2nd International Conference on Cyber Security and Digital Forensics (ICONSEC) 2022

PROCEEDINGS BOOKS

COMMITTEES

Honorary Board

- Prof. Dr. Hüseyin ÇİÇEK (Muğla Sıtkı Koçman University)
- Prof. Dr. Mehmet BAHÇEKAPILI (Yalova University)
- Prof. Dr. A. Ercan GEGEZ (Istanbul Arel University)

Conference Chair

- Prof. Dr. Murat GÖK (Yalova University)

Organizing Committee

- Assist. Prof. İrfan KÖSESOY (Kocaeli University)
- Emre SADIKOĞLU (Yalova University)
- Emine CENGİZ (Yalova University)
- Hasibe CANDAN (Yalova University)
- Fatih BULDUR (Yalova University)

Scientific Committee

- Prof. Dr. Ayhan İSTANBULLU (Balıkesir University)
- Prof. Dr. Ecir Uğur KÜÇÜKSİLLE (Süleyman Demirel University)
- Prof. Dr. Müfit ÇETİN (Yalova University)
- Prof. Dr. Ramazan BAYINDIR (Gazi University)
- Prof. Dr. Naci GENÇ (Yalova University)
- Prof. Dr. Engin AVCI (Fırat University)
- Prof. Dr. Yıldıray YALMAN (Piri Reis University)
- Prof. Dr. Resul DAŞ (Fırat University)
- Prof. Dr. Abdül Halim ZAİM (İstanbul Commerce University)
- Prof. Dr. Ahmet Bedri ÖZER (Fırat University)
- Prof. Dr. Ahmet ZENGİN (Sakarya University)
- Prof. Dr. Atilla ELÇİ (Hasan Kalyoncu University)
- Prof. Dr. Muharrem Tolga SAKALLI (Trakya University)
- Assoc. Prof. Dr. Bilgin METIN (Bogazici University)
- Assoc. Prof. Dr. Abdülkadir TEPECIK (Yalova University)
- Assoc. Prof. Dr. Ahmet KOLTUKSUZ (Yaşar University)
- Assoc. Prof. Dr. Derya AVCI (Fırat University)
- Assoc. Prof. Dr. Sunay TÜRKDOĞAN (Yalova University)
- Assoc. Prof. Dr. Fatih ERTAM (Fırat University)
- Assoc. Prof. Dr. Güzin ULUTAŞ (Karadeniz Technical University)
- Assoc. Prof. Dr. Muhammed Ali AYDIN (İstanbul University)
- Assoc. Prof. Dr. Serdar SOLAK (Kocaeli University)

