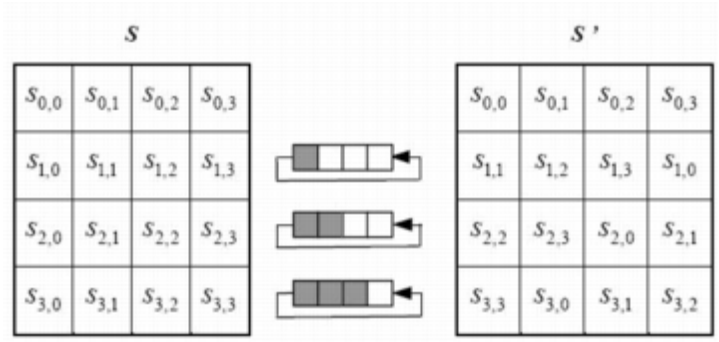
Şekil 2.6: Durum Matrisi.

- Satırları Kaydırma

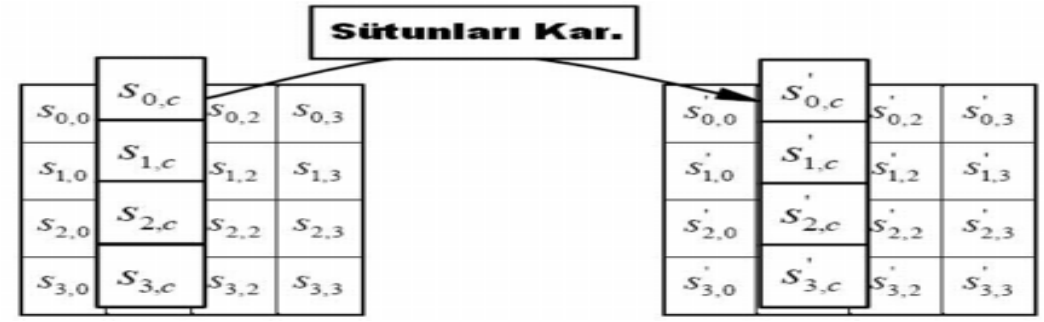
  Bu adımda Bayt Değiştirme işleminden elde edilen veri yine 8‟er bitlik 16 parçaya ayrılır ve 4x4 boyutunda bir matris haline getirilir. Martisin ilk satırı sabit bırakılarak ikinci, üçüncü ve son satırlar sırasıyla bir, iki ve üç kere sola kaydırılır ve bu işlemler sonucu yeni bir 128 bitlik veri elde edilir.

- Sütunları Karıştırma

  Süt Satırları Kaydırma adımında oluşan 128 bitlik verinin 8‟er bitlik 16 parçasının herbiri belirli işlemlere tabi tutularak yeni bir 128 bitlik veri elde edilir



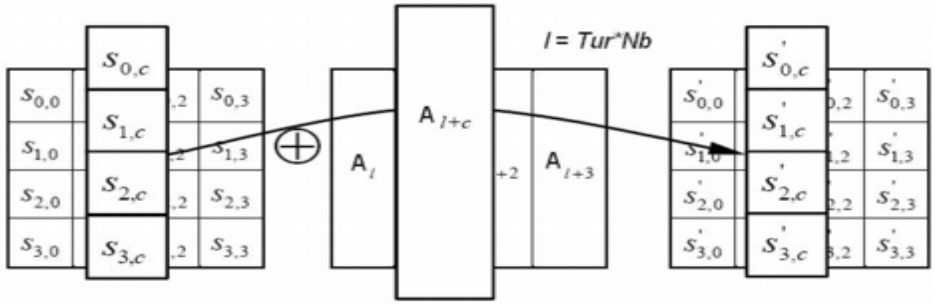
Şekil 2.7: Satırları Kaydırma.



Şekil 2.8: Sütunları Karıştırma.

- Tur Anahtarını Ekleme

  Bu aşamada bir önceki işlemin sonucunda elde edilen 128 bitlik durum matrisi ile genişletilen anahtarın o çevrimle ilgili bölümü olan 128 bitlik anahtar dizisi exorlanır.



Şekil 2.9: Tur Anahtarı Ekleme.

2.3.2. Asimetrik Şifreleme

Açık anahtarlı şifreleme algoritmaları simetrik şifreleme algoritmalarından radikal bir farklılık göstermektedir. Bu tip şifreleme algoritmaları açık (public) ve özel (private) anahtar olmak üzere iki ayrı anahtar kullanmaktadır.

Asimetrik algoritmalar da denilen açık anahtarlı algoritmalarda şifreleme için kullanılan anahtar ile şifre çözme için kullanılan anahtar birbirinden farklıdır. Anahtar çiftlerini üreten algoritmaların matematiksel özelliklerinden dolayı açık-özel anahtar çiftleri her

kişi için farklıdır, diğer bir deyişle her kullanıcının açık-özel anahtar çifti yalnızca o kullanıcıya özeldir. Ayrıca şifre çözüm anahtarı (en azından makul bir zaman dilimi içerisinde) şifre anahtarından hesaplanamaz. Bu algoritmalara açık anahtarlı algoritmalar denmesinin sebebi şifre anahtarının halka (kamuya/genel kullanıma) açık olmasıdır. Bir yabancı bir iletiyi şifrelemek için şifreleme anahtarını kullanabilir, ancak sadece ilgili şifre çözüm anahtarına sahip bir kişi iletinin şifresini çözebilir. Bu sistemde, şifre anahtarına genellikle açık anahtar adı verilmektedir. Şifre çözüm anahtarı da genellikle özel anahtar olarak adlandırılmaktadır. Özel anahtar kimi zaman gizli anahtar olarak da adlandırılır, ancak simetrik algoritmalarla karışmaması için bu terim genelde kullanılmamaktadır.

Bir kullanıcının açık anahtarıyla şifrelenen bir mesajı, yalnız ve ancak ona ait özel anahtar çözebilmektedir. Aynı şekilde, herhangi bir kullanıcının özel anahtarıyla attığı sayısal imzanın doğrulanabilmesi, yalnızca o kullanıcının açık anahtarını kullanarak mümkün olabilmektedir. Açık anahtar kamuya açıktır, elektronik kimlik belgelerinin içinde diğer kişisel bilgilerle birlikte tutulur ve herkes birbirinin açık anahtarını e-kimliklerine ulaşmak suretiyle istediği zaman elde edebilir.

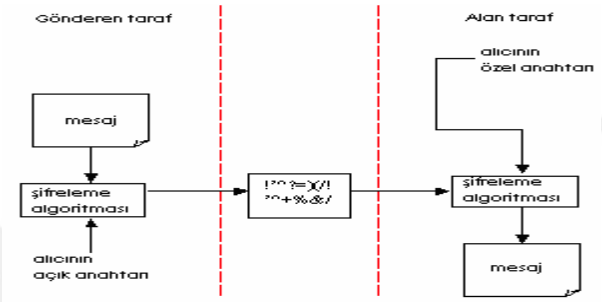
Şifreleme açık ağlardan gönderilen bilginin başkaları tarafından görülmesinin (dinlenmesinin) istenmediği zaman yapılmaktadır. Bunun için çift anahtarlı bir şifreleme algoritması kullanılabilir. Buna göre, mesajı gönderen taraf, gönderilen bilginin sayısal içeriğini, mesajı alacak tarafın açık anahtarını, sayısal şifrelemede kullanmaktadır. Mesajı alan taraf da, şifreli mesajı çözmek için şifreli mesajın sayısal içeriği ve kendisinin özel anahtarına gereksinim duymaktadır .

Burada dikkat edilecek olursa, şifreli mesajın üçüncü taraflar tarafından dinlenebilmesi ancak “özel anahtara” sahip olmaları ya da şifreli mesajı matematiksel yollarla deşifre etmeye çalışmaları ile mümkün olabilmektedir. “Güvenlik açısından iyi bir şifreleme” algoritması, özel anahtar olmadan şifreli mesajı deşifre etmeye imkân tanımayan bir algoritmadır.

Açık-anahtar şifreleme için pek çok algoritma bulunmaktadır. En yaygın olan iki tanesi RSA (Ron Rivest, Adi Shamir, Leonard Adleman) algoritması ve DSA’dır (Digital Signature Algorithm - Dijital İmza Algortiması). RSA, pek çok uygulamada kullanılan bir

algoritmadır. Mesajları şifrelemek için kullanılabileceği gibi dijital imzalarda da kullanılabilmektedir. DSA, sadece dijital imza kullanımı içindir. Mesajları şifrelemek için kullanılmamaktadır. (Halife Kodaz, 2010)

Anahtarların deneme-yanılma yöntemiyle bulunmasını engellemek için, bugünkü süper bilgisayarlardan milyonlarca kat daha hızlı çalışan bir bilgisayarla bile milyarlarca yıl sürmesi için, kullanılan anahtarların uzunluğunun mümkün olduğunca büyük olması gerekmektedir.



Şekil 2.10: Şifreli mesaj gönderilmesi ve alınması.

Sağladığı güvenlik açısından asimetrik anahtarlı şifreleme yöntemlerinin daha güvenli bir uygulamayı destekleyebileceği fark edilmiştir. Bunun arkasında yatan sebep ise asimetrik anahtarlı şifrelemede açık anahtarı etrafa gönderen yetkin tarafın sadece kendisinin deşifre etme özelliğine sahip olmasıdır. Bu tip bir sistemde ortamda bulunan diğer birimler açık anahtarı kullanarak kendi verilerini şifreleyebilirler ancak şifrelenmiş bir veriyi deşifre etme yeteneği sadece bahsedilen yetkin birime verilmiştir. Bu özelliği sayesinde asimetrik anahtarlı şifreleme uygulamalarında güvenlik faktörü daha iyi sağlanmaktadır.

2.4. SALDIRI TÜRLERİ

Çalışmamız kapsamında ve literatür araştırmaları neticesinde NFC tabanlı sistemlerin karşılaşmış oldukları saldırı türleri tespit edilmiştir ve geliştireceğimiz sistemin tespit edilen 6 adet saldırı türüne karşı güvenli olması farklı güvenlik önlemleri vasıtası ile sağlanmıştır.

2.4.1. Sniffing (Dinleme)

Birden fazla bilgisayarı, birbirine bağlayarak aralarında bir paylaşım kurmak masraflı bir iştir. Paylaşım, bir bilgisayardaki bilgilerin, başka bir bilgisayara aktarılması olarak açıklanabilir. Bu iki bilgisayar arasında yapılan bilgi alış-verişini yakalamaya "sniffing" denilir. Çalışma kapsamında, bu saldırı türünün NFC'nin RFID ortamı ya da web servisin Ethernet ortamında gerçekleştirileceği varsayılmaktadır.

Sniffing olarak bilinen dinlemede, RFID etiketler, uygun tüm okuyucular tarafından okunacak şekilde tasarlanırlar. Etiketler üzerinde bulundukları canlı ya da cansız maddenin onayını almadan menziline girdikleri okuyuculara cevap verirler. Bu durumu bilen bir saldırgan uzak menzilli bir RFID okuyucuyu kullanmak suretiyle etiketlerin bilgilerine erişebilir. Sayısal pasaportlar bunun en sık karşılaşılan örneğidir.

Literatürde ' Eavesdropping ' anlamında kullanılan gizlice dinleme, NFC hareketlerinin dinlenmesiyle kriminal bir suç olmaktadır. Gizlice dinleme iki şekilde önlenebilir. İlki iletişim mesafesini daraltmaktır. Böylelikle araya girilen diğer sinyaller önlenmiş olur ve iletişim daha sınırlı bir alanda güvenli hale gelir. Dinlemenin ikinci yöntemi, güvenli iletişim kanalları oluşturmaktır. Güvenli bir iletişim kanalı oluşturulduğunda, veriler şifrelenir ve sadece yetkili cihaz tarafından deşifre edilebilir. NFC kullanıcıları bu hizmetleri alırken, hizmeti aldıkları kurumların güvenli iletişim kanalı oluşturduklarına güvenirler.

Hiçbir enkripsiyon bir kişinin çalınan bir telefonunu asla koruyamaz…Eğer bir telefon çalınırsa, hırsız teorik olarak kart okuyucuyuda ele geçirmiş ve bir şeyler satın alabilir duruma gelmiş demektir. Bunu önlemek için telefon sahipleri, telefonlarına şifre veya diğer kilit mekanizmaları yüklemelidir. Bu sayede hırsız telefondaki hassas bilgilere ve bir takım nesnelere erişemeyecektir.

NFC' nin yeni güvenlik riskleri ortaya çıktıkta daha da geliştirilicek ve bir kredi kartından daha güvenli hale gelecektir. Eğer bir kişi kredi kartını çaldırırsa, kartı çalan hırsız kişinin kart bilgilerini ve kartın kime ait olduğunu rahatlıkla okuyabilir. Fakat aynı kişi bir kredi kartı yerine akıllı telefonunu çaldırırsa, telefonu çalan hırsız, şifre/kilit engeline takılacak ve özel bilgilere erişemeyecektir. (Kabakçı, 2013)

2.4.2. Spoofing (Aldatma)

Spoofing olarak bilinen bu yöntemde, saldırganlar boş ya da okunur-yazılır özelliğine sahip etiketleri yazmak suretiyle gerçeği anımsatmayacak şekilde RFID etiketleri oluşturabilirler. Dikkate değer bu tür bir atağı Johns Hopkins University ve RSA Security araştırmacıları gerçekleştirdiler. Araştırmacılar sinyal dinleme yöntemini kullanarak mevcut bir araba etikeninin bir kopyasını çıkardılar. Kopyaladıkları bu etiketi kullanarak önce benzin aldılar ve ardından arabayı kilitlediler. (Kabakçı, 2013)

Bu saldırı türü ile saldırgan ortamda bulunan iki cihazdan birinin kopyasını oluşturarak diğer cihaz ile haberleşmeye çalışır ve böylelikle bizim için önemli olan verilere erişir ya da sistem üzerinde yetkisiz işlemler yapar. Sistemimizde bu saldırılara karşı da gerekli önlemler alınmıştır.

2.4.3. Paket Manipülasyon

Bir kişi veride bozma yaratarak okuyucuya veya aracı bir kişiye gönderdiği zaman veri bozulması ve manipülasyon meydana getirmiş olur. Bunu önlemenin yolu yine güvenli iletişim kanalları oluşturmaktır. Bazı NFC cihazları veri bozulma saldırılarına karşı dinleme moduna geçer ve saldırı başlamadan önlemeye çalışır.

Dijital suçların bir adım ötesinde bir saldırıdır. Bir kişi iki NFC cihazı arasına girerek bilgileri alır ve manipülasyon yaratır. Bu saldırı zordur ve az rastlanır. Bunu önlemenin yolu, cihazların aktif-pasif çiftlerinde olmalarıdır. Bunun anlamı her iki cihazın bilgi alıp vermesi yerine, bir tanesinin bilgi alırken diğerinin sadece göndermesidir. (Kabakçı, 2013)

Bu saldırı türü sistem içindeki cihazların haberleşme esnasında birbirlerine gönderdikleri paketler üzerinde ekleme, değiştirme veya bozma şekline işlemler yaparak haberleşmenin aksamasına veya farklı sonuçlar üretmesine sebep olmaktadır. Bu saldırı türünün sistemin çalışması ile ilgili getirdiği olumsuzluklar Sniffing saldırısında bahsedilen güvenlik önlemlerimiz ile kontrol altına alınabilir.

2.4.4. Replay Attacks (Tekrarlı Saldırılar)

Replay attacklar olarak bilinen bu yöntemde, saldırganlar uygun RFID cihazları kullanarak, RFID okuyucudan gönderilen sorgu sinyallerini durdurup yeniden gönderebilirler. Bu tür yeniden sinyal gönderim işlemleri, sayısal pasaport okuyucularını, temassız ödeme sistemlerini, bina erişim kontrol istasyonlarını zayıf duruma sokar. (Kabakçı, 2013)

Bu saldırı türü ile saldırgan iki tür saldırı hedeflemektedir. Birincisi; Sistemdeki haberleşmelerde kesintiler ve karışıklıklar oluşturarak sistemin çalışmasını zaafa uğratmaktır, bu saldırı için Sniffing ve Paket Manipülasyonu saldırılarında alınan önlemler düzeyinde karşılık verebileceğimizden bizim veri güvenliğimizi tehdit etmemektedir. İkincisi; saldırgan tekrar göndermek üzere aldığı bir mesaj paketini farklı zamanda tekrar karşı cihaza gönderirse karşıdaki cihaz paketi sorunsuz bulup işleme alacağından sahte cihaza istediği sonucu dönecektir.

2.4.5. Denial Of Service (Hizmet Durdurma)

Denial of service olarak bilinen bu yöntemde, tamamen verilen hizmeti durdurmaya ve yavaşlatmaya yönelik olarak yapılan bir saldırı yöntemidir. Etiketlerin okunması Faraday kafesi ya da sinyal boğma yöntemiyle engellenir. Bu iki yöntem de radyo sinyallerinin RFID etiketlere erişmesini engeller. (Kabakçı, 2013)

Bu saldırı türü ile saldırganın tek hedefi sistemi meşgul ederek kullanılmaz hale getirmektir. Bu tür bir saldırıda saldırgan ile gerçek kullanıcıyı ayırt etmek zor olduğundan bunun ile ilgili geliştirdiğimiz yöntem gerçek ya da sahte olsun kullanıcıyı sürecin içine katmakla olabilir. Şöyle ki; kullanıcıya bir tuş aktivasyonu, Login gibi işlemi zorunlu tutarak farklı bir cihazla üst üste işlem yapılmasının önüne geçilmiş.

2.4.6. Man In The Middle Attack (Ortadaki Adam)

Man-in-the-Middle-Attack olarak bilinen bu yöntemde, okuyucular bu etiketler ile 10 m’ den haberleşebilirler. Bu özellik daha güçlü okuyucular kullanan kişilerin dikkatini

çekmektedir. Bu durumda okuyucu ile etiket arasındaki iletişim biçimi dinlenmeye alınmak suretiyle hem erişim şifresi hem de etiket kimlik numarası ile ele geçirilebilir.

Bu saldırı türü ile sistemimizde haberleşmek üzere bulunan iki cihazımızın dışında saldırganın ortama yerleştirdiği üçüncü bir cihaz söz konusudur. Ortamdaki 3. Cihaz A cihazından gelen veriyi alır ve aynen B'ye gönderir, B işlemlerini yapar ve cevap olarak paketi RF ortamına bırakır, 3.cihaz B'den gelen cevabı alır ve A'ya iletir ya da iletmez, sonuç olarak böyle bir senaryoda haberleşmenin 3.cihaz üzerinden ilerlediğini ve bütün mesaj paketlerimize ulaşabildiğini gördük.

3. MALZEME VE YÖNTEM

3.1. GELİŞTİRİLEN YAZILIMLAR

Apartman site yönetimlerinin ihtiyacı olan satın alma, muhasebe, aidat tahakkuk ve tahsilatı gibi önemli işlerin takibini yapmak site yönetimlerine büyük bir iş yükü getirmektedir. Site sakini sayısının yüzlerce kişiye ulaşması durumunda, bu iş yükünün üstesinden gelinmesi bir yazılım olmaksızın imkansızlaşmaktadır. Geliştirmiş olduğumuz sistemin modüllerinin bir kısmı bu ihtiyaçlara yönelik getirilmiş çözümlerdir. Site yönetimlerinin, kullandıkları yazılımlardan önemli bir beklentileri de site sakinlerinin aidatlarının tahsilatında sunulacak kolaylıklardır.

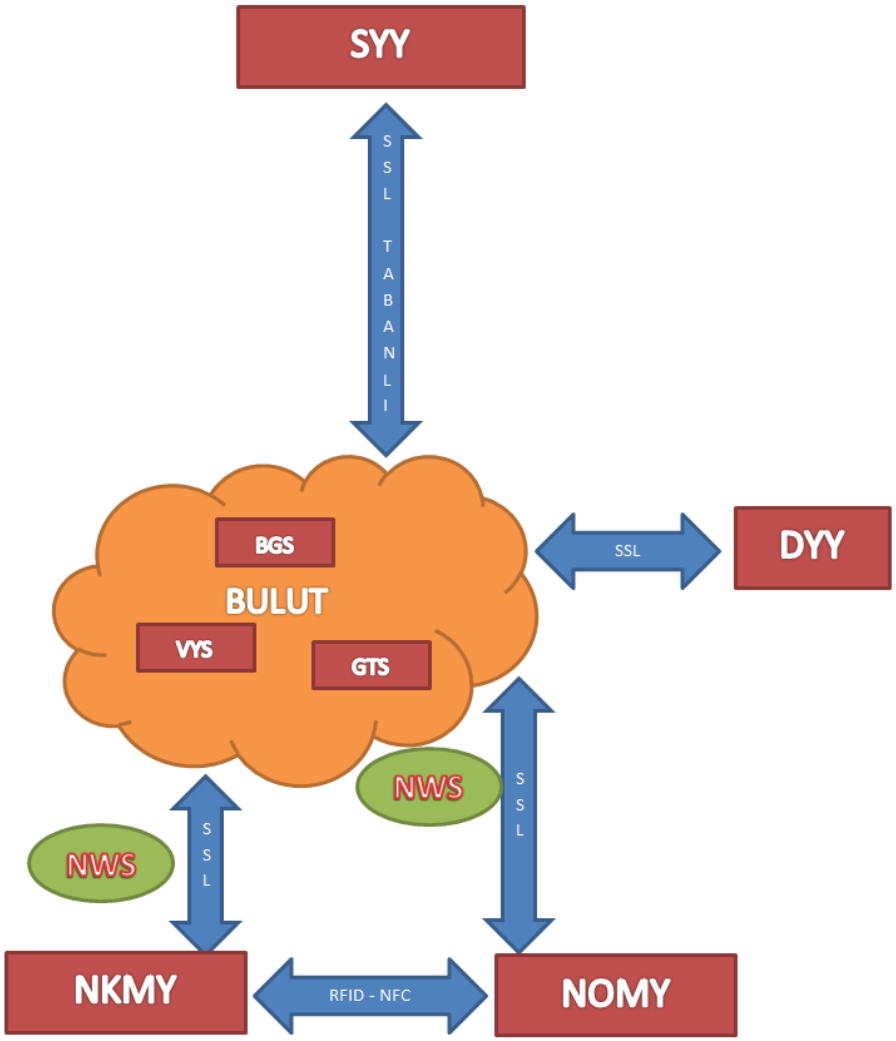
Aidat tahsilatlarında elden yapılan tahsilatlar hala devam etmekle birlikte; online ödeme, kredi kartı ile ödeme, web üzerinden ödeme gibi seçenekler de günümüzde aktif olarak kullanılmaktadır. Geliştirmiş olduğumuz bu sistem bahsi geçen yöntemlerin tamamını içermekle birlikte ayrıca tezimizin ana temasını oluşturan NFC teknolojisi ile ödeme seçeneğini de içermektedir. NFC teknolojisi ile güvenli alışveriş çalışmamız, bu sistem üzerinde uygulanmıştır. Tezimizin bulgular kısmında yapılan performans ölçümleri bu sistem üzerinde denenmiştir. Aidat tahsilat seçeneklerine eklediğimiz bu yeni seçenek sayesinde site sakinleri, yöneticilerden bağımsız olarak cep telefonlarını ödeme noktasına bir defa yaklaştırmak sureti ile saniyeler içinde kredi kartı üzerinden ya da sanal para bakiyesi üzerinden rahatlıkla aidat ödemesini yapabilmektedir.

Tezimizin diğer kısımlarında NFC teknolojisi ile ilgili kısımlar detaylıca anlatılmıştır bu kısımda ise sistemin tamamı modülleri ile birlikte anlatılacaktır. Geliştirmiş olduğumuz sistemde önemli bir seçenek olarak sunulan NFC altyapısındaki güvenli ödeme yapısı ile birlikte bu yapının uygulanması için geliştirilmiş olan büyük sistemi de detaylıca incelemekte fayda var.

Geliştirmiş olduğumuz sistemin tamamını 8 uygulama halinde inceleyeceğiz:

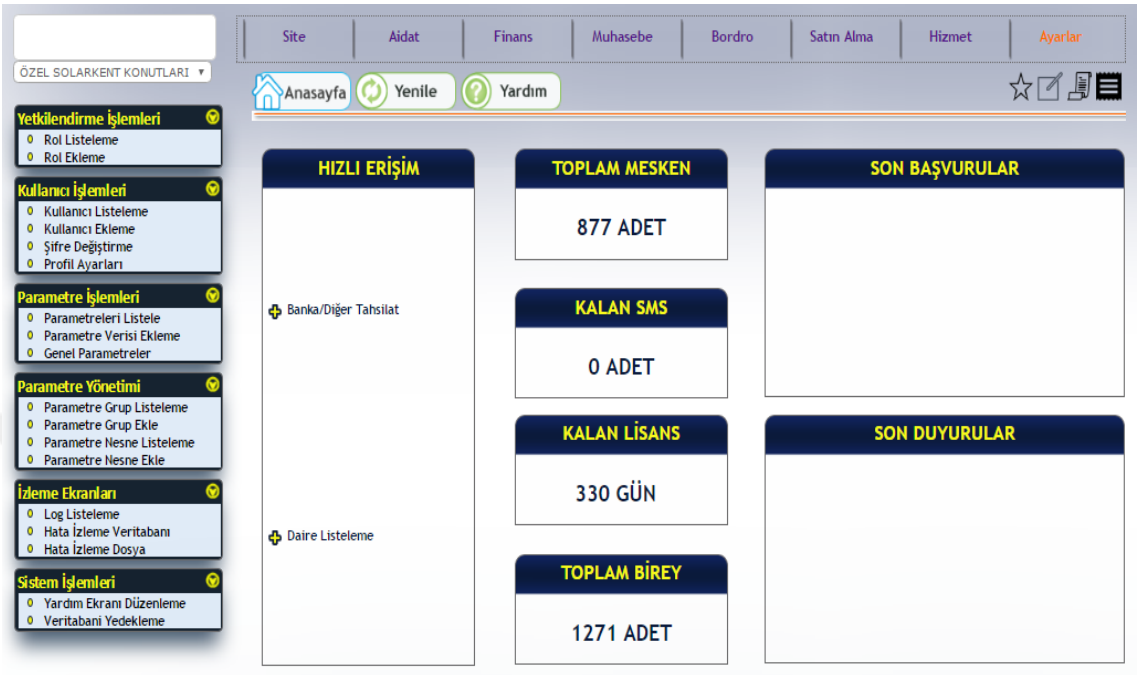
- SİTE YÖNETİM YAZILIMI (SYY)
- DAİRE YÖNETİM YAZILIMI (DYY)
- BİLDİRİM GÖNDERİM SERVİSİ (BGS)
- GECİKME TAZMİNATI SERVİSİ (GTS)
- VERİ YEDEKLEME SERVİSİ (VYS)
- NFC WEB SERVİSİ (NWS)
- NFC KULLANICI MOBİL YAZILIMI (NKMY)
- NFC ÖDEME NOKTASI MOBİL YAZILIMI (NOMY)

3.1.1. Genel Mimari



Şekil 3.1: Sistem Genel Mimarisi.

3.1.2. Site Yönetim Yazılımı (SYY)



Şekil 3.2: SYY Anasayfa.

3.1.2.1. SYY Genel Tanımı

Bu yazılımımız, sitenin yönetimi işini yapan yönetici ve personellere yöneliktir. Bir apartman sitesinin yönetiminde ihtiyaç olunan bütün temel modülleri içinde barındırmaktadır. NFC teknolojisini kullanarak ödeme yapmak isteyen kullanıcıların gerekli kayıt işlemleri de bu sistem üzerinden yapılmaktadır. NFC mobil uygulamasının ödeme ekranlarındaki veriler ve işlemler de bu sistem üzerinde yapılan işlemler ile ilgili olduğundan bu yazılımın incelenmesi çalışmamız açısından arıca bir öneme sahiptir.

3.1.2.2. SYY 'de Kullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı SYY yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak Asp.Net (c#) kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Kullanılan diğer teknolojiler; Html5, Css, Javascript, Jquery ve Ajax.Net
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.2.3. SYY 'e Ait Modüller

Şekil 3.3: SYY Modülleri.

SYY site yönetimlerinin bütün temel ihtiyaçlarını karşılamayı hedefleyen kapsamlı gelişmiş web tabanlı bir yazılımdır. SYY kendi için kullanıcılarının erişimini kolaylaştırmak için modüller bir yapıda geliştirilmiştir. Modüller de kendi içinde işlem gruplarına ayrılmıştır ve herbir grup da kendisi ile ilgili ekranları içinde barındırmaktadır. Biz SYY yazılımını incelerken ekran düzeyinde değil de grup düzeyinde inceleyeceğiz fakat NKMY ve NOMY ile ilgili olan ekranlar ayrıca incelenecektir.

SYY bütün işlemleri bazında yetkilendirme, yardım ekranları, işlem loglama, hata yönetimi ve hızlı erişimler gibi önemli özellikleri barındırmaktadır. SYY'nin modüllerini şöyle sıralayabiliriz;

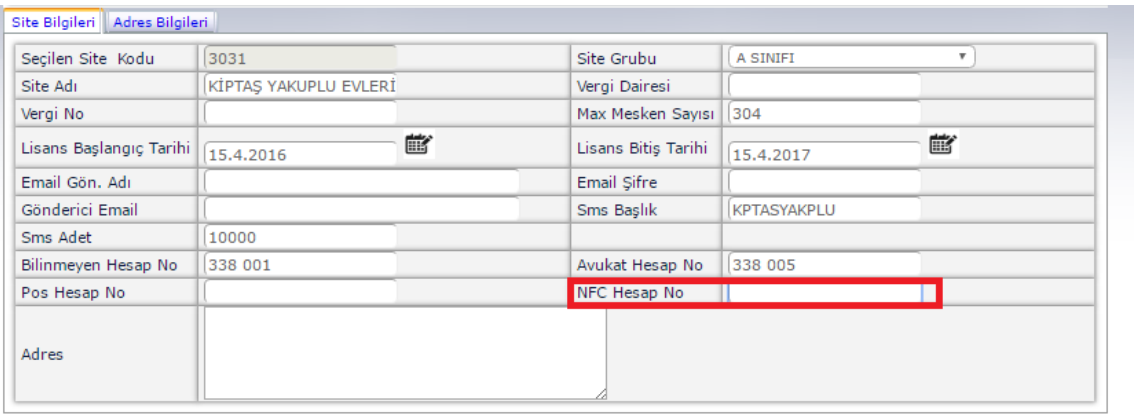
3.1.2.3.1. Daire İşlemleri

Sistemimize yeni apartman siteleri ekleyebildiğimiz ve sitelere özgü gerekli ayarlamaları yapabildiğimiz ekranları barındırır.

Şekil 3.4: SYY; Site Modülü.

3.1.2.3.1.1. Site İşlemleri

Bu gruptaki site detay ekranında NFC ile yapılan ödemelerde yapılacak muhasebe kaydının kullanacağı Muhasebe Hesap Numarası kaydedilir ve ödeme anında bu hesap numarası kullanılacaktır.



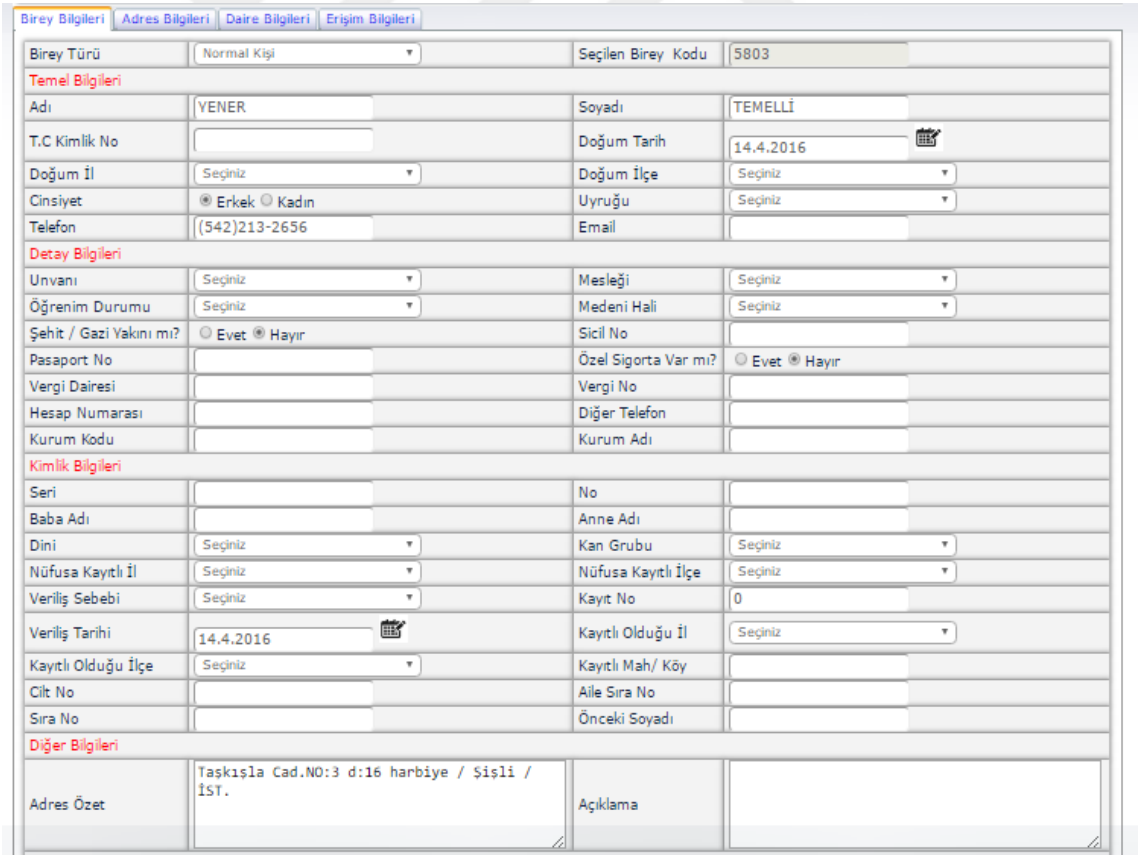
Şekil 3.5: SYY Site Bazlı NFC Ayarları.

3.1.2.3.1.2. Daire İşlemleri

Site içindeki dairelerin listelendiği ve düzenlendiği ekranları barındırır.

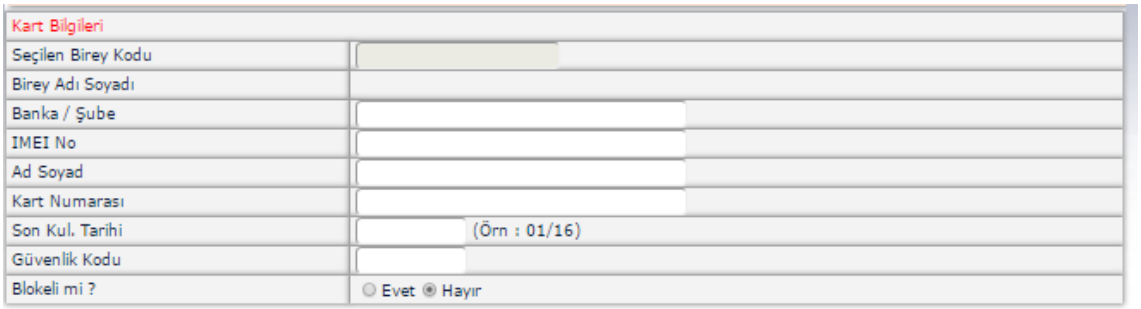
3.1.2.3.1.3. Birey İşlemleri

Birey işlemleri grubunda NFC kullanıcılarının eklenip düzenlendiği ekranlar bulunmaktadır. NFC mobil uygulamalarını kullanacak site sakinleri bu ekranlardan eklenir ve düzenlenir. Bu işlem grubundan ayrıca NFC ile ödeme yapabilmek için kullanıcının kredi kartı bilgileri de kaydedilir. Bilgiler MS Sql server veritabanında şifrelenmiş olarak saklanmaktadır.



Şekil 3.6: SYY Kullanıcı Ekleme Ekranı.

Kullanıcılarımızın ödeme işlemlerini gerçekleştirilmesi aşamasında NKMY tarafından kullanılmak üzere kart bilgilerinin girilmesi gerekmektedir.



Şekil 3.7: SYY Sanal Para Bilgileri Kayıt Ekranı.

Kullanıcıların DYY ve NKMY yazılımlarında işlem yapabilmeleri için kullanacakları erişim bilgilieri bu ekrandan düzenlenmektedir.

Şekil 3.8: Kullanıcı Şifre Düzenleme Ekranı.

3.1.2.3.1.4. Yönetim İşlemleri

Site Yönetiminin kadrosunun, yönetim kadrosunun ve personel bilgilerinin düzenlendiği ekranları barındırır.

3.1.2.3.2. Aidat Modülü

Aidat modülünde makbuz işlemleri, borçlandırma işlemleri, icra işlemleri, bakiye raporları ve daire mektupları şeklinde olmak üzere 5 farklı işlem grubu vardır. Kullanıcıların bakiye bilgilerinin raporlandığı ekranların barındırıldığı ve SYY üzerinden aidat tahsilatlarının yapıldığı ekranlar bulunmaktadır.

Şekil 3.9: Aidat Modülü Menüsü.

3.1.2.3.2.1. Makbuz İşlemleri

Aidat tahsilatlarının ve makbuzlarının eklendiği ekranları barındırmaktadır. NFC ile yapılan ödemelerin makbuzları da arka planda kaydedilmektedir ve bu ekranlardan görüntülenebilecektir.

TAHSİLAT MAKBUZU

Tarih : 24.05.2016
Fiş No : 1038
Makbuz No : 3795

Ada : STANDART
Blok : A05
Daire : 23
Ad Soyad : GONCA
Ödeme Şekli : NFC İle Ödeme
Tutar : 115,00 ₺ (YÜZONBEŞ TL SIFIR KURUŞ)
Açıklama : 2016 MAYIS AYI AİDATI / KALAN BORÇ = -0.99 TL

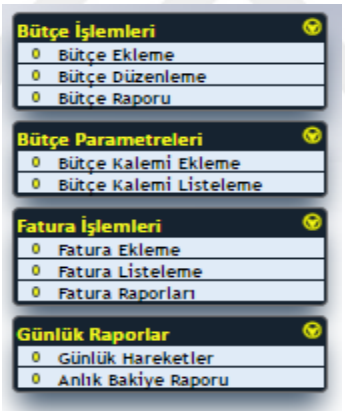
Oluşturan :

Site Kopyası: 405574892

Şekil 3.10: Örnek Makbuz.

3.1.2.3.3. Finans Modülü

SYY yazılımının, bütçe işlemleri, bütçe parametreleri, fatura işlemleri ve günlük raporlar işlem gruplarının bulunduğu modüldür.



Şekil 3.11: Finans Modülü Menüsü.

3.1.2.3.4. Muhasebe Modülü

Muhasebe işlemleri ve muhasebe raporlarının bulunduğu modüldür. Bütün yazılımlarda yapılmış olan muhasebe tabanlı işlemlerin sonuçlarının görüntülenebileceği ekranlar bulunmaktadır.

Şekil 3.12: Muhasebe Modülü Menüsü.

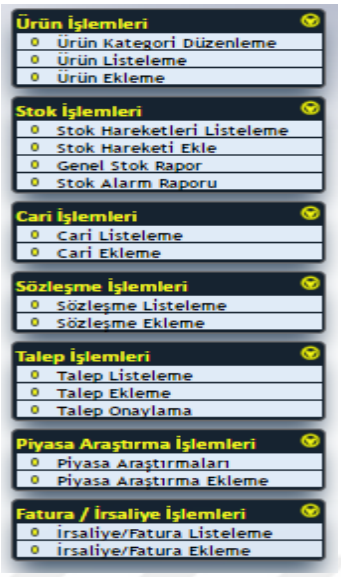
3.1.2.3.5. Bordro Modülü

Bordro modülünde; birey olarak kaydedilmiş personellerin hakkediş gibi aylık maaşlarını etkileyecek bilgilerin düzenlendiği ekranlar ve aylık olarak maaşların hesaplandığı , bordroların alındığı ekranlar bulunmaktadır.

Şekil 3.13: Bordro Modülü Menüsü.

3.1.2.3.6. Satın Alma Modülü

Site yönetimlerinin ihtiyaçları olan Ürün ,Stok, Cari, Talep, Sözleşme, Fatura ve İrsaliye işlemlerini yapabilecekleri ekranları barındıracaktır.



Şekil 3.14: Satın Alma Modülü Menüsü.

3.1.2.3.7. Hizmet Modülü

Site yönetimlerinin tebliğat işlemlerine, toplantı kararlarına, genel duyurulara içerik yönetimi, sabit içerikler ve başvuru işlemleri gibi hizmet adımlarını yönetebilecekleri ekranları barındırmaktadır.

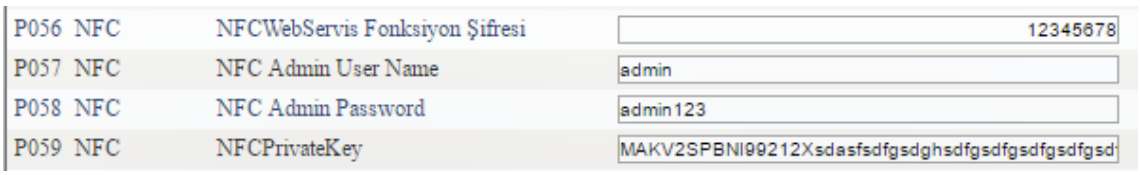
Şekil 3.15: Hizmet Modülü Menüsü.

3.1.2.3.8. Ayarlar Modülü

SYY yazılımının bütün ekranlarında kullanılmak üzere sistem ayarlarının yapıldığı, yetkilendirmelerin yapıldığı ve genel olarak ;Rol, Kullanıcı, Parametre, Sistem ve Loglama gibi işlemlerin yapılmış olduğu ekranlardır.

Şekil 3.16: Ayarlar Modülü Menüsü.

NFC ayarları ile birlikte bütün sistem ayarlarının yapıldığı ekranları barındırır.



Şekil 3.17: NFC Ayarları.

3.1.3. Daire Yönetim Yazılımı (DYY)

Genel mimarimizde bulunmakta olan DYY, çalışmamız içinde çok detaylıca anlatılmamak ile birlikte sistem içindeki yeri itibari ile kısaca bahsedilmektedir.

Şekil 3.18: DYY Ana Sayfa.