- Assoc. Prof. Dr. Bünyamin CİYLAN (Gazi University)
- Assoc. Prof. Dr. Ercan BULUŞ (Tekirdağ Namık Kemal University)
- Assoc. Prof. Dr. Sedat AKLEYLEK (Ondokuz Mayıs University)
- Assoc. Prof. Dr. Fatih ÖZKAYNAK (Fırat University)
- Assoc. Prof. Dr. Murat ARICI (Selçuk University)
- Assist. Prof. Dr. Mert ÖZARAR (HAVELSAN Cyber Security Director / Ankara Science University)
- Assist. Prof. Dr. Adem TUNCER (Yalova University)
- Assist. Prof. Dr. Bülent TUĞRUL (Ankara University)
- Assist. Prof. Dr. Burcu DEMIRELLI OKKALIOĞLU (Yalova University)
- Assist. Prof. Dr. Meltem KURT PEHLIVANOĞLU (Kocaeli University)
- Assist. Prof. Dr. Murat AK (Akdeniz University)
- Assist. Prof. Dr. Murat KARAKUŞ (Bayburt University)
- Assist. Prof. Dr. Güneş HARMAN (Yalova University)
- Assist. Prof. Dr. Önder ŞAHINASLAN (Maltepe University)
- Assist. Prof. Dr. Erhan AKBAL (Fırat University)
- Assist. Prof. Dr. Ali DURDU (Social Sciences University of Ankara)
- Assist. Prof. Dr. Murat OKKALIOĞLU (Yalova University)
- Assist. Prof. Dr. Ömer AYDIN (Manisa Celal Bayar University)
- Assist. Prof. Dr. Ömer Özgür BOZKURT (Turkish National Defense University)
- Assist. Prof. Dr. Osman Hilmi KOÇAL (Yalova University)
- Assist. Prof. Dr. Faruk BULUT (Istanbul Rumeli University)
- Assist. Prof. Dr. Süleyman UZUN (Sakarya University of Applied Sciences)
- Assist. Prof. Dr. Şebnem ÖZDEMIR (Beykent University)
- Assist. Prof. Dr. Mustafa COŞAR (Hitit University)
- Assist. Prof. Dr. Tarık YERLIKAYA (Trakya University)
- Assist. Prof. Dr. Yunus ÖZEN (Yalova University)
- Assist. Prof. Dr. Kevser OVAZ AKPINAR (Sakarya University)
- Assist. Prof. Dr. Esra N. YOLAÇAN (Eskişehir Osmangazi University)
- Assist. Prof. Dr. Mustafa Cem KASAPBAŞI (İstanbul Commerce University)
- Assist. Prof. Dr. Fatma BÜYÜKSARAÇOĞLU SAKALLI (Trakya University)
- Assist. Prof. Dr. Atila BOSTAN (Ankara Science University)
- Assist. Prof. Dr. Andaç MESUT (Trakya University)
- Assist. Prof. Dr. Burcu YILMAZEL (Eskişehir Technical University)
- Assist. Prof. Dr. Mehmet Tahir SANDIKKAYA (Istanbul Technical University)
- Assist. Prof. Dr. Alpay DORUK (Bandırma University)
- Assist. Prof. Dr. Özgür Can TURNA (Istanbul University-Cerrahpaşa)
- Assist. Prof. Dr. Mustafa KAYA (Fırat University)
- Dr. Galip Savaş İLGİ (Near East University)
- Dr. Ahmet Ali SÜZEN (Isparta University of Applied Sciences)
- Dr. Mehmet Yavuz YAĞCI (Istanbul University)
- Dr. Remzi GÜRFİDAN (Isparta University of Applied Sciences)
- Dr. Emre Cihan ATEŞ (Gendarmerie and Coast Guard Academy)

- Dr. Ömer ASLAN (Siirt University)
- Dr. Faruk Süleyman BERBER (Süleyman Demirel University)
- Dr. Yunus KORKMAZ (Dicle University)
- Dr. Semih ÇAKIR (Zonguldak Bülent Ecevit University)
- Dr. Kerem GENCER (Karamanoğlu MehmetBey University)
- Dr. Çiğdem BAKIR (Erzincan Binali Yıldırım University)
- Dr. Gülsüm AKKUZU KAYA (Recep Tayyip Erdoğan University)
- Dr. Ahmet KARAKÜÇÜK (Uludağ University)
- Dr. Ömer DURMUŞ (Samsun University)
- Dr. Oğuzhan KENDİRLİ (Düzce University)
- Dr. Duygu Sinanç TERZİ (Amasya University)
- Dr. Mehmet Mehdi KARAKOÇ (Ağrı University)
- Dr. Kerime Dilşad ÇİÇEK (Ayvansaray University)
- Dr. Sultan ZAVRAK (Düzce University)
- Dr. Maad M. MIJWIL (Baghdad College of Economic Sciences University)
- Esra SÖĞÜT (Gazi University)

CONTENTS

2nd International Conference on Cyber Security and Digital Forensics (ICONSEC) 2022

PROCEEDINGS BOOKS

Volume 1

ABSTRACT BOOK

Determination of Software Vulnerabilities with Deep Neural Networks: Literature Review

Gözde Mihran Altınsoy[1]*, İrfan Kösesoy[2],

[1]*Beykoz Üniversitesi, Bilgisayar Teknolojileri Bölümü, Bilgisayar Programcılığı, İstanbul, TÜRKİYE*

[2]*Kocaeli Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği, Kocaeli, TÜRKİYE*

Abstract

The use of software and information systems is increasing day by day. The development of software systems has brought with it security vulnerabilities. Software vulnerability can be defined as a weakness in the information system, system security procedures, internal controls, or application that a threat source can exploit. Existing software vulnerabilities have been determined by the experts on current systems. New ones are constantly added to the identified vulnerabilities. The number of vulnerabilities recorded in the NIST National Vulnerability Database was 14.500 in 2017, however, in 2021 this amount increased to 20.000. Determination of software vulnerabilities at the very beginning of the development process saves both time and cost compared to the further steps. If security vulnerabilities that occur during software development are transferred to further processes, the solution gets complicated and costly. Thus, it is important to determine software vulnerabilities at the coding stage. Studies in this area are divided into two: detecting known types of vulnerabilities (static analysis) or discovering new vulnerabilities. In recent years, deep learning algorithms have been successfully applied to image processing and natural language processing problems, and have also been used to detect security vulnerabilities in codes. In this study, recent studies in this field in the literature are reviewed.