3.1.3.1. DYY Genel Tanımı

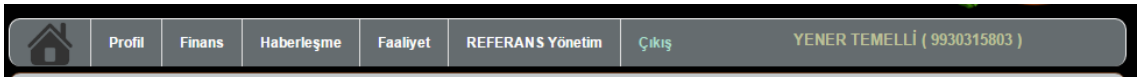
Bu yazılımımız, site sakinlerinin NFC ya da farklı ödeme türleri ile yaptıkları ödemelerin takibini ve raporlarını alınabilmelerini sağlar. DYY yazılımı ile site sakinleri Kredi Kartı bilgilerini girerek online ödeme yapabilirler.

3.1.3.2. DYY 'de Kullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı DYY yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak Asp.Net (c#) kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Kullanılan diğer teknolojiler; Html5, Css, Javascript, Jquery ve Ajax.Net
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.3.3. DYY 'e Ait Modüller



Şekil 3.19: DYY Modülleri.

DYY site sakinlerinin bütün temel ihtiyaçlarını karşılamayı hedefleyen kapsamlı gelişmiş web tabanlı bir yazılımdır. DYY kendi için kullanıcılarının erişimini kolaylaştırmak için modüller bir yapıda geliştirilmiştir. Modüller de kendi içinde ilgili ekranları barındırmaktadır. Biz DYY yazılımını incelerken ekran düzeyinde değil de genel bir bakış açısı ile fakat NKMY ve NOMY ile ilgili olan ekranlar ayrıca incelenecektir.

DYY bütün işlemleri bazında yetkilendirme, yardım ekranları, işlem loglama, hata yönetimi ve hızlı erişimler gibi önemli özellikleri barındırmaktadır. DYY'nin modüllerini şöyle sıralayabiliriz;

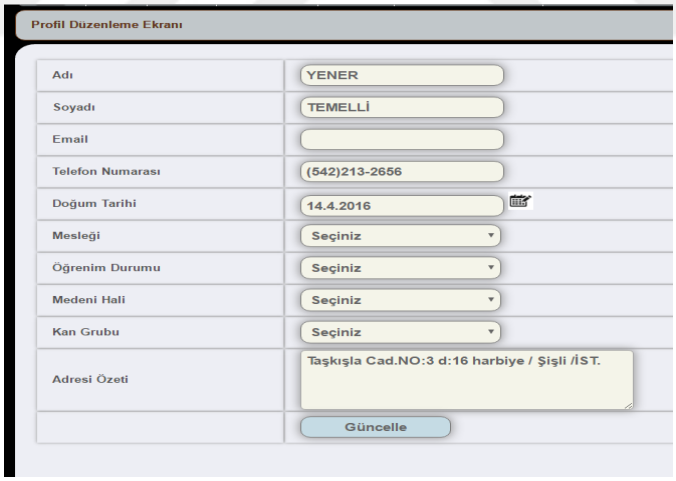
Bu uygulamada kullanıcı adı ve şifre bilgileri NFC için de kullanılmaktadır.

3.1.3.3.1. Profil Modülü

Kullanıcıların, üyelik bilgilerini güncelleyebildiği, şifrelerini değiştirebildiği ve daire portföylerini inceleyebildikleri ekranların olduğu modüldür.

3.1.3.3.1.1. Profil Düzenle

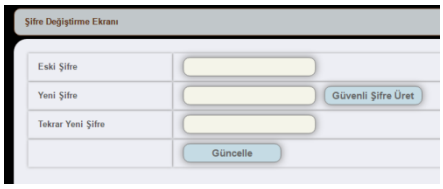
NFC Kullanıcılarının bilgilerini güncelleyebildiği ekrandır.



Şekil 3.20: DYY Profil Düzenleme.

3.1.3.3.1.2. Şifre Değiştir

NFC Uygulamamızda kullanılan şifre bilgisini kullanıcılar istedikleri takdirde bu ekran üzerinden değiştirebilirler.



Şekil 3.21: DYY Şifre Düzenleme.

3.1.3.3.2. Finans Modülü

Kullanıcıların DYY' ye giriş yaptıktan sonra kredi kartı ile borç ödeme, borç durumlarını görüntüleme, hesap hareketleri ve makbuzlarını görüntüleme gibi işlemlerin yapılabileceği modüldür.

3.1.3.3.3. Haberleşme Modülü

Kullanıcıların, başvurularını takip edebildikleri ve yeni başvurular ekleyebildiği ekranları barındırmaktadır. Bildirimlerin ve duyuruların da takip edilip görüntülendiği ekranlar barındırmaktadır.

3.1.3.3.4. Faliyet Modülü

Kullanıcıların yöneticilerin yapmış oldukları toplantıları, bütçe raporları ve bütçe mektuplarını inceleyebilecekleri ekranları barındırmaktadır.

3.1.3.3.5. Tanıtım Modülü

Kullanıcıların sistemi tanımaları için; Hakkımızda, İletişim, Sistem Hakkında, Kullanım Koşulları, Yardım ve Çıkış gibi erişimleri içeren modüldür.

3.1.4. Bildirim Gönderim Servisi (BGS)

3.1.4.1. BGS Genel Tanımı

Bu yazılımımız, Site sakinlerine iletilmek istenen Email ve Sms bildirimlerini belli bir periyot ile göndermek amacı ile geliştirilmiştir.

3.1.4.2. BGS 'deKullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı BGS yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak C# kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.5. Gecikme Tazminatı Servisi (GTS)

3.1.5.1. GTS Genel Tanımı

Bu yazılımımız, site sakinlerinin borçlarına günlük olarak gecikme tazminatı uygulayıp gerekli muhasebe kayıtlarının yapılmasını sağlar.

3.1.5.2. GTS 'deKullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı GTS yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak C# kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.6. Veri Yedekleme Servisi (VYS)

3.1.6.1. VYS Genel Tanımı

Bu yazılımımız, bulut ortamı olarak tarif edilen bütün veri havuzunu belirlediğimiz periyotlar ile yedekleme işlemini yapar.

3.1.6.2. VYS 'deKullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı VYS yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak C# kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.7. NFC Web Servis (NWS)

3.1.7.1. NWS Genel Tanımı

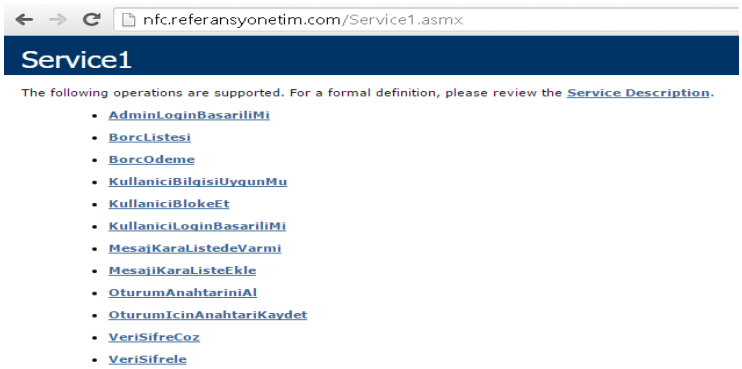
Bu web servisimiz bulut ortamı ile NKMY / NOMY yazılımlarının SSL alt yapısında haberleşmesini sağlayan ve içinde birçok fonksiyon barındıran uygulamadır. Bu web servisimizin bütün fonksiyonları çalıştırılmak için bir şifre bilgisi ister bu şifre bulgusu bulut ortamında saklanmaktadır ve SYY üzerinden kolaylıkla değiştirilebilmektedir.

3.1.7.2. NWS 'de Kullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı NWS yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak C# kullanılmıştır.
- Geliştirilme ortamı olarak Visual Studio 2015
- .Net Framework versiyonu olarak 4.5 kullanılmıştır.
- Veritabanı olarak Microsoft Sql Server 2014
- Nesneye dayalı programlama
- Entity Framework yapısında Data Access Layer (DAL)

3.1.7.3. NWS Fonksiyonları



Şekil 3.22: NWS Genele Görünüm.

3.1.7.3.1. AdminLoginBasarilimi

NKMY' yi android telefonuna kuran site sakini, site yönetimine gelir ve NKMY yazılımını aktifleştirmesini talep eder. Site yönetimindeki yetkili personel mobil uygulamada "Kullanıcı Kaydet" ekranını kullanmak üzere yönetici kullanıcı adı ve şifresini girerek işlem yapar. Girdiği şifrenin başarılı olup olmadığını kontrol etmek üzere NKMY yazılımı tarafından bu fonksiyon kullanılır. Yöneticinin şifre ve kullanıcı adı bilgisi bulut ortamında saklanmakta olup SYY ile üzerinden gerektiğinde değiştirilebilir.

Bu fonksiyon kullanıcı adı, Şifre ve Fonksiyon Şifresi bilgilerinin girilmesini gerektirir sonuç olarak da "OK" ya da "ERROR" bilgisi dönüşü yapar. Fonksiyon şifresi ise yine bulut ortamında saklanıp SYY üzerinden değiştirilebilir.

AdminLoginBasariliMi

Test

The test form is only available for requests from the local machine.

SOAP 1.1

The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual values.

```
POST /Service1.asmx HTTP/1.1
Host: nfc.referansyonetim.com
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://nfc.referansyonetim.com/AdminLoginBasariliMi"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AdminLoginBasariliMi xmlns="http://nfc.referansyonetim.com/">
      <adminName>string</adminName>
      <adminPass>string</adminPass>
      <funcPass>string</funcPass>
    </AdminLoginBasariliMi>
  </soap:Body>
</soap:Envelope>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <AdminLoginBasariliMiResponse xmlns="http://nfc.referansyonetim.com/">
      <AdminLoginBasariliMiResult>string</AdminLoginBasariliMiResult>
    </AdminLoginBasariliMiResponse>
  </soap:Body>
</soap:Envelope>
```

Şekil 3.23: NWS Fonksiyon Görüntüsü.

3.1.7.3.2. BorcListesi

Bu fonksiyon NKMY tarafından kullanılmaktadır. Kendisine şifrelenmiş olarak gönderilen Kullanıcı Kodu ve Fonksiyon Şifresi bilgilerini alarak sonuç olarak NKMY ekranında görüntülenmek üzere ilgili kullanıcının daire ve borç türü bazında tüm borçlarının olduğu listeyi kendisine göndermektedir.

3.1.7.3.3. BorcOdeme

Bu fonksiyon NKMY tarafından kullanılmaktadır. NKMY BorcListesi fonksiyonundan gelen veri listesini telefon kullanıcısına ilgili ekranda sunar ve her bir borcun yanında bir "Öde" butonu yer alır. Kullanıcı bunlardan herhangi birine basarsa seçtiği borcun bilgilerini bu fonksiyon vasıtası ile bulut ortamına iletir ve Başarılı/Başarısız şeklinde dönüş yapılır.

3.1.7.3.4. KullaniciBilgisiUygunMu

Bu fonksiyon NMOY tarafından kullanılır. NOMY, NFC ortamından NKMY tarafından gönderilen Kullanıcı Kodu bilgisinin sistemimizin standartlarına uygun olup olmadığını, bulut ortamında böyle bir kullanıcı olup olmadığını ve bu kullanıcının bloke edilmemiş bir kullanıcı olup olmadığını kontrol etmek üzere "Kullanıcı Kodu" bilgisini bu fonksiyona gönderir Olumlu/Olumsuz şeklinde bir geri dönüş alarak algoritmanın ilerleyişine yön verir.

3.1.7.3.5. KullaniciBlokeEt

Bu fonksiyon NKMY tarafından kullanılır. Ödeme işlemi devam ederken en son ödeme ekranına geçebilmek için NKMY kullanıcısından bulut ortamında saklı olan ve SYY ya da DYY üzerinden değiştirilebilen şifre bilgisini girmesi istenir. Bu bilginin 5 defa yanlış girilmesi durumunda ilgili NKMY kullanıcısı bu fonksiyon vasıtası ile bulut ortamında blokeli olarak işaretlenir ve SYY üzerinden tekrar yetki verilene kadar da

işlem yapması KullaniciBilgisiUygunMu fonksiyonundan gelen veri doğrultusunda engellenmiş olur.

3.1.7.3.6. KullaniciLoginBasariliMi

Bu fonksiyon NKMY tarafından kullanılır. Ödeme işlemi devam ederken en son ödeme ekranına geçebilmek için NKMY kullanıcısından bulut ortamında saklı olan ve SYY ya da DYY üzerinden değiştirilebilen şifre bilgisini girmesi istenir. Bu şifre bilgisi cihazda kayıtlı "Kullanıcı Kodu" ile birlikte bu fonksiyona iletilir ve bu fonksiyondan Onay/Red şeklinde bir sonuç beklenir bu sonuca göre NKMY geri kalan sürecini işletir.

3.1.7.3.7. MesajKaraListedeVarMi

Bu fonksiyon NOMY tarafından kullanılır. NOMY kendisine NKMY tarafından NFC ortamından iletilmiş olan NDEF mesajlarının bulut üzerindeki Mesaj Kara Listesinde olup olmadığını kontrol eder ve buradan gelecek cevaba göre sürecin işletilmesi devam eder.

3.1.7.3.8. MesajiKaraListeEkle

Bu fonksiyon NOMY tarafından kullanılır. NOMY tekrarlı mesajları ya da işaretli mesajları bu fonksiyon vasıtası ile bulut ortamına kaydeder.

3.1.7.3.9. OturumAnahtariniAl

Bu fonksiyon NKMY ve NOMY tarafından kullanılır. NFC ortamından alınan NDEF mesajından "Oturum Id" bilgisi kısmı alınır ve bu fonksiyon vasıtası ile bulut ortamından ilgili "Oturum Id" bilgisine bağlı anahtar bilgisi alınır ve NDEF içindeki şifreli mesaj bu anahtar vasıtası ile Asimetrik Şifreleme Yönteminde özünde çevrilmek sureti ile kullanılır.

3.1.7.3.10. OturumAnahtarKaydet

Bu fonksiyon NKMY ve NOMY tarafından kullanılır. NFC ortamından herhangi bir veri göndermek isteyen cihaz öncelikle veriyi o an rastgele bir anahtar üreterek bu anahtar ile Asimetrik Şifreleme metodunu kullanarak şifreler. Şifrelenmiş veri NFC ortamına bırakılmadan önce bu anahtarda bulut ortamına bir "Oturum ID" bilgisi alınarak bu fonksiyon vasıtası ile kaydedilir. Bu alınan "Oturum Id" bilgisi ve Şifreli mesaj NFC ortamına bırakılır.

3.1.7.3.11. VeriSifreCoz

Bu fonksiyon NKMY ve NOMY tarafından kullanılır. Sistemde kullanılan ve anahtar bilgisi bulut ortamında saklanan tek taraflı Simetrik Şifreleme yöntemi ile yapılan tüm işlem adımlarında Şifreli Verilerin çözülmesi aşamasında kullanılmaktadır.

3.1.7.3.12. VeriSifrele

Bu fonksiyon NKMY ve NOMY tarafından kullanılır. Sistemde kullanılan ve anahtar bilgisi bulut ortamında saklanan tek taraflı Simetrik Şifreleme yöntemi ile yapılan tüm işlem adımlarında Şifresiz Verilerin şifrelenmesi aşamasında kullanılmaktadır.

3.1.8. NFC Kullanıcı Mobil Yazılımı (NKMY)

3.1.8.1. NKMY Genel Tanımı

Bu yazılımımız, Site sakinlerine yönelik android alt yapısında geliştirilmiş bir mobil uygulamadır. Site sakinlerinin ödeme noktasına telefonlarını dokundurup ödeme yapabilmesi için gerekli alt yapıyı ve ara yüzü sunmaktadır.

3.1.8.2. NKMY 'deKullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı NKMY yazılımımızın önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak Java kullanılmıştır.
- İşletim Sistemi olarak Android 4.3 (Jelly Bean)
- Donanım olarak Samsung Galaxy Note 3
- Geliştirilme ortamı olarak Android Studio 1.5.1.
- Nesneye Dayalı Programlama
- SQLite

3.1.8.3. NKMY Ekranları ve İşlevleri

3.1.8.3.1. Karşılama Ekranı

Şekil 3.24: NKMY Ana Sayfa.

Site sakini android telefonunda kurulu olan NKMY'yi başlattığında karşısına ilk çıkacak ekrandır. Şekilde de görüldüğü üzere "Ödeme İşlemine Başla" ve "Yönetici Girişi" şeklinde 2 seçenek sunulmaktadır.

Kullanıcı "Ödeme İşlemine Başla" seçeneğini seçtiği takdirde uygulama NOMY ile NFC haberleşmesi başlar ve NKMY yazma moduna geçmek üzere "Ödeme Başlangıç Ekranına"'ına yönlendirilir.

"Yönetici Giriş" butonu ise sadece site yöneticilerinin kullanacağı bir seçenektir. NKMY telefona ilk kurulduğunda yöneticiler bu seçeneği kullanarak bulut sistemindeki ilgili kişinin "Kullanıcı Kodu" bilgisini bu telefona kaydetmesi gerekmektedir. Bu butona basıldığında "Yönetici Kullanıcı Adı" ve "Yönetici Şifre" bilgilerini girmek üzere "Yönetici Giriş Ekranı"'na yönlendirilir.

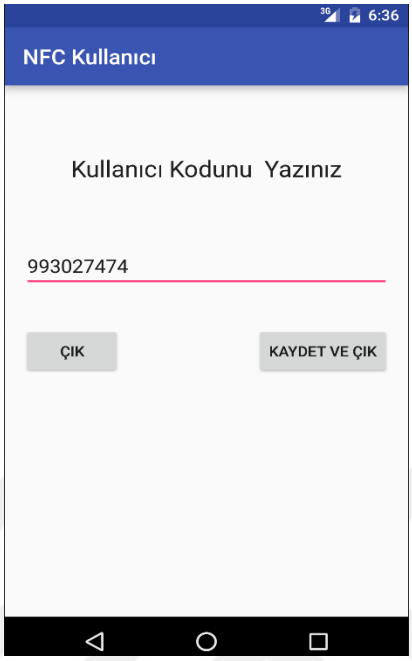
3.1.8.3.2. Yönetici Giriş Ekranı

Şekil 3.25: NKMY Yönetici Girşi.

Bu ekranda site yöneticileri bulut ortamında kayıtlı olan giriş bilgilerini kullanarak onay almak suretiyle "Kullanıcı Kayıt" ekranına geçecektir aksi takdirde kullanıcı kayıt işlemi yapamayacaklardır. Web servis vasıtası ile bulut ortamından yapılacak yetki kontrolünün haberleşmesi SSL güvencesinde olduğundan sistemimiz için bir açık olarak düşünülemez.

Yönetici başarılı bir şekilde login olduğu takdirde "Kullanıcı Kayıt Ekranı"'na yönlendirilecektir. Login bilgileri SYY üzerinden değiştirilebilir.

3.1.8.3.3. Kullanıcı Kayıt Ekranı



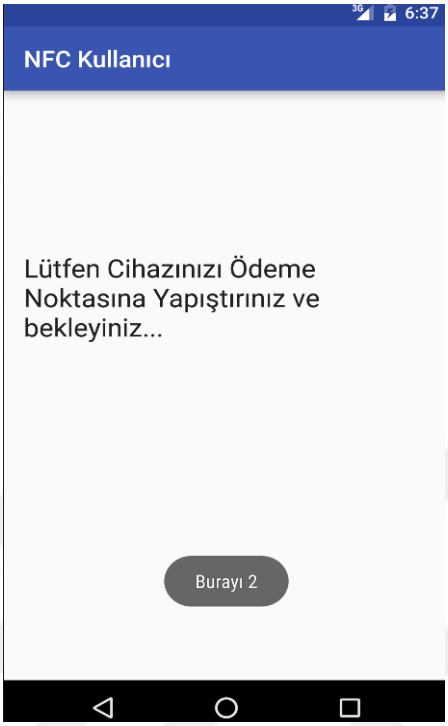
Şekil 3.26: NKMY Kullanıcı Kayıt.

Bu ekran ilk açılışta android altyapısında bulunan Sqlite veritabanına erişerek anahtar bilgisi bulut ortamında bulunmak suretiyle AES şifreleme tekniği ile şifrelenmiş olarak kaydedilmiş "Kullanıcı Kodu" bilgisi var ise o bilgiyi alır ve şifresini yine aynı teknik ile çözerek metin kutusunun içine yazar. Daha önceden kaydedilmiş bir bilgi yok ise metin kutusu boş gelir.

Yönetici eski bilgiyi değiştirmek ya da yeni bilgiyi eklemek için metin kutusuna kullanıcı kodunu yazar ve "Kaydet ve Çık" butonuna basar. Böylelikle metin kutusundaki bilgi yukarıda bahsedilen teknikler ile şifrelenerek diğer ekranlarda kullanılmak üzere Sqlite veritabanına kaydedilir.

Bu ekrandaki bilgilerin şifrelenmiş olarak saklanması güvenlik açısından çok önem arz etmektedir. Sistemimiz kopyalandığında ya da Sqlite içeriği ele geçirildiğinde içindeki verinin şifreli olması önemlidir.