Keywords: *Deep Learning, Vulnerability Detection, Code Inspection, Static Code Analysis, Software Security*

* İletişim e-posta: gmihran@gmail.com

Protection of Internet Information Services Logs with OWASP Principles

Ahmet TOPRAK[1]*,

[1]*Istanbul Commerce University, Computer Engineering, Istanbul, TURKEY*

Abstract

Considering the increasing data volume in digital environments, information security has become an increasingly important element with each passing day. In an environment where data is so dense, secure access is as important as fast access to data. The system must not allow access by unauthorized users and constantly be on the alert against attacks. Especially for institutions operating in the finance and banking sectors, the control and security of unauthorized access are even more important due to the magnitude of financial losses. In this study, structural emphasis has been made to protect and store client logs on Internet Information Services, a Windows-based server, within the framework of OWASP principles. The integration of OWASP principles has been mentioned at the point of hiding important user logs (password, account, etc.) in Internet Information Services logs, controlling user privileges, and processing user logs. In the study, both OWASP Top 10 principles and Internet Information Services architecture are discussed in detail. This study will also be a reference source for systems integrated with different technology to ensure web server security.

Keywords: *Internet Information Server, Information Security, Log Analysis, OWASP, Privacy, Security, Web Server Security*

* İletişim e-posta: ahmetoprak190363@gmail.com

An Approach to JSON Web Token-Based Client Authentication

Ahmet TOPRAK[1]*,

[1]*Istanbul Commerce University, Computer Engineering, Istanbul, TURKEY*

Abstract

Internet-based applications are widely used today. With the widespread use of the Internet, the use of web services and mobile applications has increased at the same level. The intense use of mobile resources necessitated the inclusion of some security-related issues on the agenda. Security vulnerabilities, especially in applications such as e-commerce and banking, cause huge financial losses. Therefore, in almost any organization where user-sensitive data exists, the security and privacy of data play a vital role. In this study, the gains to be obtained at the point of performing client verifications with JSON Web Token-based security methods are structurally discussed. A client-based web application has been developed to evaluate the proposed system. First of all, when the user makes the first request to the system, a JSON Web Token paired with the user's session information is generated. Then, all requests sent by the user from the frontend layer are validated with this JSON Web Token. If the JSON Web Token sent by the user is valid, server-side requests are allowed and user requests are forwarded to the IIS-based web server. In this way, web security vulnerabilities are prevented. In this study, the JSON Web Token structure is implemented with the working logic and real-life application of best practices. It is thought that this study will be very beneficial for web application designs and client-based validation studies.

Keywords: *JSON Web Token, Authentication, Session Cookie, Security, Privacy*

* İletişim e-posta: ahmetoprak190363@gmail.com

Multi Purpose Security Analysis of Software Projects Against Cyber Threats and Development of Security Scoring Algorithms

Abdulkadir ŞEKER[1]*, Halil ARSLAN[2], Emre DELİBAŞ[3], Hakan KEKÜL

[1,2,3]Sivas Cumhuriyet University, Computer Engineering, Sivas, TURKEY
[3]Fırat University, Computer Engineering, Elazığ, TURKEY

Abstract

In recent years, it is known that as a result of cyber-attacks, people and even governments confront serious problems, especially loss of reputation or financial losses. Various security software is used to prevent these cyber-attacks. Apart from these, ensuring the security of the software used will provide a critical defense mechanism as it will directly prevent security vulnerabilities that will cause attacks.

Today, software projects have become complex systems consisting of many modules serving different purposes. These systems are developed with the distributed software development method, which has become more widespread especially after the pandemic we are living in. Also, while developing projects, instead of developing code from scratch, open-source software or code snippets hosted on various platforms such as GitHub, StackOverFlow, etc. are used. While all these development strategies allow projects to grow faster, they also bring with them a wide variety of security problems. At this stage, secure software development, which is a precautionary mechanism against cyber-attacks, comes into play.