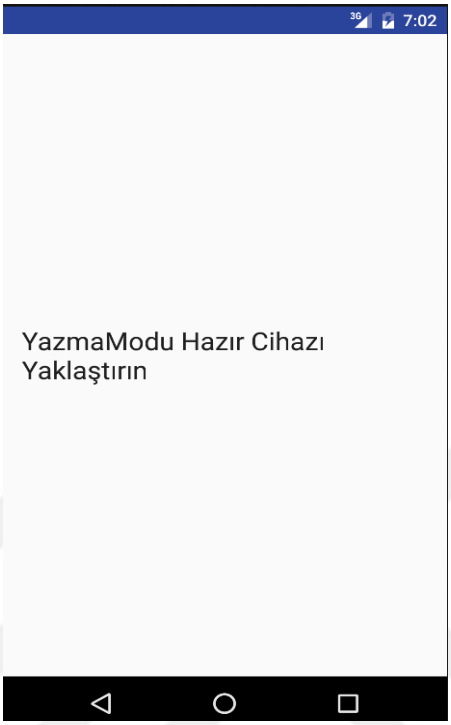
3.1.8.3.4. Ödeme Başlangıç Ekranı



Şekil 3.27: NKMY Bekleme Ekranı.

Bu ekranımız Sqlite üzerinde kayıtlı bir kullanıcı olup olmadığını kontrol eder ve bu bilginin geçerli bir bilgi olup olmadığına bakılır. Bu aşamada bir sorun olduğu takdirde tekrar bekleme ekranına geçilerek kullanıcıya gerekli uyarı mesajı verilir. Eğer her şey yolunda ise "NFC Yazma" Ekranına yönlendirilir. Yazma işlemine başlamadan önce gerekli kontrollerin yapıldığı bir geçiş ekranıdır ve herhangi bir kullanıcı müdahalesi gerektirmeksizin kendiliğinden yönlendirmeleri yapmaktadır.

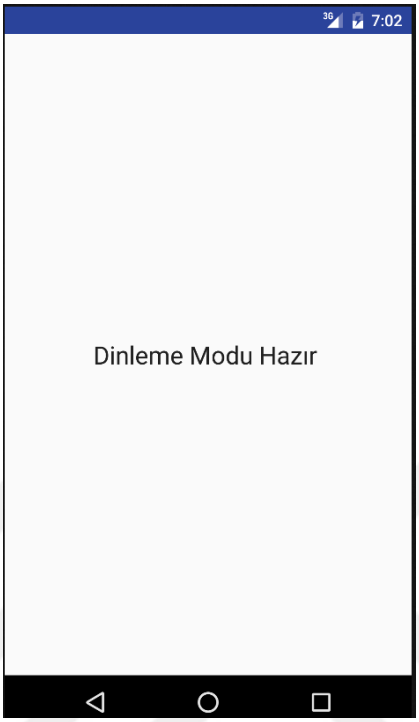
3.1.8.3.5. NFC Yazma Ekranı



Şekil 3.28: NKMY Yazma Modu.

Bu ekrana NKMY üzerinde kullanıcı bilgileri kaydedilmiş kişiler sadece erişebilir. Kullanıcı NOMY' nin kurulu olduğu stand cihazına telefonunu yakınlaştırır ve haberleşme işlemi başlamış olur. Öncelikle NKMY anlık olarak rastgele bir anahtar oluşturur ve bu anahtarı NWS vasıtası ile bulut ortamına göndererek bir oturum kodu bilgisi alır. Kullanıcı kodu bilgisini oluşturduğu anahtar ile birlikte AES 128 şifreleme tekniği ile şifreleyerek bulut ortamından aldığı oturum kodunu NDEF mesajına dönüştürüp NFC ortamına bırakır. NFC ortamına yazma işlemi tamamlandıktan sonra NKMY otomatikman "NFC Dinleme Ekranı"' na yönlendirilir ve bundan sonra NOMY yazılımından gelecek olan cevap beklenir.

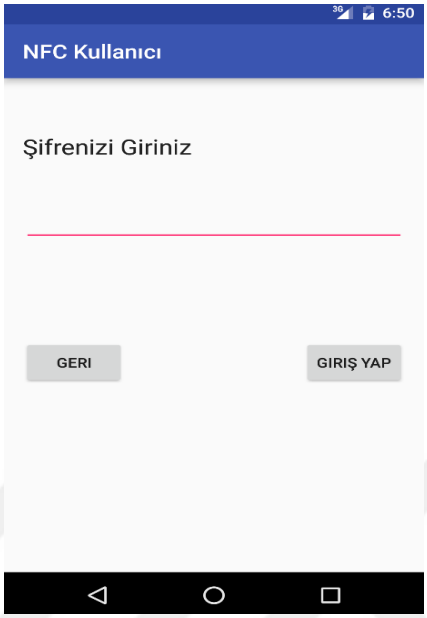
3.1.8.3.6. NFC Dinleme Ekranı



Şekil 3.29: NKMY Dinleme Modu.

NFC ortamına yazma işlemi tamamlandıktan sonra bu ekrana geçildiğini söylemiştik. NOMY yazılımının NFC ortamına bıraktığı NDEF mesajı bu ekran vasıtası ile dinlenerek alınır. NDEF mesajında bulunan oturum kodu bilgisi SSL alt yapısında çalışan NWS vasıtası ile bulut ortamına gönderilerek NOMY'nin anlık ve rastgele oluşturup kaydetmiş olduğu anahtar bilgisi alınır ve NDEF mesajının içindeki AES 128 ile şifrelenmiş geri dönüş bilgisinin şifresi çözülür. NOMY tarafından geri dönüş olarak olumsuz bir dönüş yapılmış ise "Karşılama Ekranına" yönlendirilir, olumlu bir dönüş yapılmış ise de kullanıcının sistem üzerinde onaylı olduğuna karar verilerek "Şifre Giriş Ekranına" yönlendirlir.

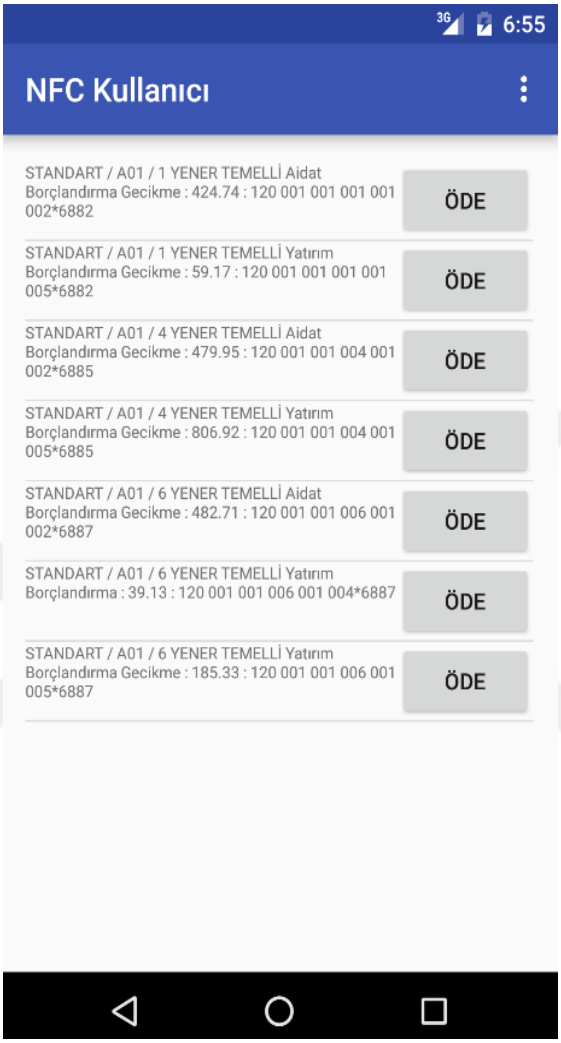
3.1.8.3.7. Şifre Giriş Ekranı



Şekil 3.30: NKMY Onay Ekranı (Şifre Girişi).

Bu ekran bulut üzerinde onaylanmış ve NOMY tarafından yetkilendirilmiş kullanıcıları erişebileceği ekrandır. Bu ekran üzerinde kullanıcı sadece kendisinin bildiği SYY, DYY ve NKMY sistemlerinde ortak olarak kullanabildiği şifresini girer ve borç listesi ekranına geçiş yapar aksi takdirde "Karşılama Ekranına" yönlendirilir. Kullanıcı bu ekranda 5 defa hatalı şifre girerse sistem tarafından bloke edilir ve bloke kaldırılana kadar bu ekrana tekrar erişemez.

3.1.8.3.8. Borç Listeleme ve Ödeme Ekranı



Şekil 3.31: NKMY Borç Listeleme.

Bu ekran şifresini başarılı olarak girebilen kullanıcıların erişebileceği ekrandır. Kullanıcının site yönetimine olan tüm borçları daire ve hesap türüne göre sıralanır ve istediği borcun yanındaki "ÖDE" butonuna basarak o borcun ödemesini SSL tabanlı NWS vasıtası ile Kredi Kartı veya Sanal Para vasıtası ile yaparak bulut ortamına gerçek zamanlı olarak kaydetmiş olur. Bu işlemin sonucunda olumsuz veya olumlu olarak gelen geri dönüşe göre uygun uyarı verilir ve "Karşılama Ekranına" tekrar geçilir. Böylelikle işlem tamamlanmış olur.

3.1.9. NFC Ödeme Noktası Mobil Yazılımı (NOMY)

3.1.9.1. NOMY Genel Tanımı

Bu yazılımımız, NKMY yazılımı ile birlikte çalışmak üzere geliştirilmiş site yönetimlerinin site girişlerinde android tabanlı bir telefonda kurulu olmak suretiyle stant vasıtası ile sabitlenmesi öngörülmüş mobil bir uygulamadır. Site sakinlerinin ödeme işlemi için kullanacağı bilgilerini NFC ortamından alıp bulut üzerinden gerekli kontrolleri yaparak istemciye izin veren ya da işlemini sonlandıran yazılımdır.

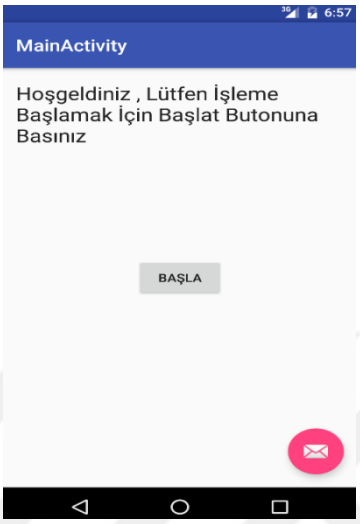
3.1.9.2. NOMY 'de Kullanılan Teknolojiler

Birçok teknolojinin bir arada kullanıldığı NOMY 'nin önemli olan bazı teknolojileri aşağıda listelenmiştir.

- Programlama dili olarak Java kullanılmıştır.
- İşletim Sistemi olarak Android 4.3 (Jelly Bean)
- Donanım olarak Samsung Galaxy Note 3
- Geliştirilme ortamı olarak Android Studio 1.5.1.
- Nesneye Dayalı Programlama

3.1.9.3. NOMY Ekranları ve İşlevleri

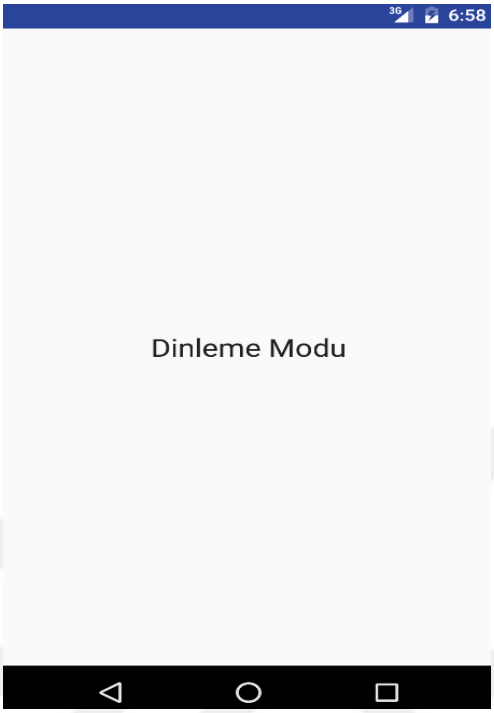
3.1.9.3.1. Bekleme Ekranı



Şekil 3.32: NOMY Bekleme Ekranı.

Bu ekran standımızın gereksiz yere dinleme ya da yazma modunda beklemesini önlemek amacıyla bekleme ekranı olarak geliştirilmiştir. İşleme başlamak isteyen kullanıcı Başla butonuna basarak NOMY' yi dinleme moduna geçirmiş olur. Bulgular kısmında detaylıca belirtilecektir fakat sistemi kilitlemeyi hedefleyen saldırıların da önüne geçilmiş olmaktadır çünkü NOMY başla butonuna basıldıktan belli bir süre sonra tekrar bu ekrana yönlendirmektedir.

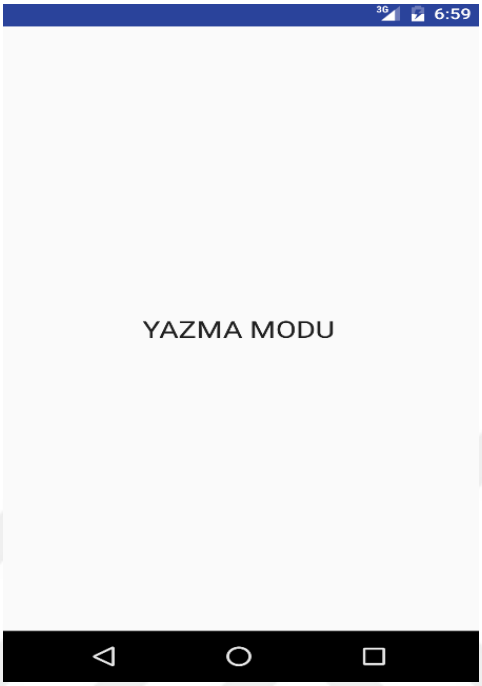
3.1.9.3.2. Nfc Okuma Ekranı



Şekil 3.33: NOMY Dinleme Modu.

NKMY yazılımının NFC ortamına bıraktığı NDEF mesajı bu ekran vasıtası ile dinlenerek alınır. NDEF mesajında bulunan oturum kodu bilgisi SSL alt yapısında çalışan NWS vasıtası ile bulut ortamına gönderilerek NKMY'nin anlık ve rastgele oluşturup kaydetmiş olduğu anahtar bilgisi alınır ve NDEF mesajının içindeki AES 128 ile şifrelenmiş geri dönüş bilgisinin şifresi çözülür. NWS vasıtası ile talepte bulunan kullanıcının blokeli olup olmadığı sanal para ve kredi kartı gibi bilgileri kontrol edildikten sonra NKMY' ye ulaştırmak üzerine NFC ortamına olumlu ya da olumsuz bir bilgi yazmak üzere "NFC Yazma Ekranı"' na yönlendirilir.

3.1.9.3.3. Nfc Yazma Ekranı



Şekil 3.34: NOMY Yazma Modu.

Öncelikle NOMY anlık olarak rastgele bir anahtar oluşturur ve bu anahtarı NWS vasıtası ile bulut ortamına göndererek bir oturum kodu bilgisi alır. Olumlu ya da Olumsuz geri dönüş bilgisini oluşturduğu anahtar ile birlikte AES 128 şifreleme tekniği ile şifreleyerek bulut ortamından aldığı oturum kodunu NDEF mesajına dönüştürüp NFC ortamına bırakır. NFC ortamına yazma işlemi tamamlandıktan sonra NOMY otomatikman "Bekleme Ekranı"' na yönlendirilir ve bundan sonra yeni bir işleme başlamayı beklemek üzere işlemi tamamlar.

3.2. ÇALIŞMA YÖNTEMLERİ

3.2.1. Kullanıcı Kayıt

Site yönetimleri öncelikle SYY üzerinden tüm site sakinlerini bulut ortamına kaydederler. Bireyler sisteme kaydedildikten sonra daireler ile gerekli ilişkiler kurulur. Bireylerin detay ekranında şifre bilgileri girilir ve yetkilendirilmesi yapılır. SYY' de son olarak kullanıcının kart bilgileri düzenlenir. SYY tarafında işlemler tamamlandıktan sonra NKMY üzerinde kurulumların yapılması gerekmektedir. NKMY üzerinde site yöneticisi erişim bilgilerini girerek SYY üzerinde oluşan Kullanıcı Kodu Bilgisini NKMY üzerine kaydeder ve site sakini artık ödemelerini yapabilecek hale gelir.

Şekil 3.35: Kullanıcı Kayıt İşlem Akışı.

3.2.2. Ödeme İşlemi

Kullanıcı kaydını tamamlamış olan site sakinleri android telefonlarında kurmuş oldukları NKMY ile artık ödemelerini sorunsuz bir şekilde yapabilecektir. Planladığımız genel sistemde; Apartman sitelerinin giriş kapısının önünde bir kiosk olduğu düşünülmüştür ve bu kioskun üzerinde NOMY' nin kurulu olduğu kabul edilen android cihazın sabitlendiğini düşünüyoruz.

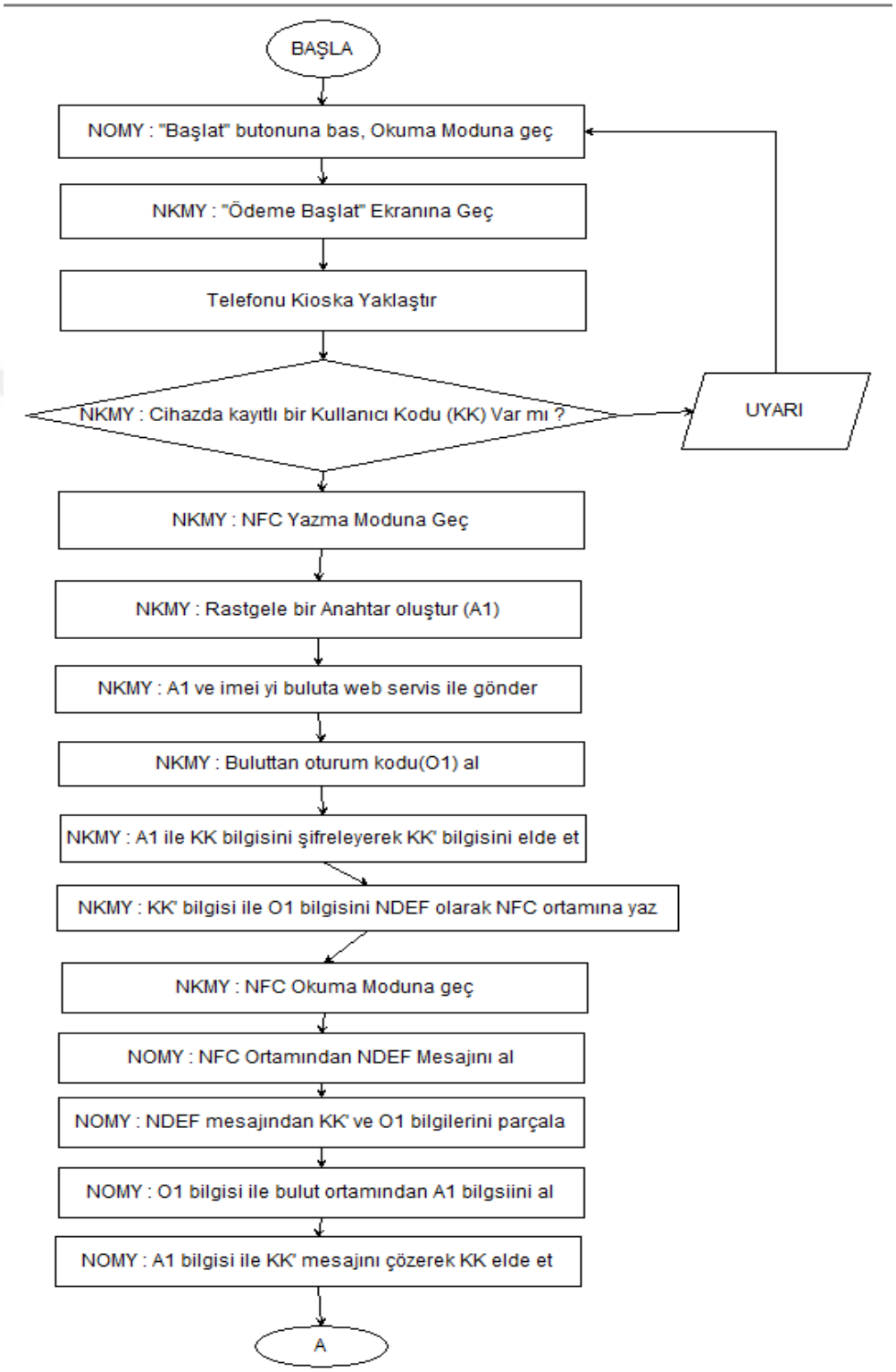
Site sakinleri, android telefonlarında NFC özelliğini aktifleştirdikten sonra NKMY yazılımımızı çalıştırırlar. Kioskda çalışmakta olan NOMY' nin bekleme ekranında Başla'ya basılır ve Kullanıcı telefonunu kioska yaklaştırır ve cihazlar arasında NFC tabanlı haberleşme başlatılır. Karşılıklı veri alışverişleri sırasında gerekli kontroller yapılır ve şartlar sağlanmış ise kullanıcının uygulamasında şifre giriş ekranı gelir kullanıcı sadece kendisinin bildiği güvenli şifresini girmek sureti ile ödeme yapmak istediği borcunu seçer ve ödemesini tamamlar. Özet olarak anlatılan sürecin akış diyagramı detayları ile birlikte aşağıdadır.

Kullanıcıların işlem yapabilmeleri için yapılan kontrollerin bir kısmı şöyledir;

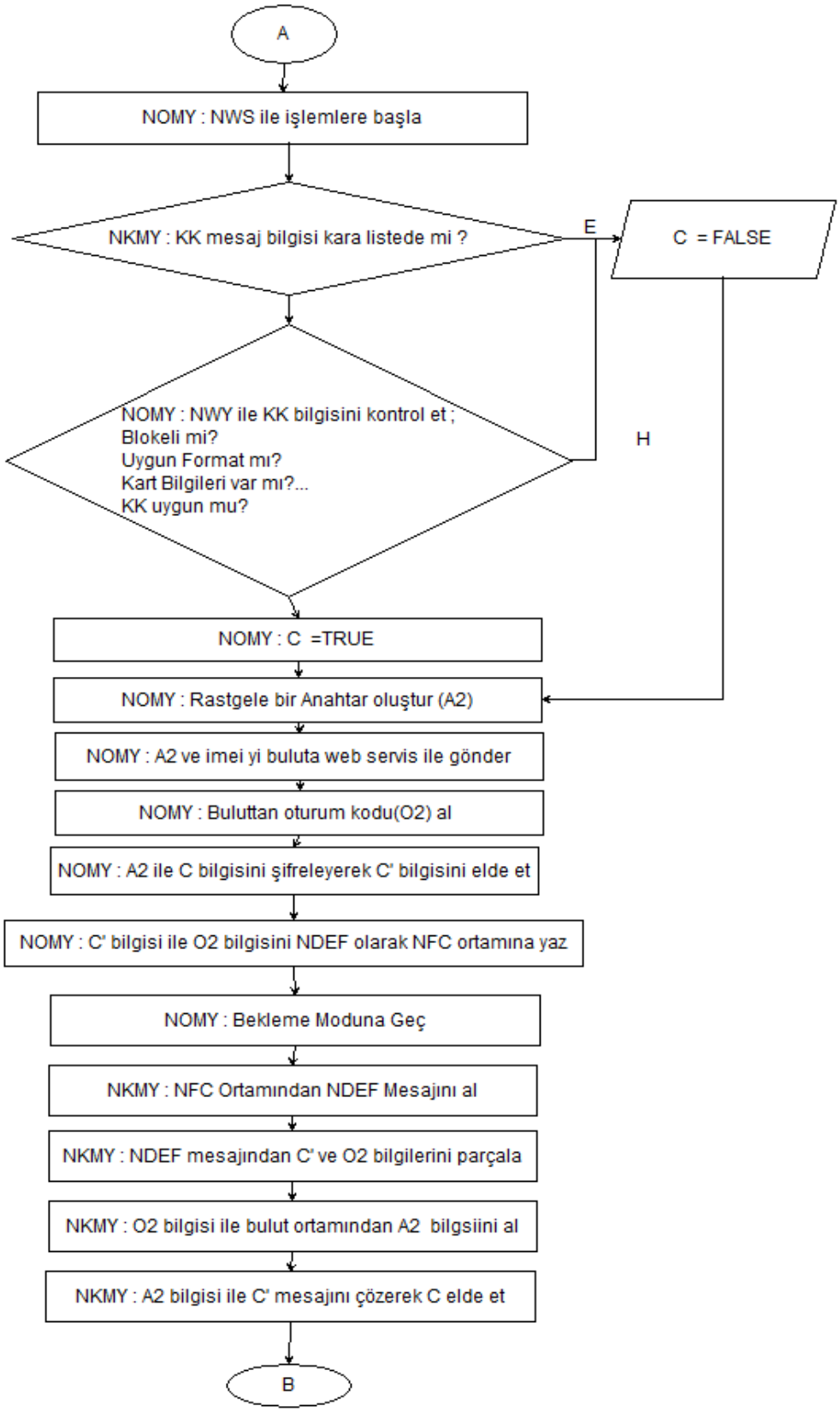
- Kullanıcı blokeli mi?
- Mesaj paketi kara listede var mı?
- Kullanıcı kart bilgileri var mı?
- Kullanıcı Kayıtlı mı?
- Kullanıcının borcu var mı?
- NFC özelliği aktif mi?
- Kullanıcının şifre bilgisi doğru mu?
- Kullanıcın NKMY' de kayıtlı olan Kullanıcı kodu bilgisi doğru mu?
- NDEF mesajı standartlara uygun mu?

Yukarıdaki kontrollerin tamamından başarılı bir şekilde ilerleyebilen kullanıcılar ödemelerini tamamlamış olacaktır ve kullanıcıların bu başarılı işlemlerinin makbuzları bulut ortamında saklanacaktır. Kullanıcılar isterlerse site yönetimlerinden SYY vasıtası ile bunu talep edebilecekleri gibi DYY üzerinden kendileri de bu makbuzlara

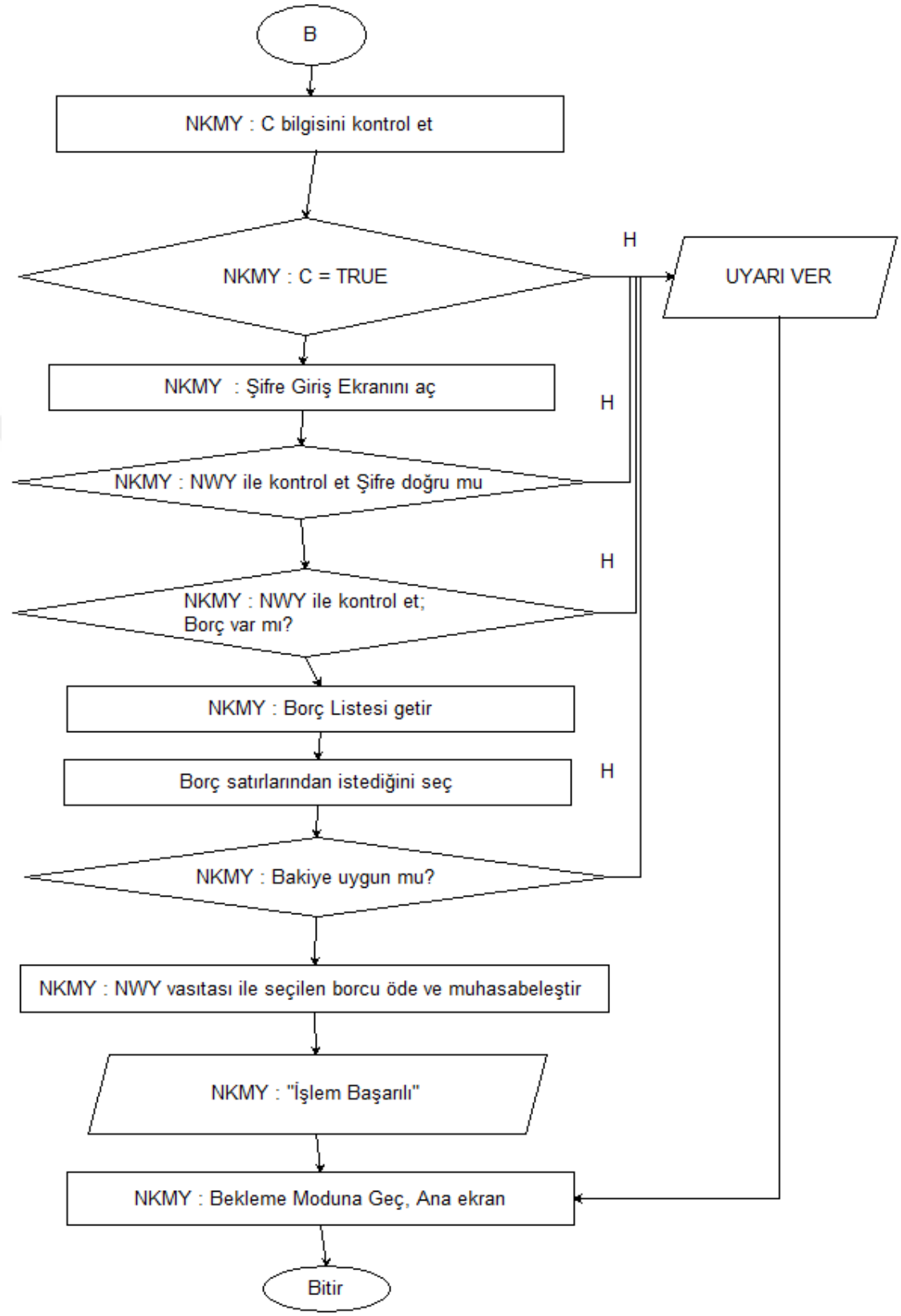
erişebileceklerdir. Böylelikle kullanıcılar sadece bir şifre bilgisi girmek sureti ile site yönetimine uğramadan ödemelerini direkt yapabilecektir.



Şekil 3.36: Ödeme İşlem Akışı 1.



Şekil 3.37: Ödeme İşlem Akışı 2.



Şekil 3.38: Ödeme İşlem Akışı 3.

4. BULGULAR

Geliştirdiğimiz mimariyi Performans ve Güvenlik olmak üzere 2 açıdan değerlendirmemiz uygun olacaktır. Muhtemel saldırı türleri ve bu saldırılara karşı alınan önlemlerin başarıları "saldırı türü" bazında ifade edilecektir. Sistemin güvenilirliği gösterildikten sonra alınan önlemlerin performans üzerindeki etkisi incelenecektir. Güvenlik önlemlerinin performans açısından oluşturdukları zafiyet, toplam sistem maliyeti ve saldırı türlerinin yaygınlığı oranları üzerinden ayrıca incelenecektir. Bu doğrultuda bulgularımız aşağıdaki başlıklar çerçevesinde incelenecektir.

1. Güvenlik
   1.1.Saldırı türleri ve alınan önlemler
   1.2.Güvenlik önlemleri ve sistem üzerindeki etkileri
2. Performans
   2.1.Güvenlik önlemlerinin sistem maliyetlerinin hesaplanması
3. Karşılaştırmalar
   3.1.Güvenlik Karşılaştırmaları
   3.2.Performans Karşılaştırmaları

4.1. GÜVENLİK

4.1.1. Saldırı Türleri Ve Alınan Önlemler

NFC teknolojisi haberleşmenin gerçekleşmesi için cihazlar arasında çok yakın mesafe (en fazla 4cm) gerektirdiğinden bluethoot gibi RFID ortamında çalışan birçok teknolojiye göre daha güvenli kabul edilmektedir. (Özdemir S. , 2011)Gelişen teknoloji ile birlikte saldırı türleri ve araçları da geliştiğinden NFC teknolojisinin yakın alan haberleşmesi birçok saldırıya maruz kalmıştır ve bu saldırılardan saldırganlar açısından başarılı sonuçlar alınmıştır. Bunun sonucunda haberleşme ortamlarının maruz kaldığı birçok saldırı türüne NFC tabanlı sistemlerde maruz kalmıştır.

Bu kısımda saldırı türlerinden kısaca bahsedilerek bu saldırı türlerine karşı aldığımız önlemler incelenecektir. Tabloda saldırı türleri ve önlemler özet olarak görülmektedir.

Tablo 4.1: Saldırı Türleri ve Güvenlik Önlemleri.

Saldırı Türü	**Etkili Olan Güvenlik Önlemleri**
Sniffing	Yalıtkan Ortam Tasarımı, İki taraflı aktif cihaz kullanımı, NDEF AES Simetrik Şifreleme, SSL tabanlı ve yetkili web service
Spoofing	İki taraflı aktif cihaz kullanımı, Şifreli Veri Saklama, Kullanıcı Login, Kullanıcı Şifre bilgisinin bulut ortamında saklanması
Paket Manipülasyon	Mesaj Formatı ve Kara Liste
Replay Attacks	Kullanıcı Login, Mesaj Formatı ve Kara Liste
Denial Of Service	Yalıtkan Ortam Tasarımı, Tuş Kombinasyonu
Man In The Middle Attack	Kullanıcı Login, NDE F AES Simetrik Şifreleme, SSL tabanlı web servis yetkilendirme, Şifreli veri saklama, Kullanıcı Şifresinin bulut ortamında saklanması

4.1.1.1. Sniffing (Dinleme)

Bu saldırı türü ile saldırgan haberleşme esnasında RFID üzerinden paylaşılan mesaj paketlerini dinleyerek sistem üzerinde istemediğimiz veya öngörmediğimiz işlemler yapmak istemektedir. Gelişmiş ve güçlü RFID antenlerine sahip cihazlar rahatlıkla ortam dinlemesi yapabilmektedir. Ortamın, fiziksel olarak tam anlamıyla yalıtkan hale getirilmesi bir seçenek olarak düşünülse de ortam dinlemeleri ilgili geliştirilen donanımlar da bu yönde zaman içinde yalıtkan ortamlar ile ilgili alternatif yöntemler geliştirecektir. Sniffing saldırılarından etkilenmemenin en etkili yolu saldırganın ortam üzerindeki mesaj paketlerini ele geçirdikten sonra mesajımız ve sistemimiz ile ilgili

önemli verilere ulaşmasını engellemektir. Saldırganın elinde anlamlandıramayacağı veya herhangi bir amaç için kullanamayacağı bir mesaj paketinin bulunmasının bizim için bir önemi yoktur.

Dinleme sonucunda ele geçirdiği verilerin bizim için sorun olmaması, saldırganın elindeki verilerin şifreli olmasını gerektirir. Saldırganın elde ettiği verilerin şifreli olması bizim sistemimizin güvenliğini sağlamış olmamız için yeterli bir kriter değildir çünkü saldırgan elindeki birçok paketi inceleyerek bizim şifreleme algoritmamızı ve var ise anahtarımızı elde ederek asıl veriye ulaşmayı da deneyecektir. Günümüz gelişen teknolojisindeki başarılı şifreleme algoritmaları çalışmamızın önceki kısımlarında detaylıca anlatılmıştı. Bu algoritmaların genellikle bir anahtar vasıtası ile şifreleme işlemi yaptığını göz önünde bulundurursak saldırganın aslında ulaşmak istediği önemli bir bilginin de aslında şifreleme algoritmamızın kullandığı anahtarın olduğunu düşünebiliriz. Saldırgan elindeki birçok mesaj paketimizden de farklı yazılımlar veya deneme yanılma yöntemleri ile de asıl veri ve mesaj paketi arasında bir desen tespit ederek anahtarı tespit etmeye çalışacaktır. Bütün bunlardan yola çıkarak saldırganın elindeki mesaj paketlerinden anahtar bilgimize ulaşmasını engellememiz gerekmektedir, şimdi bunun ile ilgili aldığımız güvenlik önlemlerini inceleyebiliriz.

Sniffing Saldırı türüne karşın alınmış güvenlik önlemleri;

1.Yalıtkan ortam tasarımı; Bu önlem çalışmamız kapsamında gerçekleştirilmemiş olup sadece bir seçenek olarak belirtilmiştir. Gerçek anlamda bir yalıtkan ortamın sağlanması durumunda bile saldırganın bu yönde yapacağı karşı geliştirme ve çalıştırmaları öngöremediğimiz için bu kısım ile ilgili çalışmalar kapsam dışında tutulmuştur.

2.İki taraflı aktif cihaz kullanımı; Mimarimizde haberleşmenin her iki ucunda da aktif NFC tabanlı cihazlar kullanılmıştır. Her iki ucun da aktif olması, uçlara şifreleme ve şifre çözme kabiliyeti kazandıracağından haberleşmenin programlanabilir ve şifreli olması sağlanmıştır. Böylelikle sniffing saldırılarında ele geçirilen mesajlarımızın şifreli olması şartı yerine getirilmiştir.

3.NDEF AES Simetrik Şifreleme; NFC haberleşmede kullanılan NDEF paketleri RFID ortamına bırakılmadan önce gönderici tarafından anlık olarak rastgele oluşturulan

bir “Private Key” ile şifrelenir ver şifreli NDEF paketi RF ortamına bırakılır. “Private Key” ise SSL tabanlı bir web servis aracılığı ile bulut ortamında bir oturum oluşturularak aktarılır. Alıcı cihaz ise bulut ortamındaki açık oturumdan “Private Key” Bilgisini yine SSL tabanlı web servis vasıtası ile alır ve RF ortamından gelen şifreli NDEF mesajının şifresini çözerek kullanır.

Saldırgan sniffing sonucunda mesaj paketimizi ele geçirse bile “Private Key” bilgisine sahip olmadığı için asıl verimize ulaşamayacaktır. Elindeki birçok mesaj paketinden bir desen de oluşturamayacaktır çünkü “Private Key” karşılıklı veri alışverişi dâhil olmak üzere her seferinde rastgele oluşturulmaktadır.

Mesaj paketlerimizin rastgele anahtarlar ile şifrelenerek paylaşılması ortamı dinleyen saldırganların paketlerimizi ele geçirdikten sonra herhangi bir işlem yapamayacaklarını garanti altına almaktadır.

4.SSL Tabanlı Ve Yetkili Web Servis; Haberleşme esnasında AES şifreleme metodunun kullanmış olduğu “Private Key” bilgisinin RF ortamından değil de web servis tabanlı ve 128 bitlik SSL sertifikası güvencesindeki bulut ortamından transfer edildiğinden saldırgan tarafından ele geçirilen mesaj paketlerimizden asıl veriye ulaşılamayacaktır ve sistemimiz güvenliğini gerçekleştirmiş olacaktır.

Web ve modem ortamının dinlenilme durumunu da göz önünde bulundurursak bulut ile cihaz arasındaki haberleşmenin de önemli olduğunun farkına varıyoruz. Bu açık 128 bitlik SSL sertifikası kullanılarak kapatılmıştır yine benzer şekilde web servis fonksiyonlarının çalışması için gerekli olan ve bulutta saklanıp kontrolünün de bulut da yapıldı bir web servis şifresi kullanılmıştır.

4.1.1.2. Spoofing (Aldatma)

Bu saldırı türü ile saldırgan ortamda bulunan iki cihazdan birinin kopyasını oluşturarak diğer cihaz ile haberleşmeye çalışır ve böylelikle bizim için önemli olan verilere erişir ya da sistem üzerinde yetkisiz işlemler yapar. Sistemimizde bu saldırılara karşı da gerekli önlemler alınmıştır.

Spoofing saldırıları genellikle pasif NFC etiketlerinin kullanıldığı mimarilerde etkili olmaktadır. Sistemimizin her iki ucunun da aktif cihazlardan oluşması spoofing saldırısının büyük oranda önüne geçmektedir fakat cihazların da kopyalanabileceğini düşünürsek hala bu saldırıya karşı yeterince önlem almış olmayız. Aktif cihazların tamamen kullanıcılardan bağımsız çalışması bu saldırı türüne için büyük bir açık vereceğinden sistemimizde başlayan bir haberleşmenin devam etmesi sadece kullanıcının bildiği ve bulut ortamında şifreli olarak saklanan kullanıcı şifresinin ekrana doğru bir şekilde girilmesi gerekmektedir. Böylelikle; bütün cihazlar kopyalansa dahi haberleşmenin devam etmesi bir diğer ifade ile ödemenin tamamlanması için bir insanın kullanıcıya ait şifreyi girmesi gerekmektedir.

Cihazın kopyalandığını varsayarak cihazın içinde sistem ile ilgili bilgileri tehlikeye attığımız düşünülebilir bunun ile ilgili de sistem ile ilgili cihazdaki bütün bilgilerin şifreli olarak tutulduğunu ve ilgili "Private Key" bilgisinin de bulut ortamında saklandığını belirtmek gerekir.

Spoofing Saldırı türüne karşın alınmış güvenlik önlemleri;

1.İki taraflı aktif cihaz kullanımı; Sistemdeki cihazların pasif NFC etiketleri olmaması spoofing saldırılarının büyük bir kısmına karşı sistemimizi korunaklı kılmaktadır. Aktif cihazlar kullanıyor olmamız, kopyalanma işleminde NFC modülünü içinde barındıran teknolojinin donanım ve yazılım kapsamında alınan bütün güvenlik engellerini aşmış olmayı gerektirecektir.

2.Şifreli Veri Saklama; Sistemimizdeki cihazların donanım ve yazılım düzeyinde kopyalandığını kabul etsek dahi cihaz üzerinde kayıtlı ve kullanıcı ile ilgili bilgiler AES altyapısında şifrelenmiş bulunacaktır. AES algoritmasının kullanmış olduğu "Private Key" bilgisi de bulut ortamında saklandığından saldırgan elindeki şifreli veriyi normal yollarla çözemeyecektir.

3.Kullanıcı Login; Saldırgan sistemimizdeki cihazlardan herhangi birini kopyaladıktan sonra haberleşmeyi başlatıp ödeme yapmak istediğinde ödeme işlemi gerçekleşmeden önce saldırgandan sadece kullanıcının bildiği kullanıcı şifresi bilgisinin girilmesi istenecektir. Saldırgan bu şifreyi doğru bir şekilde giremediği sürece işleme devam edemeyecektir, saldırgan şifreyi 5 defa yanlış girdiği takdirde ilgili kullanıcı

otomatikman bloklanacaktır ve incelemeye alınacaktır. AES ile şifrelenmiş ve elinde "Private Key" bilgisini barındırmadan en fazla 5 deneme ile doğru şifrenin bulunması ihtimali de ihmal edilecek kadar düşük bir ihtimaldir.