There are various security and quality tools in the literature that analyze different subcomponents of software. These tools generally report security vulnerabilities and problems in the project. In this paper, a novel framework will be proposed that will conduct comprehensive security analyzes of all components of a software project, including the source code, the third-party components it uses, and the binary files it contains. In addition, software security scores will be produced for the project related to the original algorithms we will develop from the data obtained as a result of the analysis. In this way, a comprehensive report on a software project passed through the framework we propose and a security score that will show how safe the project is for use will be produced. Developers will be able to decide on the security of their own software or the software they want to integrate into their projects according to the results of this framework. In this way, pecuniary or nonpecuniary losses will be prevented by developing software that does not contain security vulnerabilities that will lead up to cyber-attacks.

Keywords: *Cybersecurity, Open source software, Security of software, Vulnerability analysis, Secure coding.*

* İletişim e-posta: aseker@cumhuriyet.edu.tr

2nd International Conference on Cyber Security and Digital Forensics (ICONSEC) 2022

PROCEEDINGS BOOKS

Volume 2

FULLTEXT BOOK

Türkiye Rekabet Kurumu'nun Yerinde İncelemelerde Dijital Verilerin İncelenmesine İlişkin Yöntem Önerileri

İsmail Sinan TATLGİL[1]*, Erkan BOLAT[2], Dr. Erdal GÜVENOĞLU[3]

[1]*Volfram Bilgi Teknolojileri, İstanbul, TÜRKİYE*
[2]*SİSAMER, İstanbul, TÜRKİYE*
[3]*Maltepe Üniversitesi, Bilgisayar Mühendisliği, İstanbul, TÜRKİYE*

Özet

Rekabet Kurumu'nun son dönemlerde yapmış olduğu rekabet incelemelerinde, teknoloji tabanlı sistemler olan teşebbüste (Şirkette) ve/veya dışında kullanılan bilişim, mobil ve bulut sistemlerin kullanımına ilişkin incelemeler gerçekleştirmektedir. Buna ilişkin kılavuz yayınlanmasına karşın tartışmalar sürmekte olup, teşebbüsler ile kurum karşı karşıya gelmektedir. Tartışmalar kanunlar, özel hayatın gizliliği ve bilişim sistemlerinin incelenmesine ilişkin yöntemler olarak üç ana başlıkta gerçekleşmektedir. Ancak bu üç ana başlığın temelinde yer alan ana tartışma teşebbüs çalışanlarının kullanmış olduğu bilişim cihazlarının incelenip incelenemeyeceği üzerine yoğunlaşmaktadır. Burada da cihazların sahipliğinin teşebbüse mi yoksa kişinin kendisine mi ait olduğu üzerine yoğunlaşmaktadır. Bu çalışmada, günümüzde uygulanan adli bilişim yöntemleriyle birlikte, uluslararası standartlar ve kanunlarla birlikte kişilere ait cihazların tespiti, hızlı gözden geçirme, adli inceleme ve makul süreler mütalaa edilerek yöntem önerileri sunulmaktadır.

Anahtar Kelimeler: *Mobil İnceleme, Adli Bilişim, Siber Güvenlik, Rekabet, Rekabet Kurumu, Yerinde İnceleme*

Turkish Competition Authority's Methodology Recommendations Regarding the Investigation of Digital Data in On-Site Inspections

Abstract

In the competition examinations that the Competition Authority has made recently, it carries out examinations on the use of technology-based systems, informatics, mobile and cloud systems used in and/or outside the enterprise (Company). Despite the publication of a guide on this issue, discussions are still ongoing, and the enterprises and the institution come face to face. Discussions take place under three main headings as laws, privacy and methods of examining information systems. However, the main discussion underlying these three main topics focuses on whether the IT devices used by the employees of the enterprise can be examined or not. Here, too, it focuses on whether the ownership of the devices belongs to the enterprise or the person himself. In this study, along with the forensic methods applied today, together with international standards and laws, method suggestions are presented by considering the detection of personal devices, rapid review, forensic examination and reasonable periods.

Keywords: *Mobile Investigation, Digital Forensics, Cyber Security, Competition, Competition Authority, On-Site Inspection*

* İletişim e-posta: sinan.tatligil@volfram.com.tr

1 Giriş

Günümüz dijital teknolojisinin gelişmesi ile birlikte son yıllarda rekabet hukuku uygulamaları hızlı bir ivme kazanmıştır. Bu ivmelenme COVID-19 pandemisi nedeniyle daha da artmıştır. Klasik ticaretin dijital ticarete kayması buna örnek olarak verilebilir. Dolayısı ile sektörlerin çok ciddi bir çoğunluğunun dijitalleşmesi, geleneksel sektör sisteminde uygulanan sınırların yeniden çizilmesini gerekli kılmıştır. Bu doğrultuda Avrupa'da olduğu gibi ülkemizde de rekabet otoriteleri yeni sorunlara cevap verebilmek adına dijital sektörde rekabet hukuku üzerine çeşitli çalışmalar yürütmektedir [1]. Ülkemizde bu çalışmalar Rekabet Kurumu tarafından yürütülmektedir.