4.Kullanıcı Şifresinin Bulut Ortamında Saklanması; Spoofing saldırısını gerçekleştirmek üzere asıl cihazın kopyası olarak sistemde kullanılan sahte cihaz ile yapılan denemelerde şifre engelinden bahsetmiştik, Şifre bilgisinin de cihazda saklanması durumunda saldırgan başarılı bir şekilde login olacaktır. Bunun önüne geçebilmek için kullanıcıların şifre bilgileri kullandıkları cihazda değil de bulut ortamında saklanmaktadır bundan dolayı cihazdan bağımsız olarak saldırganın elinde olmayan ve sistemin işlemlerine devam edebilmesi için gerekli olan önemli bir bilgi korunmuş olmaktadır.

4.1.1.3. Paket Manipülasyon

Bu saldırı türü sistem içindeki cihazların haberleşme esnasında birbirlerine gönderdikleri paketler üzerinde ekleme, değiştirme veya bozma şekline işlemler yaparak haberleşmenin aksamasına veya farklı sonuçlar üretmesine sebep olmaktadır. Bu saldırı türünün sistemin çalışması ile ilgili getirdiği olumsuzluklar Sniffing saldırısında bahsedilen güvenlik önlemlerimiz ile kontrol altına alınabilir.

Manipülayon Saldırı türüne karşın alınmış güvenlik önlemleri;

1.Mesaj Formatı; Şifreli NDEF mesajı "Private Key" ile çözüldükten sonra elde ettiğimiz mesaj mimarimizde belirli bir formata bağlanmıştır ve bu formatın dışındaki mesajlar tehdit olarak algılanarak işleme alınmamaktadır. Bu mekanizma Paket Manipülasyonu saldırılarına karşın sistemimizi güvenli kılmaktadır aksi takdirde başarılı bir şekilde değiştirilmiş bir içerik yine başarılı bir şekilde şifresi çözülebilirse ve ana mesajın formatının da mimarimizdeki formata uygunluğu kontrol edilmediğinden saldırgan sistemimiz üzerinde istemediğimiz bir işlem gerçekleştirmiş olacaktı.

2.Kara Liste; Sistem, Paket Manipülasyonu saldırısı sonucunda oluşan tehlikeli mesaj paketlerinin bulut ortamındaki kara listeye ekleyerek bir sonraki haberleşmelerde işleme

alınmamasını sağlamaktadır. Bu güvenlik önlemi bu saldırı türündeki denemelerin boşa çıkarılması ve sistemin kaynaklarının gereksiz yere harcanmaması açısından önemlidir.

4.1.1.4. Replay Attacks (Tekrarlı Saldırılar)

Bu saldırı türü ile saldırgan iki tür saldırı hedeflemektedir. Birincisi; Sistemdeki haberleşmelerde kesintiler ve karışıklıklar oluşturarak sistemin çalışmasını zaafa uğratmaktır, bu saldırı için Sniffing ve Paket Manipülasyonu saldırılarında alınan önlemler düzeyinde karşılık verebileceğimizden bizim veri güvenliğimizi tehdit etmemektedir. İkincisi; Saldırgan tekrar göndermek üzere aldığı bir mesaj paketini farklı zamanda tekrar karşı cihaza gönderirse karşıdaki cihaz paketi sorunsuz bulup işleme alacağından sahte cihaza istediği sonucu dönecektir. Bu tehlike ye karşı sistemimizin kullanıcıların her işlem için login olma şartını getirmesini ileri sürebiliriz, böylelikle paket karşı tarafa gitse bile login gerçekleşmeyeceğinden işlem yapılmayacaktır.

Replay Attacks Saldırı türüne karşın alınmış güvenlik önlemleri;

1.Kullanıcı Login; Saldırgan başarılı işlem görülmüş bir paketi tekrar gönderse bile bulut ortamında saklanan ve sadece mesajın asıl sahibinin bildiği şifreyi doğru bir şekilde giremediği sürece işleme devam edemeyecektir, saldırgan şifreyi 5 defa yanlış girdiği takdirde ilgili kullanıcı otomatikman bloklanacaktır ve incelemeye alınacaktır. Aynı mesajı en fazla 5 defa gönderebilecek olması da Tekrarlı saldırıların önünde ayrıca bir engel olarak düşünülebilir.

4.1.1.5. Denial Of Service (Hizmet Durdurma)

Bu saldırı türü ile saldırganın tek hedefi sistemi meşgul ederek kullanılmaz hale getirmektir. Bu tür bir saldırıda saldırgan ile gerçek kullanıcıyı ayırt etmek zor olduğundan bunun ile ilgili geliştirdiğimiz yöntem gerçek ya da sahte olsun kullanıcıyı sürecin içine katmakla olabilir. Şöyle ki; Kullanıcıya Bir tuş aktivasyonu, Login gibi işlemi zorunlu tutarak farklı bir cihazla üst üste işlem yapılmasının önüne geçilmiş olacaktır.

Diğer saldırılarda alınan önlemlerin tamamı aslında DOS saldırıları için saldırganın önünde engel teşkil etmektedir.

Denial Of Service Saldırı türüne karşın alınmış güvenlik önlemleri;

1.Yalıtkan Ortam Tasarımı; Daha önce belirttiğimiz üzere bu önlem çalışmamız kapsamında gerçekleştirilmemiş olup sadece bir seçenek olarak belirtilmiştir. Gerçek anlamda bir yalıtkan ortamın sağlanması durumunda bile saldırganın bu yönde yapacağı karşı geliştirme ve çalıştırmaları öngöremediğimiz için bu kısım ile ilgili çalışmalar kapsam dışında tutulmuştur.

2.Tuş Kombinasyonu; Bu saldırı türü için en etkili güvenlik önlemimiz Tuş Kombinasyonudur. Saldırgan sistemdeki ana cihaza paketler göndererek sistem üzerinde aksaklık oluşturmak istemektedir fakat ana cihazımız işleme başlamak için "Başla" butonuna basılmayı gerektirmektedir ve işlem bittikten sonra ya da 10 saniye sonra otomatikman yine dinleme modu kapatılarak uyku moduna geçecektir. Böylelikle üstüste yapılan her saldırıda tekrar ana cihazında aktif edilmesi gerekmektedir ki bu da Dos saldırılarının hoşlandığı bir durum olmayacağından gerçek anlamda bir koruma sağlanmış olacaktır.

4.1.1.6. Man In The Middle Attack (Ortadaki Adam)

Bu saldırı türü ile sistemimizde haberleşmek üzere bulunan iki cihazımızın dışında saldırganın ortama yerleştirdiği üçüncü bir cihaz söz konusudur. Ortamdaki 3. Cihaz A cihazından gelen veriyi alır ve aynen B'ye gönderir, B işlemlerini yapar ve cevap olarak paketi RF ortamına bırakır, 3.cihaz B'den gelen cevabı alır ve A'ya iletir ya da iletmez, sonuç olarak böyle bir senaryoda haberleşmenin 3.cihaz üzerinden ilerlediğini ve bütün mesaj paketlerimize ulaşabildiğini gördük.

Bu saldırı türü her iki ucun da aktif olduğu durumlarda gerçekleştirilebilir. Taraflardan biri bile pasif olmuş olsa bu saldırı gerçekleştirilemez. Bizim mimarimizde iki uç da aktif olduğundan bu saldırının riski altındayız. Ortadaki adam saldırısının sistem üzerindeki riski şöyledir; bütün mesaj paketlerimizi elde ederek verilerimiz hakkında bilgi edinmesi ve haberleşmeye müdahale ederek taraflara istemedikleri işlemleri

yaptıracak paketler göndermesi. Bizim sistemimiz yukarıda belirtilen güvenlik önlemleri doğrultusunda bu saldırı türünden gelecek tehlikelere karşı koyabilmektedir. Sistemdeki veriler üzerinde değişiklik yapılması ya da sisteme istemediği bir işlem yaptırması gibi senaryolar yukarıdaki tüm önlemler ile engellenmektedir.

Man-in-the-Middle-Attack Saldırı türüne karşın alınmış güvenlik önlemleri;

- ✓ Kullanıcı Login
- ✓ NDEF AES Simetrik Şifreleme
- ✓ SSL Tabanlı ve Yetkili Web Servis
- ✓ Şifreli Veri Saklama
- ✓ Kullanıcı Şifresinin Bulut Ortamında Saklanması

4.1.2. Güvenlik Önlemleri Ve Sistem Üzerindeki Etkileri

4.1.2.1. Kullanıcı Login

Tamamı insandan bağımsız mimarilerin birçok saldırı türüne karşı üreteceği çözümler sınırlıdır. Cihazların yazılım veya donanım olarak kopyalanması saldırganın yetkisiz işlemler yapabilmesi için yeterlidir aynı şekilde cihazın hırsızlık sonucunda çalınması da benzer şekilde kolay bir şekilde saldırganların sistem üzerinde yetkisiz işlemler yapmasına sebep olacaktır. Geliştirmiş olduğumuz Hibrit model, ödeme işlemi başlatıldıktan sonra borç bakiyeleri listelenmeden hemen önce Kullanıcını sadece kendisinin bildiğini kabul ettiğimiz şifresini girmesi için login ekranını açıyoruz ve ancak burada en az 5 denemede şifreyi başarılı girdiği takdirde ödeme işlemine devam ediyoruz. NFC uyumlu araba anahtarları çalışmasında da (Suman Chaudhary, 2014) benzer yapı kullanılmıştır. İlgili çalışmada login şartı getirilerek etkin bir güvenlik önlemi alınmıştır fakat haberleşmenin tamamı RF ortamından yani tek kanal üzerinden gerçekleştiğinden yukarıda bahsi geçen ve ilerleyen aşamalarda detayları ile birlikte vereceğimiz birçok saldırıya açık vermiş durumdadır.

Login işleminde saldırganın 5 hatalı denemesi kullanıcının bloke edilmesine ve tekrar işlem yapılmamasına sebep olacağından deneme yanılma yöntemi ile sistem üzerinde yetkisiz işlem yapma ihtimali kalmayacaktır.

Kullanıcı Login ekranında sadece şifresini girmektedir çünkü kullanıcı adı bilgisi Android cihazımızın Sqlite veritabanında şifreli olarak saklanmaktadır ve şifre bilgisi ile birlikte SSL tabanlı web servisimiz vasıtası ile bulut üzerinden kontrol edilmektedir.

Kullanıcı Login güvenlik önlememiz sistemimizin üzerinde çok etkili bir koruma yöntemi olarak yerini almaktadır. Bu güvenlik önlemimizin etkili olduğu saldırı türlerini şöyle sıralayabiliriz; Spoofing, Replay Attacks, Denial of Service ve Man in The Middle Attack.

Sonuç olarak; bahsi geçen saldırılara karşı etkili olduğu gibi gerçek hayattaki hırsızlık gibi birçok sistemi savunmasız bırakıldığı durumlarda da etkili bir engel oluşturulmuştur.

4.1.2.2. Yalıtkan Ortam Tasarımı

Bu tezimizin kapsamında detaylandırılmamış fakat bir öneri düzeyinde yeri geldikçe öne sürülmüş birçok saldırıya karşı etkili avantajlar sağlayabilecek bir önlem türüdür. Gerçek anlamda bir yalıtkan ortam yapmak teknoloji ile orantılı olarak daha da ilerleyecektir bununla beraber saldırganlarında kullandıkları donanımlar gelişecektir. Bu yüzden bu yöntem tezimizin dışında düşünülmüştür.

NFC teknolojisi, maksimum 4cm mesafede haberleştiğinden ortam dinlemelerine karsı diğer kablosuz haberleşme teknolojilerine göre daha güvenlidir fakat gelişmiş RFID antenleri vasıtası ile bu mesafede de dinlemeler yapabileceğinden NFC teknolojisi de ortam dinlemelerine karşı tehdit altındadır. Bu güvenlik önerimiz ile bu saldırı ve tehditlere karşı büyük oranda güvenlik sağlanmış olacaktır. Bu güvenlik önlemi Sniffing, Denial of Sevice gibi saldırılara karşı etkilidir.

4.1.2.3. İki Taraflı Aktif Cihaz Kullanımı

NFC Teknolojisinde kullanılan 2 çeşit donanım olduğundan daha önce bahsetmiştik. Bu donanımlar aktif ya da pasif cihazlar şeklinde tasarlanmıştır. Pasif etiketler üzerinde kopyalama işlemi daha kolay olmakla birlikte kullanım esnasında kopya etiketlerin tespit edilmesi de zordur. Çalışmamız da haberleşmenin her iki ucunda da aktif cihazlar kullanılmıştır. Man In The Middle saldırıları için her iki tarafın da aktif olması gerekiyor ve bu durum mimarimiz için özel bir risk oluşturmaktadır. Bu risk için aldığımız önlemler önceki bölümde açıklanmıştır.

Her iki ucun da aktif olması sistemimizi Sniffing ve Spoofing saldırılarından büyük oranda korumaktadır. Saldırganın sistemimiz üzerinde bu tür saldırıları rahatlıkla yapabilmesi için pasif etiket türünden donanımları kullanması gerekecektir, bu etiketler mimarimizde kullanılmadığı için de saldırılardan netice alınamaz. Haberleşmede IMEI kullanılması da aktif cihazları birbirine karşı güvenli kılmıştır.

4.1.2.4. Ndef Aes Simetrik Şifreleme

NFC tabanlı haberleşmenin RF ortamında gerçekleştiğini belirtmiştik. Haberleşmek isteyen uçlar göndermek istedikleri mesajları bu ortama bırakır ve ortamdaki diğer bütün cihazlar ortamı dinleyerek bu mesajı alabilir. Sistemimiz de korunması gereken bilgilerin RF ortamına bırakılması ve servis yazılımımız tarafından alınması bizim yapmak istediğimiz şey olduğunu düşünürsek, ortamdaki başka cihazların da bu bilgiye ulaşması mümkündür. NFC teknolojisinin bütün sistemler ile entegre olabileceğini düşünürsek bu konuda katı önlemler almasını bekleyemeyiz bu yüzden NFC ile haberleşmede kullanılan NDEF mesajları herhangi bir şifrelemeye tabi olmadan direk transfer edilir.

Uygulamamızda veri transfer işlemi yapılmadan ve NDEF mesajı oluşturulmadan önce AES 128 ile simetrik şifreleme yöntemi kullanılarak şifrelenir. Simetrik şifrelemenin genel mantığından gelen ve şifrelemesinde kullanılan “Private Key”’in de mesajı alıp şifreli veriyi çözebilecek uca iletilmesi gerekir.

Şifreleme de sabit bir “Private Key” kullanılması ortamı dinleyip paketlerin büyük kısmını eline geçiren saldırganların çok ciddi anlamda işine yarar. Elinde birçok mesaj olan saldırgan bu mesajlardan bir desen elde ederek “Private Key” bilgimizi elde edebilir. Bir diğer senaryo da aktif uçlardan birinin gönderdiği bir şifreli mesajı ele geçiren saldırgan sabit “Private Key” kullanılırsa aynı mesajı farklı zamanlarda ortama bırakarak sistem üzerinde istemediğimiz işlemler yapılabilir. Bu risklerin önüne geçmek için sistemimizde kullanılan “Private Key” bilgisi her haberleşmede cihazın guid bilgisi kullanılarak rastgele “Private Key” oluşturulur.

Sonuç olarak; her transfer işlemi için özel bir anahtar üretilir ve güvenilir bir şekilde şifrelenerek transfer edilir. “Private Key” her işlemde tekrar oluşturulduğundan saldırganlar tarafından ele geçirilirse bile bir işlem yapamayacaktır. Man in the middle, Sniffing, Spoofing gibi saldırıların önüne geçmektedir.

4.1.2.5. SSL Tabanlı ve Yetkili Web Servis

Simetrik şifrelemede kullanılan “Private Key” bilgisinin karşıdaki cihaza da gönderilmesi gerekir. Anahtar bilgisi de şifrelenmiş NDEF mesajı gibi RF ortamından gönderilirse sistemin tamamı tehlikeye atılmış olur çünkü iki bilgiyi de ele geçiren saldırgan anahtar bilgisini kullanarak mesajı çözebilecektir. Bu sorunun önüne geçebilmek için “Private Key” bilgisi farklı bir ortamdan gönderilmelidir. Mimarimiz de fiziksel ortamdan bağımsız olarak Web Servis tercih edilmiştir. Geliştirdiğimiz web servis üzerinden bulut ortamına bir bağlantı kurularak” anahtar bilgisi gönderilir RF ortamına ise açılan oturuma özgü bir kod gönderilir. Alıcı cihaz oturum kodu ile birlikte bulut ortamına bağlanarak anahtar bilgisini alır RF ortamından aldığı mesajı bu anahtar ile çözerek işlemine devam eder.

Yukarıda belirtilen önlemler birçok soru işaretini beraberinde getiriyor. Örneğin; saldırgan aynı anda kablosuz ya da kablolu internet ağını dinleyerek bulut ortamına göndermek istediğimiz anahtar bilgisini almak isteyebilir ve bu da sık karşılaşılan bir saldırı yöntemidir. Bu tehlikeye karşı aldığımız önlem de SSL sertifikası kullanılarak yayınlanan web servisimizdir. SSL ile ilgili tezin önceki bölümlerde detaylı bilgiler

verilmiştir. SSL' in güvenlik anlamındaki başarısı ile ilgili de ayrıca önceki kısımlarda anlatılmıştır. Kullanıcının dinlediği veri 128 bitlik imzalanmış sertifikalar ile şifrelenmiş bir veri olduğundan ve uçtan uca bir şifreleme söz konusu olduğundan saldırganın elindeki veri ile bir işlem yapması mümkün değildir. Bir diğer senaryo ise, Örneğin; Web servisimizin internet ortamına açık olduğunu düşünürsek kötü niyetli kişilerin bu web servise direk erişerek sistem üzerinde işlemler yapması mümkündür. Bu da önemli bir açık olacak iken aldığımız iki alt önlem tehlikeyi bertaraf etmektedir. Bunlardan birinci web servisimizin bütün fonksiyonları bulut ortamında saklanan bir Şifre Bilgisi kullanılarak çalıştırılmaktadır. Bu Şifre bilgisi bilinmeden web servisin hiçbir fonksiyonu çalıştırılamaz. Bir diğer alt önlemimiz ise; Web servisimizin bütün parametreleri şifreli olarak olması ve dönüşlerinin de şifreli olarak dönmesidir ve yine bu şifrelemenin AES 128 ile sadece sistem sahibinin bildiği bir "Private Key" ile şifrelenmiş olmasıdır.

Bu güvenlik önlemimiz Man in the middle, Sniffing, Spoofing gibi saldırıların önüne geçmekle de sistemimize büyük oranda katkı sağlamaktadır. Performans kısmında da değerlendireceğimiz üzere bu önlemin performans anlamında sisteme önemli maliyeti olmaktadır.

4.1.2.6. Şifreli Veri Saklama

Haberleşmenin uçları olarak düşünülen NFC destekli Android cihazlarımızın kendi bünyelerinde sakladıkları veriler de saldırganlar için önemlidir. Saldırganlar cihazların kopyalanması ya da cihazın donanım ve yazılım zaaflarını kullanarak bizim için önemli verilere ulaşmak isteyecektir. Sistemimizde cihazlar üzerinde sakladığımız veriler AES 128 ile simetrik şifreleme tekniği ile şifrelenerek korunmaktadır böylelikle cihazlar üzerinde yapılacak işlemler boşa çıkmaktadır.

Bulut ortamındaki veriler de cihazlar ile aynı risk altında olduğundan, verilerin şifrelenmesi bu ortamda da aynı şekilde sağlanmaktadır. Spoofing ve Man in the Middle saldırılarına karşı da sistemi güvenli kılmaktadır.

4.1.2.7. Kullanıcı Şifresinin Bulut Ortamında Saklanması

Ödeme işlem akışının belli bir aşamasında kullanıcının şifre bilgisini girmesi gerektiğini belirtmiştik. Şifre bilgisi kullanıcın cihazında saklanmış olsa cihaz kopyalandığında ya da cihazın yazılım ve donanım zaaflarından kaynaklanan bir saldırı sonucunda ele geçirilebilir. Bu riske karşılık olarak şifre bilgisini bulut ortamında saklayarak güvenliği önemli ölçüde sağlamış oluyoruz.

Bulut ile haberleşme işleminin SSL sertifikası ile web servis ile sağlandığından şifre bilgisinin transferi de güvenli bir şekilde sağlanmış olacaktır. Kullanıcının şifre bilgisinin de bulut ortamında MD5 şifreleme tekniği ile şifrelenmiş olarak saklandığını da göz önünde bulundurursak sistemimizin güvenliğine önemli ölçüde katkısı olan bu önlemimizin kendisi yeni bir açığa yol açmamış olacaktır. Bu önlemin sistem üzerindeki önemli bir dezavantajı kullanıcının işlem yapmasını sağladığımızdan zaman ve kullanım açısından olumsuz not alabilmektedir.

Bu güvenlik önlemimiz Spoofing, Man in the Middle ve birçok atak türüne karşı etkili olarak sistemimizi korumuş olmaktadır. Özellikle, hırsızlık gibi teknik olarak önleminin alınması mümkün olmayan risklere karşı en etkili yöntemdir.

4.1.2.8. Mesaj Formatı

Haberleşme esnasında tarafların birbirlerine göndermiş oldukları verilerin belirli bir formatta ve standartta olması saldırganların sisteme dışardan göndermek istediği mesajların işleme alınmaması imkanını sunmuş olacaktır.

Kullandığımız Mesaj Formatı ;

9930270451|25 = message_type+site_id+person_id+|+session_id

Yukarıdaki şekilde bir standardımızın olması özellikle Paket Manipülasyonu saldırı türüne karşı etkili bir önlem teşkil etmektedir.