Dijital veriler, kurum tarafından herhangi bir şikâyet veya rekabet ihlalinin düşünüldüğü durumlarda incelenmektedir. Rekabet kurumu, dijital verilerin yerinde incelenmesi durumunda dikkat edilecek hususlara ilişkin bir kılavuz yayınlamıştır. 16.06.2020 tarih ve 7246 sayılı Kanun ile 4054 sayılı Rekabetin Korunması Hakkında Kanunun (Kanun) "Yerinde İnceleme" başlıklı 15. maddesinin birinci fıkrasının (a) bendinde önemli değişiklikler yapılmıştır. Bu değişiklikler çerçevesinde, teşebbüslerin elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerinin ve belgelerinin yerinde inceleme mahallinde incelenmesine ve/veya bunların kopyalarının alınarak Rekabet Kurumu merkezine getirilerek incelenmesine ve muhafazasına ilişkin genel esasların belirlenmesinde yarar görülmüştür [2]. Bu kılavuzda, kanunun 15. Maddesi uyarınca dijital verilerin incelenmesi süreçlerinde uygulanacak usullere yer verilmiştir.

Kılavuzun üçüncü maddesinde "Görevli Meslek Personeli (Rekabet Başuzmanı, Rekabet Uzmanı ve Rekabet Uzman Yardımcısı), teşebbüse (teşebbüslerin yanı sıra teşebbüs birliklerini de içermektedir) ait sunucu, masaüstü/dizüstü bilgisayar, taşınabilir cihaz gibi bilişim sistemleri ile CD, DVD, USB, harici hard disk, yedekleme kayıtları, bulut servisleri gibi depolama araçlarında inceleme yapmaya yetkilidir." denilmekte olup teşebbüse ait sistemlerin incelenmesine yetkili olduğu açıkça ifade edilmektedir. Kılavuzun dördüncü maddesinde ise "Taşınabilir iletişim cihazlarının (cep telefonu, tablet vb.) teşebbüse ait dijital veri içerip içermediğinin tespiti amacıyla yapılacak hızlı gözden geçirme sonucunda bu cihazların incelemeye tabi tutulup tutulmayacağına karar verilir. Tümüyle şahsi kullanıma özgü olduğu tespit edilen taşınabilir iletişim cihazları inceleme konusu yapılmaz." denilmektedir.

İlgili kılavuzda kişisel cihazların tespitiyle ilgili olarak hızlı gözden geçirmenin nasıl yapılacağına dair tartışmaya açık noktalar bulunmaktadır. Bu çalışmada, tartışmaya açık noktaları, illiyet bağı, ölçülülük ve adli bilişim yöntemleri değerlendirilerek ortadan kaldıran öneriler bulunmaktadır.

2 Materyal ve Yöntem

2.1 Kişisel Cihazın Teşebbüs ile İlliyet Bağı

Kılavuzda kişiye ait cihazın incelemeye tabi tutulup tutulamayacağına "hızlı gözden geçirme" sonucunda karar verileceği belirtilmiş olsa da "hızlı gözden geçirme" yöntem ve usulleri tanımlanmamaktadır. Bu nedenle T.C. Anayasasında Özel Hayatın Gizliliği [3], Ceza Muhakemesi Kanunu Makul Şüphe [4], Kişisel Verilerin Korunması [5] ve delillerin elde edilmesi [4] konuları gündeme gelmektedir.

Dünya genelinde teşebbüsler BYOD (Bring Your Own Device – Kendi Cihazını Getir), BYOE (Bring Your Own Environment/Everything – Kendi Ortamını/Herşeyi Getir) kurallarını uygulamaktadır. Teşebbüslerin bu kuralları olsa dahi yapılacak incelemede kişisel cihazın teşebbüs ile illiyet bağı kurulması, sadece teşebbüs kaynaklarına erişimi ile iddia edilmesi mümkün olmayacaktır.

İlliyet bağı teşebbüsün kullandığı yazılımlar ile kurulabilir. Bu tarz yazılımların başında e-posta gelecektir. Teşebbüse ait bir e-posta adresi kullanılması inceleme konusu yapılabilecektir. Bunun dışında çevrimiçi toplantı, mesajlaşma gibi uygulamalar olan Microsoft 365, Microsoft Teams, Skype Business, Google Meet, Cisco Jabber ve benzeri uygulamalar makul illiyet bağı olabilecektir.