4.1.2.9. Kara Liste

Sistem yöneticisi, uygulama için tehlike arz eden ya da sisteme sorunlara yol açan NDEF paketlerini bulut ortamında bulunan kara listeye ekleyebilir böylelikle haberleşme esnasında gelen paketler eğer kara listede var ise haberleşme yarıda kesilerek işlem yapılmaz.

Kara listenin Android cihazda tutulması kaynak kullanımını olumsuz etkileyeceğinden bu bilgi bulut ortamında saklanmaktadır. Bulut ortamının kaynakları sunucu kapasitesi ile ilgili olduğundan kaynak problemi yaşanmayacaktır.

Kara liste kullanımı özellikle Paket Manipülasyonu saldırısında çok etkili bir koruma sunmaktadır.

4.1.2.10. Tuş Kombinasyonu

Her an haberleşme modunda geliştirilen bir sistem enerji ve cihaz işlemci kaynaklarını her an kullanacağından sistemin performansını olumsuz yönde etkileyecektir. Performans ile birlikte güvenliği de riske atmış olacaktır çünkü Saldırgan devamlı dinleme modunda olan sisteme paketler göndererek deneme yanılma yoluyla ya da özel geliştirilmiş tekrarlı ve hızlı işlemler yapabilen donanımlarla sistem üzerinde sıkıntılara yol açabilmektedir.

Haberleşme ve ödeme işleminin başlamasını kullanıcının cihaz üzerinde “Başla” butonuna basması şartına bağladık. Bu şart yukarıdaki riskleri ve sorunları ortadan kaldırmaktadır fakat kaçınılmaz olarak işlem süresini kullanıcının yapacağı işlemden dolayı uzatmış oluyoruz.

Tuş kombinasyonu yöntemi ile ilgili yapılmış çalışmalar ve öneriler (Quinlan, 2013)bulunmaktadır. Ek olarak çalışmamızda 10 sn içinde sistemin tekrar tuş kombinasyonu gerektirme moduna geçmesini sağladık. Özellikle Replay Attacks ve Denial of Service türündeki saldırılar için etkili bir engel oluşturmaktadır.

Güvenlik önlemlerimizin özet açıklamalarını yapmış olduk tezimizin önceki kısımlarında, bu kısımda detaylarına girmediğimiz özet olarak belirttiğimiz teknikler ile ilgili gerekli detaylar ayrıca belirtilmiştir. Bu kısımda ayrıca güvenlik önlemlerimizin hangi saldırı türlerine ne tür tepkiler verdiğini, sisteme güvenlik anlamında katkıları nelerdir ve örnek senaryolarda ne tür tepkiler verildiği belirtilmiş oldu.

Bir sonraki kısımda performans değerlendirmeleri yapılacaktır. Performans değerlendirilmesi iki farklı yaklaşımla sunulacaktır. Birinci yaklaşıma göre; Güvenlik önlemlerimizin sistemimize getirdikleri maliyetler incelenecektir. İkinci Yaklaşıma göre ise; Saldırı türlerine özgü aldığımız önlemlerin sistem maliyetleri hesaplanacaktır. Böylelikle sistem performans olarak da detaylıca incelenmiş olacaktır.

4.2. PERFORMANS

4.2.1. Güvenlik Önlemlerinin Sistem Maliyetlerinin Hesaplanması

Sistemde güvenlik ile ilgili alınmış önlemlerin performans üzerindeki etkilerini incelemek üzere uygulamalar üzerinde bazı ölçümler yapılmıştır. Sistem birçok defa baştan sona çalıştırılmıştır ve başlangıç ile bitiş arasındaki süre nanosaniye cinsinden tespit edilmiştir, elde edilen bu değerlerin ortalaması elde edilerek aşağıdaki tablonun 1.satırındaki “Çalışma Süresi” bilgisi elde edilmiştir. Tablodaki 10 adet güvenlik kriterlerinin her biri sistemden tek tek çıkarılarak sistemin çalışma süresi aynı şekilde birçok kez hesaplanmıştır ve elde edilen sonuç 1.satırda hesaplanan toplam çalışma süresinden çıkarılarak “Zaman Maliyet” bilgisi hesaplanmıştır ve son olarak hesaplanan bu bilginin toplam çalışma süresine oranı hesaplanarak sistem üzerindeki yüzdelik maliyeti hesaplanmıştır.

Sistemde kullanılan cihazlar;

Cihazların teknik detayları önceki bölümlerimizde detaylıca açıklanmıştır.

- ✓ Samsung Galaxy Note 3
- ✓ Samsung Galaxy S III

Android cihaz üzerinde şifreli olarak saklanmış kullanıcı bilgisi, ödeme işlemi başladığında şifresi çözülerek işleme alınmaktadır. 2. satırdaki istatistik kullanıcı bilgisinin cihaz üzerinde şifreli olarak değil de şifresiz olarak tutulduğu ve şifre çözme işleminin yapılmadığı senaryo üzerinden yapılarak hesaplanmıştır.

NDEF mesaj paketlerinin transfer edilmeden önce şifrelenmesi için her transfer işlemi için rastgele bir "Private Key" oluşturulduğundan bahsetmiştik, bu anahtarın anlık olarak oluşturulmadan sistemde sabit olarak kullanılması durumundaki sistem çalışma zamanı hesaplanarak sonuçları 3. satırda görüntülenmiştir.

Web servisimiz SSL Sertifikasına sahip olduğundan, SSL 'in sistemimiz üzerindeki maliyetini ölçmek için https üzerinden yapılan haberleşmeyi SSL 'li iptal ederek http üzerinden yapmayı denedik ve gerekli ölçümleri aynı şekilde yaptık. 4. satırda görüldüğü üzere sisteme yaklaşık olarak %12 'lik etkisi olduğu görülmüştür.

Web servis üzerindeki haberleşmenin şifreli olduğunu belirtmiştik bu şifrelemenin sisteme getirdiği maliyeti görebilmek için uygulama bu özellik devre dışı bırakılarak denenmiştir ve 5. satırdaki sonuçlar elde edilmiştir.

Sistemimiz üzerinde büyük öneme sahip olan AES şifreleme tekniğinin kullanılmasının sisteme maliyetini analiz edebilmek için NDEF şifrelemesi hariç diğer haberleşmeyi tamamen şifresiz olarak yapmayı da deneyerek 6. satırda görüntülenen sonuçları elde etmiş olduk.

6.satırda tespit ettiğimiz veriler AES 128'in sisteme olan maliyeti hesaplanmak üzere gösterilmiştir. AES 196 ve AES 256 şifreleme tekniklerinin sisteme getirdikleri maliyetler de fikir olması açısından ayrıca hesaplanarak 7. ve 8. satırlarda gösterilmiştir. Hesaplama yöntemi diğer kriterlere göre farklılık göstermektedir çünkü AES 196 ve AES 256 sistemde yokken sisteme eklenerek hesaplamalar yapılmıştır.

Sistem üzerindeki şifreleme işlemlerinden sadece NDEF paketinin şifrelenmesi iptal edilerek yapılan ölçümlerde 9. satırdaki sonuçlar elde edilmiştir. Sonuçlara göre NDEF paketinin şifrelenmesinin sisteme maliyeti 13%'ler civarındadır.

Kara Liste kullanımı Servis Uygulamasının her işlemde bulut üzerinden kontrol sağlattığından sisteme maliyeti herhangi bir uygulamada tercih edilme konusunda bize

önemli fikir sunacaktır. Kara listenin devre dışı bırakılarak yapılan ölçümlerinde 10. satırdaki veriler elde edilmiştir.

Şifreleme işleminde kullanılan ve RF ortamındaki haberleşmede cihazlar üzerinde bulut üzerinden transfer edilerek paylaşılan "Private Key" bilgisinin bulut ortamından değil de NDEF de olduğu gibi RF ortamından paylaşılması durumu da hesaplanmıştır. Bulut ortamındaki paylaşımın sistem üzerindeki etkisi 11. satırda belirtilmiştir.

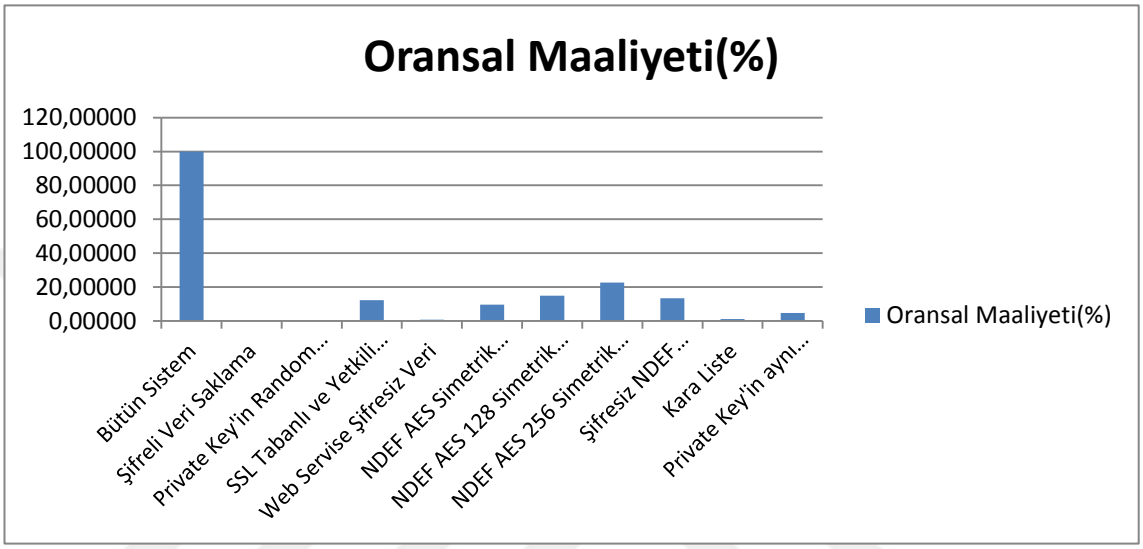
Tablo 4.2: Sistem Performans Metrikleri.

Sistem Performans Metrikleri (NANOSECOND)				
No	**Sistem Kapsamı**	**Çalışma Süresi**	**Zaman Maliyeti**	**Oransal Maliyeti(%)**
	Bütün Sistem	336496044	336496044	100,00000
1	Şifreli Veri Saklama	336477606	18438	0,00548
2	Private Key'in Random değil sabit olması	336480011	16033	0,00476
3	SSL Tabanlı ve Yetkili Web Servis	295356821	41139223	12,22577
4	Web Servise Şifresiz Veri	334012245	2483799	0,73814
5	NDEF AES Simetrik Şifreleme Yokken	303727642	32768402	9,73812
6	Şifresiz NDEF gönderilerek	290990312	45505732	13,52341
7	Kara Liste	332451251	4044793	1,20203
8	Private Key'in aynı ortamda paylaşılması	320235012	16261032	4,83246

Tablodaki verilerin elde ediliş şekli şöyledir; İlk satırda bütün sistemin çalışma süresi nanosaniye olarak belirtilmiştir. Her bir güvenlik önlemi sistemden çıkarılarak sistem tekrar çalıştırılmıştır ve elde edilen çalışma süresi toplam süreden çıkarılmıştır. Bu işlemin neticesinde ilgili güvenlik önleminin "Zaman Maliyeti" hesaplanmıştır. Elde edilen bu değer toplam süreye oranlanarak "Oransal Maliyet" bilgisi elde edilmiştir. Bu sonuçlardan yola çıkarak ilerleyen aşamalarda bu değerler, hesaplamalarda kullanılacaktır.

Yapılan hesaplamalar sonucunda sistemimiz için büyük önemler arz eden güvenlik önlemlerimizin herbirinin sistem üzerinde belli oranlarda fazladan performans maliyetlerinin olduğu görülmüştür. Geliştirilen uygulamaların doğasına ve ihtiyaçlarına uygun olarak bu önlemlerden bir kısmı tercih edilip bir kısmı tercih edilmeyebilir. Çalışmamız literatürdeki birçok çalışmanın üzerinde genel bir analiz yapmak suretiyle hibrit bir modele örnek olduğundan bütün güvenlik önlemleri kullanılmıştır. Sistemin

tam güvenilir hale getirilmesinin maliyeti de hesaplanmıştır. Aşağıdaki grafikte de güvenlik önlemlerimizin sistem üzerindeki maliyet dağılımları farklı bir görsellikte gösterilmiştir. Şifreleme işlemlerinin sistem üzerinde özel bir maliyetinin olduğu da ortaya çıkmıştır.



Şekil 4.1: Güvenlik Önlemleri Oransal Maliyetleri.

4.3. KARŞILAŞTIRMALAR

Geliştirmiş olduğumuz Hibrit modelimizin karşılaşılabilecek 6 saldırı türüne karşı içinde barındırdığı güvenlik önlemlerini ve bu önlemlerin hangi saldırı türlerine karşı koyduklarını detaylıca belirtmiş olduk. Çalışmamızın temel olarak aldığı ve tezin önceki kısımlarında detaylıca açıklanan 9 adet çalışmanın da karşılaştırmasını yaptık.

Karşılaştırmalardaki çalışmalar bulgularımızın "Saldırı türleri ve alınan önlemler" kısmındaki kriterlere göre değerlendirilmiştir. Çalışmaların güvenli olup olmadıkları çalışmamızda detaylıca değindiğimiz saldırı türleri ve bunlara karşı alınması gereken önlemler kapsamında değerlendirilerek belirlenmiştir.

4.3.1. Güvenlik Karşılaştırmaları

Bu kısımda daha önce yapılmış 9 çalışma güvenlik açısından değerlendirilmiştir. Bu değerlendirme Saldırı türlerine karşı bizim tespit ettiğimiz alınması gereken önlemlerin alınmış olup olmama durumuna göre yapılmıştır. Her çalışma kendi içinde özel bir saldırı türü için çözümler üretmiştir fakat farklı saldırı türleri ile ilgili yeterince önlem alınmamıştır. Bu yüzden değerlendirme yaparken sistemin tamamına güvenli veya güvensiz demek yerine saldırı türlerine göre güvenli ya da güvensiz olduklarını ifade etmeye çalıştık.

3.Makale olarak tabloda görmüş olduğumuz makale Tuş kombinasyonu, Simetrik ve asimetrik şifreleme gibi önlemler almakla Sniffing ve DDos saldırılarının önüne geçmiştir fakat diğer 4 saldırı türü için yeterince önlem alınmadığından güvenli olmadığı durumlar ortaya çıkmıştır. Benzer şekilde birçok güvenlik önleminin alındığı fakat Kullanıcı Login önlemi alınmadığı için çalınma tehlikesine ya Man in the Middle saldırısına karşı güvenli olmayacaktır. Rapor oluşturulurken izlenen yöntemi daha iyi kavrayabilmek için ilgili makaleler ayrıca incelenerek ve “Saldırı türleri ve alınan önlemler” başlığındaki tespitlerimiz incelenerek anlaşılabilir. Bahsi geçen 9 makale tezin önceki kısımlarında konumuz ile ilgili olduğu kadarı ile detaylandırıldığından aşağıdaki sonuçların direk verilmesi uygun görülmüştür.

4.3.1.1. Saldırı Türlerine Göre Karşılaştırmalar

Tablo 4.3: Saldırı Türlerine Göre Karşılaştırma.

Saldırı Türleri	(QUINLAN, 2013)	(Michael Roland, 2011)	(Deepa S Pillai, 2014)	(Suman Chaudhary, 2014)	(Helena Rodrigues, 2014)
Sniffing	Güvenli	Güvenli Değil	Güvenli	Güvenli Değil	Güvenli
Spoofing	Güvenli Değil	Güvenli	Güvenli Değil	Güvenli	Güvenli
Paket Manipülasyon	Güvenli Değil	Güvenli Değil	Güvenli	Güvenli Değil	Güvenli Değil
Replay Attacks	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli
DoS	Güvenli	Güvenli	Güvenli Değil	Güvenli Değil	Güvenli Değil
Man In The Middle	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli

Saldırı Türleri	(Chang, 2014)	(Pardis Pourghomi, 2014)	(Wei, 2013)	(Urien, 2015)	HYBRID MODEL
Sniffing	Güvenli	Güvenli	Güvenli	Güvenli Değil	Güvenli
Spoofing	Güvenli	Güvenli	Güvenli Değil	Güvenli	Güvenli
Paket Manipülasyon	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli	Güvenli
Replay Attacks	Güvenli	Güvenli	Güvenli Değil	Güvenli	Güvenli
DoS	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli Değil	Güvenli
Man In The Middle	Güvenli Değil	Güvenli	Güvenli Değil	Güvenli Değil	Güvenli

İncelemiş olduğumuz makalelerin güvenlik ile ilgili aldıkları güvenlik önlemleri aşağıdaki tablodan incelenebilir. Saldırı türleri ile ilgili alınması gereken önlemleri de incelemiştik bu iki bilgi doğrultusunda her çalışmanın saldırı türleri ne göre güvenli olup olmadıkları şeklinde bir analiz yapılmıştır.

Örneğin; (Quinlan, 2013) ‘ nın çalışmasında alınan güvenlik tedbirleri şöyledir; Tuş kombinasyonu, simetrik ve asimerik Şifreleme. Bu güvenlik önlemlerinin hangi saldırı türlerine karşı etkili oldukları Tablo 4’ de belirtilmişti. Bu durumda bu çalışma Sniffing ve DoS saldırılarına karşı güvenlidir fakat diğer saldırılar için gerekli önlemler alınmamıştır.

4.3.1.2. Çalışmaların Almış Oldukları Önlemler

Tablo 4.4: Önceki Çalışmaların Almış Oldukları Önlemler.

Çalışma	Alınan Önlemler
(Quinlan, 2013)	Tuş kombinasyonu,Simetrik ve Asimerik Şifreleme
(Michael Roland, 2011)	Simetrik ve Asimetrik Şifreleme,İmzalama
(Deepa S Pillai, 2014)	Sayısal İmzalama
(Suman Chaudhary, 2014)	Kullanıcı Login, Bloke , NDEF Şifreleme,Secure Element
(Helena Rodrigues, 2014)	Kullanıcı Login,Bulut yapısı,Asimetrik Şifreleme
(Chang, 2014)	Kullanıcı Login,SSL,IMEI,Simetrik Şireleme,Web Servis
(Pardis Pourghomi, 2014)	Bulut,Secure Element,Login,Sayısal imza,Asimetrik Şifreleme
(Wei, 2013)	Simetrik Şifreleme,
(Urien, 2015)	Kullanıcı Login

Çalışmamız boyunca gerek kendi tezimizle karşılaştırmak gerekse incelemek üzere dokuz adet çalışma incelenmiştir. Yukarıdaki tabloda 9 çalışmanın her birinin almış oldukları güvenlik önlemleri listelenmiştir.

4.3.2. Performans Karşılaştırmaları

Karşılaştırma yapacağımız her bir çalışmanın aldığı önlemlerin bizim çalışmamızdaki zaman maliyetlerine göre toplam sürelerden farkları alınarak hesaplamalar yapılmıştır. Örneğin; bizim sistemimizin toplam çalışma süresi 100 sn olsun ve A güvenlik önleminin bizdeki maliyeti 10 sn olsun, diğer çalışmalardan A güvenlik önlemini almayanın 90 sn de işlem yapacağı düşünülmüştür. Farklı uygulamaların çalışma sürelerini bilmediğimizden çekirdek uygulama bizim uygulamamız gibi düşünülecektir ve ilgili makalede olmayan özellik bizim çalışmamızda olmasaydı çıkacak sonuç gibi değerlendirilecektir. Bu analizin neticesinde güvenlik karşılaştırması yapılan 10 tane çalışmanın performans karşılaştırmaları da yapılmış olacaktır.

Tablo 4.5: Önceki Çalışmalar Performans Tahminleri.

Çalışma	Çalışma Süresi (Nanosaniye)	Performans Kazanç Farkı (Yüzde)
(Quinlan, 2013)	282482979	19,1208
(Michael Roland, 2011)	287448172	17,0632
(Deepa S Pillai, 2014)	282482979	19,1208
(Suman Chaudhary, 2014)	246327387	36,6052
(Helena Rodrigues, 2014)	260086182	29,3787
(Chang, 2014)	260086182	29,3787
(Pardis Pourghomi, 2014)	260086182	29,3787
(Wei, 2013)	282482979	19,1208
(Urien, 2015)	282482979	19,1208
HİBRİT MODEL	336496044	0,0000

5. TARTIŞMA VE SONUÇ

Bu tezde NFC teknolojisi kullanılarak güvenli ve sanal alışveriş sistemi geliştirilmiştir, NFC teknolojisinin yeni nesil bir teknoloji olması ve mobil cihazlarda artık entegre olarak bu teknolojinin üretiliyor olması birçok çalışmada geliştiriciler için tercih sebebi olmaktadır. NFC tabanlı sanal alışveriş sistemlerinin en önemli sorunu güvenliği sorunsuz olarak sağlayabilmektir. Özellikle ödeme sistemlerinde alıcı ve satıcıların her ikisinin de kötü niyetli olma ihtimali söz konusudur. Riskin bu şekilde yüksek olması bu yönde yapılan çalışmalarda güvenlik konusunda ayrıca çalışmalar yapmayı gerektirmiştir.