İlliyet bağı sadece teşebbüs yazılımları ile kurulması kamu yararının gözetilmesi çerçevesinde yeterli olmayacaktır. Çünkü günümüzde Whatsapp, Telegram, Wiber, WeChat, Line, Google Hangouts ve BİP gibi birçok çevrimiçi mesajlaşma uygulaması ve aynı zamanda doküman paylaşımı gibi kabiliyetleri bulunan uygulamalar da bulunmaktadır.

Teşebbüsün kablosuz ağına bağlanması illiyet bağı oluşturmayabilir ancak kablosuz ağa bağlanarak şirket sistemlerine erişerek işlemler gerçekleştirmesi örneğin portal sayfası ve benzeri

intranet sitelerine erişmesi illiyet bağını ortaya çıkarabilecektir.

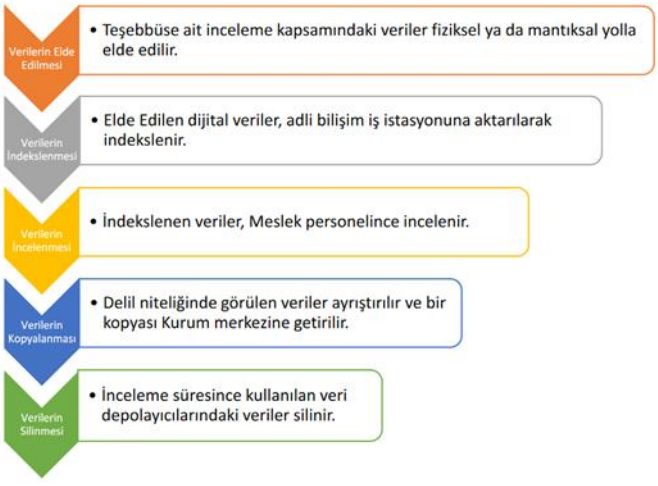
2.2 İlliyet Bağında Ölçülülük

Kişisel cihaz ile teşebbüs arasında kurulacak illiyet bağının ölçülü olması gerekecektir. [6] Bu nedenle teşebbüs dışı çevrimiçi bir uygulamanın bulunması da illiyet bağı için yeterli olmayacaktır. Kılavuzun beşinci [2] maddesinde "İnceleme süresince, inceleme kapsamındaki verilere ve verilerin tutulduğu ortama müdahale edilmesini engellemek teşebbüsün sorumluluğundadır." denilmektedir. Bu nedenle bilimsel ve mesleki şüphe ölçülülük çerçevesinde ele alınmalıdır.

2.3 İnceleme ve Adli Bilişim Yöntemleri

Kılavuzun altıncı maddesinde "İnceleme esnasında görevli Meslek Personelince gerekli görülmesi durumunda; incelenecek dijital veriler, adli bilişim yöntemleri ile kısmen veya bütün olarak ayrı veri depolayıcılarına kopyalanır." denilmektedir. Alınacak olan verilerin adli kopya olması bir hash değerinin olacağını göstermektedir. Adli bilişimde hash değeri matematiksel bir yöntem ile verinin bütünlüğü ve inkâr edilememezliği anlamına gelmektedir [7].

Bu nedenle kılavuzun sekizinci maddesinde "İnceleme sonunda gerekli görülen dijital veriler iki ayrı veri depolayıcısına kopyalanır. Elde edilen kopyalardan biri teşebbüse teslim edilir." denilerek tutanak altına alınması CMK 134 maddesi ile de uyumludur. Ayrıca inceleme sürecine ilişkin izlenecek adımlar kılavuzda belirtilmiştir. Belirtilen adımlar Şekil 1' de gösterilmiştir.



Şekil 1. İncelemede izlenecek adımlar [2]

Kılavuzun onuncu maddesinde "İncelemenin teşebbüse ait yerleşkede tamamlanması esastır. Ancak gerekli görülmesi durumunda incelemeye Kurum bünyesindeki adli bilişim laboratuvarında devam edilmesine karar verilebilir. Cep telefonlarından elde edilen dijital verilerin incelenmesi her halükarda teşebbüs yerleşkesinde tamamlanır." denilmektedir. Cep telefonlarının incelenmesinin her halükarda teşebbüs yerleşkesinde tamamlanması kişisel cihazların incelenmesindeki ölçülülük ve makul süre olarak değerlendirilebilecektir.

Kılavuzun on birinci maddesinde "dijital veriler içerisinde ticari sır niteliğinde veri bulunduğu hususunun ilgili teşebbüs tarafından ileri sürülmesi durumunda 2010/3 sayılı "Dosyaya Giriş Hakkının Düzenlenmesine ve Ticari Sırların Korunmasına İlişkin Tebliğ" kapsamında işlem yapılır. Ticari sırrın korunmasını garanti altına almaktadır. Yine kılavuzun on ikinci maddesinde Avukat-Müvekkil gizliliğine ilişkin olarak "Yerinde inceleme sırasında kopyalanan veriler, avukat-müvekkil gizliliği ilkesi kapsamında korumadan yararlanır." denilerek garanti altına alınmaktadır.

3 Yöntem Önerileri

Yerinde incelemelerde dijital verilerin incelenmesine ilişkin kılavuzda her ne kadar bir takım bilgiler ve izlenecek adımlar verilmiş olsa da tartışmaya açık hususlar bulunmaktadır. Bu öneriler ile tartışmaya açık hususların ortadan kaldırılabileceği düşünülmektedir. Önerilen yöntemler aşağıda sıralanmıştır.

Rekabet ihlaline yönelik bilinen anahtar kelimeler teşebbüs sistemleri üzerinde araştırılarak iltisaklı olabilecek çalışanlar tespit edilebilir. Anahtar kelimeler rekabete ilişkin daha önce edinilmiş tecrübeleri içermektedir. Bu tecrübelerden yola çıkarak örneğin "WP den konuşuruz", "telegram'dan yaz" gibi ifadeler tespit edilebilir. Bu durumda, çalışanların mobil cihazlarına ilişkin incelemenin yapılması için meslek personeline mobil cihazın teşebbüsle iltisaklı olabileceği kanaati oluşturabilecektir.

Rekabet ihlaline yönelik bilinen anahtar kelime sonuçlarına göre yeni anahtar kelimeler üretilerek ikinci kez araştırma yapılabilir. Bilinen anahtar kelimeleri marifetiyle tespit edilen yazışmalardan elde edilebilecek olan teşebbüse özel yeni anahtar kelimeler kullanılarak derinlemesine inceleme ve rekabete aykırı durumlar tespit edilebilir. Örneğin "zili çal, çan çalınır" gibi ifadeler tespit edilirse tekrardan anahtar kelime incelemesi yapılması gerekebilir.

İkinci araştırma sonucunda elde edilen bulgularla iltisaklı olabilecek çalışanlar tespit edilebilir. Teşebbüse özel yeni anahtar kelimeler rekabete aykırı bir durum olduğu değerlendirildiğinde buna istinaden ilgili yazışmaları yapan çalışanlar iltisaklı olduğu değerlendirilerek kanaat edildiği takdirde çalışan mobil cihazları da incelenmesi ölçülülük ve iltisak bağı oluşturulduğu belirtilebilir.

Teşebbüste yapılacak incelemelerde ve çalışan cihazlarında yapılacak incelemeler hukuk kuralları çerçevesinde gerçekleştirilmesi gerekir. Yargı yollarının açık olduğu değerlendirildiğinde kullanılacak adli bilişim donanım ve yazılımları ile birlikte kullanılan e-keşif (E-discovery) gibi yöntemlerin raporda açıkça yazılması yargıya elverişli olmasını sağlayabilecektir [8].

Çalışanlara ait cihazların adli imajları alındığı takdirde teşebbüs yetkilisi ve çalışanın imzası alınarak tutanağa bağlanabilir. İmtina edilmesi halinde, bu durum tutanağa yazılarak ve tutanak, en az iki Meslek Personeli tarafından imzalanabilir. Teşebbüs ya da ilgili çalışanın hukuk çerçevesi içerisindeki itirazlarının usül olarak reddedilmesini sağlayacaktır. Bu durum hem teşebbüsü hem de kurumu koruyacaktır.