Literatürde NFC tabanlı geliştirilen veya geliştirilmesi muhtemel sistemler için çeşitli çözüm önerileri ve analizler yapılmıştır. Literatürde yapmış olduğumuz araştırmalar neticesinde öncelikli olarak NFC tabanlı sistemlerin maruz kaldığı 6 adet saldırı türü tespit edilmiştir. Bu saldırı türleri;

- Dinleme
- Aldatma
- Paket Değiştirme
- Tekrarlı Saldırılar
- Hizmet Durdurma
- Ortadaki Adam

Tespit edilen saldırı türleri tezimizin önceki kısımlarında detaylıca işlenmiştir. Bu saldırı türlerine karşı gerekli önlemleri almış olan sistemlerin, güvenli olduğu kabul edilebilir. Geliştirmiş olduğumuz sistemde tespit etmiş olduğumuz 6 farklı saldırı türüne karşı 10 adet güvenlik tedbiri alınmıştır. Almış olduğumuz güvenlik tedbirleri bu saldırı türlerine karşı etkili çözümler sunmuştur. Çalışmamızın bulgular kısmında güvenlik önlemlerinin her birinin hangi saldırı türüne karşı etkili olduğu detaylıca işlenmiştir. Güvenlik önlemlerinin bir kısmı birden fazla saldırıyı önleyebiliyorken bazı saldırı türlerinden korunmanın yolu birden fazla güvenlik önlemimizin kullanılıyor olmasını gerektiriyor.

Almış olduğumuz güvenlik önlemlerini şöyle sıralayabiliriz;

- Kullanıcı Şifreli Giriş Şartı
- Yalıtkan Ortam Tasarımı Önerisi
- İki Taraflı Aktif Cihaz Kullanımı
- NDEF AES Simetrik Şifreleme
- SSL Tabanlı ve Yetkili Web Servis
- Şifreli Veri Saklama
- Kullanıcı Şifresinin Bulut Ortamında Saklanması
- Mesaj Formatı
- Kara Liste Tuş Kombinasyonu

Literatürde yapmış olduğumuz araştırmalarda NFC tabanlı güvenli sistem önerileri ve çalışmaları incelenmiştir. Bu araştırmalar neticesinde daha önce yapılmış 9 adet çalışmaya ayrıca ilgi duyulmuştur. Özellikle üzerinde çalışmış olduğumuz 9 çalışmanın ortak özellikleri şöyledir;

- NFC Tabanlı Haberleşme Yapılıyor Olması
- NFC Tabanlı Haberleşmeye Yönelik Geliştirilen Saldırı Türleri ile İlgili Çalışma Yapılıyor Olması
- Bahsi Geçen Saldırı Türlerine Karşı Güvenlik Önerilerinin ve Çalışmalarının Yapılıyor Olması

Yukarıdaki özellikleri barındıran 9 adet çalışma tespit edilmiştir ve bu çalışmaların her birinin hangi güvenlik önlemlerini aldıklarını ve hangi saldırı türlerine karşı güvenli oldukları tezimizin Bulgular kısmında detaylıca anlatıldığı üzere tespit edilmiştir.

Tezimiz geliştirilirken seçmiş olduğumuz 9 çalışmanın eksikleri tespit edilmiş ve incelemiş olduğumuz 6 saldırı türüne karşı almış olduğumuz 10 adet güvenlik önlemi türü geliştirilerek ortaya Hibrit bir model koyulmuştur. Literatürdeki çalışmalarda bütün bu güvenlik önlemlerinin bir arada bulunduğu bir sanal ödeme modeli bulunmadığından, bu alandaki eksiklik uygulanmış bir sistem ortaya koyularak ve gerekli performans ölçümleri yapılarak ortaya koyulmuştur.

Geliştirmiş olduğumuz sistem, güvenlik önlemleri sırasıyla devreden çıkarılarak sistemin toplam zaman maliyeti tespit edilerek aslında her bir güvenlik önleminin sisteme maliyeti hesaplanmıştır.

Saldırı türlerine karşı alınması gereken güvenlik önlemleri tespit edildiğinden ve güvenlik önlemlerinin zaman maliyetleri hesaplandığından saldırı türlerinin ayrı ayrı önlenmesi için gerekli olan zaman maliyetleri de hesaplanmıştır.

Literatürde ki araştırmalar sonucunda tercih etmiş olduğumuz 9 çalışmanın her birinin almış olduğu güvenlik önlemlerini tespit etmiştik ve her bir güvenlik önleminin zaman maliyetini de hesaplamıştık bu bilgilerden yola çıkarak gerekli hesaplamalar yapılarak bu 9 çalışmanın toplam çalışma zamanları bizim geliştirmiş olduğumuz sisteme uyarlanarak hesaplanmıştır. Geliştirmiş olduğumuz hibrit modelin de çalışma süreleri hesaplandığından bu çalışmalar ile bizim çalışmamız performans metrikleri bakımından karşılaştırılarak incelenebilmiştir. Bütün bu tespitler neticesinde performans ve güvenlik anlamında birçok sonuçlar tespit edilmiştir.

Bu sonuçlara göre sistemimizin, başından beri incelenen saldırı türlerine karşı güvenli olduğu görülmüştür. İncelenen diğer çalışmalar birçok konuda güvenlik sağlamışlarsa da bu saldırı türlerinin tümüne karşı güvenlik sağlanmamıştır. Geliştirmiş olduğumuz Hibrit modelin önceki çalışmalara nispeten daha güvenli olduğunu fakat performans açısından daha iyi olduğunu söyleyemeyiz.

Çalışmamız çerçevesinde almış olduğumuz güvenlik tedbirleri detaylıca işlenmiştir ve saldırı türleri ile olan ilişkileri de ayrıca belirtilmiştir. Geliştirmiş olduğumuz sistemin farklı saldırı senaryoları göz önünde bulundurulduğunda ve adım adım uygulandığında güvenli olduğu görülmüştür. Sistemimizi güvenli kılmak için aldığımız önlemlerin her biri sistem üzerinde ayrı ayrı zaman maliyetlerine yol açmaktadır. Bu maliyetler sistemin güvenliğine katkı sunmakla birlikte performansı olumsuz yönde etkilemiştir fakat bizim tezimizin amacı öncelikli olarak güvenli bir ödeme sistemi geliştirmek olduğundan çalışmalarımız bu şekilde ilerlemiştir.

Sistemimizin performansının iyileştirilmesi için çalışmalar yapılabileceği gibi güvenlik ile ilgili de bazı çalışmalar yapılabilir. Geliştirmiş olduğumuz sistem, Android işletim sistemi tabanlı mobil bir uygulama olduğundan işletim sisteminin ve mobil cihazın mevcut bütün açıklarına ve saldırılarına muhataptır. Bu ödeme sistemi mobil uygulamadan bağımsız olarak işletim sistemi ve donanımsal olarak tasarlanabilir. Tamamen bu çalışmaya yönelik özel bir işletim sistemi geliştirilerek veya bu çalışmaya

özel elektronik devre tasarımları yapılarak uygun donanımlar oluşturularak açıklardan ve saldırılardan uzak bir sistem tasarlanabilir.

Geliştirmiş olduğumuz sistemin performans alanındaki tedbirleri bulunmaktadır fakat önceliğimiz güvenli bir sistem geliştirmek olduğundan performans kısmı ile detaylı çalışmalar ve analizler yapılmamıştır. Önümüzdeki çalışmalarda güvenlik olarak bu önerilen mimari kullanılarak geliştirilecek sistemde performans konusuna öncelik verilerek hem bu kadar güvenli hem de daha performanslı modeller üzerinde mesai harcanabilir.

KAYNAKLAR

Bank For International Settlements, W. P. (1996). *Implications For Central Banks of The Development of Electronic Money.*

Chang, T.-K. (2014). *A Secure Operational Model for Mobile Payments.*

Deepa S Pillai, S. (2014). *Prevention of Relay Attack Using NFC.*

Destot, M. (2009). *Several NFC initiatives in Europe, Forum des services mobiles sans contact-Mobile Contactless Services Forum Bülteni.*

Destot, M. (2009). *Several NFC initiatives in Europe, Forum des services mobiles sans contact-Mobile Contactless Services. .*

Doğan, A. H. (2006). *2006: "AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı", İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Türkiye.*

Fips, 1. (tarih yok). *2001: Advanced Encryption Standard. National Institute of Standarts and Technology (NIST).*

Halife Kodaz, F. M. (2010). *Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması.*

Helena Rodrigues, R. J. (2014). *MobiPag: Integrated Mobile Payment, Ticketing and Couponing Solution Based on NFC.*

Kabakçı, F. (2013). *NFC Mobil Ödeme Sistemi.*

Kula, Ç. (tarih yok). *Gelişmiş Şifreleme Standardı Blok Şifreleme Algoritmasının Bir Mikroişlemci Üzerinde Gerçeklenmesi Yan Kanal Saldırısı.*

Michael Roland, J. L. (2011). *Security Vulnerabilities of the NDEF Signature.*

Özdemir, S. (2011). *Yakin Alan Haberlesmesi Teknolojisi Kullanilarak Bir Uygulama Gerceklestirilmesi.*

Özdemir, S. (tarih yok). *Yakın alan haberleşmesi.*

Pardis Pourghomi, M. Q. (2014). *A Secure Cloud-Based Nfc Mobile Payment Protocol.*

Passeri, P. (2016). *http://www.hackmageddon.com/2016/04/21/march-2016-cyber-attacks-statistics/.*

Quinlan, M. (2013). NFC Security On Android Devices. *NFC Security On Android Devices*.

Shen, S. (2012). *Forecast: Mobile payment, Worldwide.*

Suman Chaudhary, N. G. (2014). *Multi Level Security Architecture For NFC Enabled Car Keys.*

Urien, P. (2015). *EMV-TLS, a Secure Payment Protocol For NFC Enabled Mobiles.*

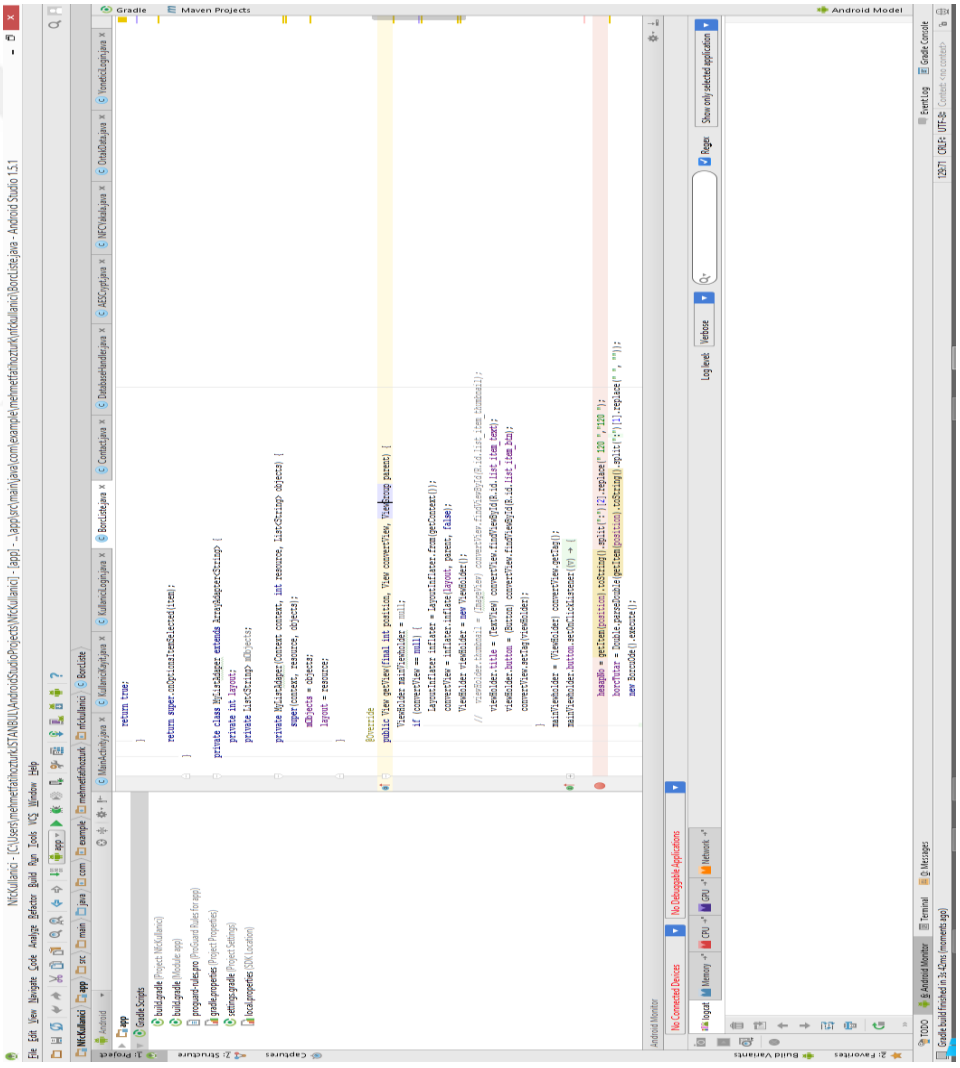
Vural, A. P. (2006). *A Report On Block Ciphersonal Aerospace Laboratories.*

Wei, X. M. (2013). *The Architecture of Mobile Wallet System Based on NFC (Near Field Communication).*

EKLER

EK 1.

Mobil uygulamaların geliştirildiği ortam olan “Android Studio” uygulamasına ait ekran görüntüsü aşağıdadır.



EK 2.

Web uygulamalarının geliştirildiği ortam olan “Visual Studio 2012” uygulamasına ait ekran görüntüsü aşağıdadır.

EK 3.

NWY ile bulut ortamına anahtar gönderimi için kullanılan c# kodu. Bu kaynak kodlar vasıtası ile haberleşme anında AES şifrelemede kullanılan anahtarların uçlar arasında iletilmesi sağlanmaktadır.

```
[WebMethod]
public string OturumIcinAnahtariKaydet(string imei, string privateKey, string funcPass)
{
    try
    {
        if (funcPass == GenelParametre.NFCWebServisFonksiyonSifresi)
        {
            if (imei.Trim() != "" && privateKey.Trim() != "")
            {
                VeritabaniIslemleri veritabaniIslemleri = new VeritabaniIslemleri();
                veritabaniIslemleri.Baslat(VeritabaniIslemleri.IslemTip.BAGLI);
                NfcOturumlar nfcOturumlar = new NfcOturumlar(veritabaniIslemleri);
                nfcOturumlar.Imei = imei;
                nfcOturumlar.Private_key = privateKey;
                if (nfcOturumlar.Ekle())
                {
                    int nfcSessionId = nfcOturumlar.MaxIdGetir();
                    if (nfcSessionId > 0)
                    {
                        veritabaniIslemleri.Uygula();
                        veritabaniIslemleri.Bitir();
                        return "0:" + nfcSessionId.ToString();
                    }
                    else
                    {
                        veritabaniIslemleri.GeriAl();
                        veritabaniIslemleri.Bitir();
                        return "5:ANAHTAR OLUŞMADI";
                    }
                }
                else
                {
                    veritabaniIslemleri.GeriAl();
                    veritabaniIslemleri.Bitir();
                    return "4:ANAHTAR KAYDEDILEMIYOR";
                }

            }
            else
            {
                return "3:EKSIK BILGI";
            }
        }
        else
        {
            return "2:YETKISIZ";
        }
    }
    catch
    {
        return "1:BILINMEYEN HATA";
    }
```

EK 4.

NWY ile bulut ortamına anahtar gönderimi kaynak kodları için kullanılan c# kodları.

```
[WebMethod]
public string OturumAnahtariniAl(string guid, string funcPass)
{
    try
    {
        if (funcPass == GenelParametre.NFCWebServisFonksiyonSifresi)
        {
            int gu_id = Convert.ToInt32(guid);
            if (gu_id > 0)
            {
                VeritabaniIslemleri veritabaniIslemleri = new VeritabaniIslemleri();
                veritabaniIslemleri.Baslat(VeritabaniIslemleri.IslemTip.BAGIMSIZ);
                NfcOturumlar nfcOturumlar = new NfcOturumlar(veritabaniIslemleri);
                nfcOturumlar.Id = gu_id;
                if (nfcOturumlar.Doldur())
                {
                    if (nfcOturumlar.Private_key.Trim() != "")
                    {
                        veritabaniIslemleri.Bitir();
                        return "0:" + nfcOturumlar.Private_key.Trim();
                    }
                    else
                    {
                        veritabaniIslemleri.Bitir();
                        return "5:ANAHTAR SORUNLU";
                    }
                }
                else
                {
                    veritabaniIslemleri.Bitir();
                    return "4:ANAHTAR BULUNAMADI";
                }

            }
            else
            {
                return "3:EKSIK BILGI";
            }
        }
        else
        {
            return "2:YETKISIZ";
        }
    }
    catch
    {
        return "1:BILINMEYEN HATA";
    }
}
```

EK 5.

NWY ile bulut ortamından anahtar temini için kullanılan java kaynak kodları.

```
public AESCrypt(String password) {
    try {
        // hash password with SHA-256 and crop the output to 128-bit for key
        MessageDigest digest = MessageDigest.getInstance("SHA-256");
        digest.update(password.getBytes("UTF-8"));
        byte[] keyBytes = new byte[32];
        System.arraycopy(digest.digest(), 0, keyBytes, 0, keyBytes.length);

        cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
        key = new SecretKeySpec(keyBytes, "AES");
        spec = getIV();
    } catch (Exception ex)
    {
    }
}
```

```
public AESCrypt(String password) {
    try {
        // hash password with SHA-256 and crop the output to 128-bit for key
        MessageDigest digest = MessageDigest.getInstance("SHA-256");
        digest.update(password.getBytes("UTF-8"));
        byte[] keyBytes = new byte[32];
        System.arraycopy(digest.digest(), 0, keyBytes, 0, keyBytes.length);

        cipher = Cipher.getInstance("AES/CBC/PKCS7Padding");
        key = new SecretKeySpec(keyBytes, "AES");
        spec = getIV();
    } catch (Exception ex)
    {
    }
}
```

```
public String decrypt(String cryptedText) {
    try {
        cipher.init(Cipher.DECRYPT_MODE, key, spec);
        byte[] bytes = Base64.decode(cryptedText, Base64.DEFAULT);
        byte[] decrypted = cipher.doFinal(bytes);
        String decryptedText = new String(decrypted, "UTF-8");

        return decryptedText;
    } catch (Exception ex) {
        return "";
    }
}
```

```
public class OrtakData {
    static public String WebServisSifre="12345678";
    static  public String WebServisNAMESPACE="http://nfc.referansyonetim.com/";
    static public String WebServisURL = "http://nfc.referansyonetim.com/Service1.asmx";


}
```

EK 6.

NFC haberleşmesinde okuma/yazma işlemlerini yapmak üzere kullanılan java kodları.

```
public class NFCYakala extends Activity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_nfcyakala);
    }
    @Override
    protected void onResume(){
        super.onResume();
        Intent intent = getIntent();
        if (NfcAdapter.ACTION_NDEF_DISCOVERED.equals(intent.getAction())) {
            Parcelable[] rawMessages = intent.getParcelableArrayExtra(NfcAdapter.EXTRA_NDEF_MESSAGES);

            NdefMessage message = (NdefMessage) rawMessages[0]; // only one message transferred
            String mesaj = new String(message.getRecords()[0].getPayload());

            Intent i = new Intent(NFCYakala.this,IslemActvity.class).putExtra("DEGER",mesaj);
            startActivity(i);
        }
        else {

            //mTextView.setText("Waiting for NDEF Message");
        }
    }
}
```

```
public class NFCYolla extends Activity implements NfcAdapter.CreateNdefMessageCallback,NfcAdapter.OnNdefPushCompleteCallback {

    String GELENCEVAP="";
    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_nfcyolla);

        GELENCEVAP= getIntent().getStringExtra("DEGER");

        NfcAdapter mAdapter = NfcAdapter.getDefaultAdapter(this);
        if (mAdapter == null) {
            return;
        }

        if (!mAdapter.isEnabled()) {
            Toast.makeText(this, "NFC Özelliğini Aktif Edin", Toast.LENGTH_LONG).show();
        }

        mAdapter.setNdefPushMessageCallback(this, this);
    }

    @Override
    public NdefMessage createNdefMessage(NfcEvent nfcEvent) {
        String message = GELENCEVAP;
        NdefRecord ndefRecord = NdefRecord.createMime("text/plain", message.getBytes());
        NdefMessage ndefMessage = new NdefMessage(ndefRecord);
        return ndefMessage;
    }

    @Override
    public void onNdefPushComplete(NfcEvent event) {
        Intent i = new Intent(NFCYolla.this,MainActivity.class);
        startActivity(i);
    }
}
```

ÖZGEÇMİŞ

Kişisel Bilgiler	
Adı Soyadı	Mehmet Fatih ÖZTÜRK
Doğum Yeri	Eleşkirt
Doğum Tarihi	20.04.1988
Uyruğu	☑ T.C. ❒ Diğer:
Telefon	0 507 533 72 04
E-Posta Adresi	mfozturk04@gmail.com

Eğitim Bilgileri	
Lisans	
Üniversite	Sakarya Üniversitesi
Fakülte	Mühendislik Fakültesi
Bölümü	Bilgisayar Mühendisliği
Mezuniyet Yılı	09.06.2005

Yüksek Lisans	
Üniversite	İstanbul Üniversitesi
Enstitü Adı	Fen Bilimleri Enstitüsü
Anabilim Dalı	Bilgisayar Mühendisliği Anabilim Dalı
Programı	Bilgisayar Mühendisliği Programı
Mezuniyet Tarihi	01.07.2016