Adli bilişim yöntemleri ile silinen veriler elde edebileceğinden çalışan cihazlarına müdahale bilimsel ve mesleki şüphe ölçülülük çerçevesinde ele alınarak makul sürelerde değerlendirilebilir. Eğer çalışan anahtar kelime çalışmaları esnasında her hangi bir nedenle cihazından bir veri silerse, delil olarak değerlendirilecek bu veriler tespit edilebilir. Bu nedenle teşebbüste görevli Meslek Personeli bu farkındalıkla çalışmalarını soğukkanlılıkla devam edebilecektir. Tabii ki cihazın tamamen sıfırlanması durumunda inceleme gerçekleştiremeyecektir. Ancak bu durum incelemeye yardımcı olmamak olarak değerlendirilerek idari para cezasına sebep olacaktır.

Teşebbüsler, çalışanlarına Rekabet Kurumu ile ilgili olarak kanuni sorumluluklarını anlatan farkındalık eğitimleri vererek, teşebbüslerin çalışanlarından kaynaklı psikolojik/kişisel yaklaşımlardan dolayı zarar görmesinin önüne geçebilir.

Teşebbüs anahtar personellerine Rekabet Kurumu gibi adli ve idari durumlarda kılavuzun beşinci maddesinde ifade edildiği gibi ilgili görevlinin "talep ettiği hususlarda tam ve aktif destek vermek zorunda" olduğu hatırlatılması faydalı olacaktır.

Teşebbüs çalışanlarının kişisel cihazlarının güvenliğini sağlamak için kullanmış oldukları desen, rakam, harf yada karışık olarak belirledikleri parolalarını inceleme için cihaza girmeleri yada vermeleri gerektiğinin bildirilmesi ile olumsuz sonuçların önüne geçilebilir.

Teşebbüslerin faaliyetleri ve faaliyet gösterdikleri ülkeler çerçevesinde çalışanlarıyla yapmış oldukları iş sözleşmelerinin içerisine Rekabet Kurumu özelinde olmamakla beraber adli ve idari konularda Kişisel Verilerin Korunması Kanunu gibi ulusal ve GDPR (EU General Data Protection Regulation, Avrupa Birliği Genel Veri Koruma Tüzüğü) /CCPA (California Consumer Privacy Act, Kaliforniya Tüketici Gizlilik Yasası) gibi uluslararası kanunlar çerçevesinde adli imajlarının alınabileceği, incelenebileceği gibi maddeler eklemeleri faydalı olabilecektir.

4 Sonuçlar

Bu çalışmada önerilen yöntemler ile birlikte hem teşebbüslerin hem de çalışanlarının farkındalıklarının arttırılmasına ilişkin öneriler sunularak hukuk karşısında kendilerini savunmalarına ilişkin önlemler alınabilecektir. Teşebbüslerle ilgili olarak yapılan öneriler, teşebbüs ve çalışanlarının haklarının yanı sıra teşebbüse istemeden verecekleri zararların önüne geçmesini sağlayacaktır. Teşebbüs yöneticileri ya da çalışanların istemeden yapacağı olumsuz bir durum ciddi idari para cezalarına sebep olabilecektir. Kurum uzmanları hızlı gözden geçirme yaparlarken illiyet bağının kurulmasını, bunu gerçekleştirirlerken de ölçülülük ilkesi doğrultusunda bağlı bulundukları kurumları yüksek mahkeme de koruyabilmelerini sağlayacaktır. Adli bilişim yöntemlerinin kullanılmasına ilişkin olarak yönetmelikte de bulunan mobil cihazların yerinde incelenmesinin tamamlanmasında uluslararası mobil inceleme yazılım ve donanımlarının kullanılması ve hash değerleriyle bunların kayıt altına alınmasında inkâr edilememezliliği sağlayacaktır. Hukuk sistemi içerisinde kararlara itiraz ve üst mahkemeye gitme imkanları bulunmaktadır. Denetime elverişli olmayan süreçler gerçekleştiği takdirde ilgili kararlar üst mahkeme tarafından bozulabilmektedir. Kararın bozulması ise emsal teşkil edeceğinden ve sonraki mahkemelerde bu kararlar kullanılabileceğinden kurumun çalışmalarında zorluklar çıkarabilecektir.

Kaynaklar

[1] Güzel O, Coşkun B.İ., Dijital Sektörlerde Rekabet Hukuku Uygulamaları, Legal Banka ve Finans Hukuku Dergisi, Cilt.9, Sayı. 35, Sayfa. 833-864, 2020.

[2] Rekabet Kurumu- Yerinde İncelemelerde Dijital verilerin İncelenmesine İlişkin Kılavuz, https://www.rekabet.gov.tr/Dosya/kilavuzlar/yerinde-inceleme-kilavuz1-20201009091644514-pdf, Erişim Tarihi: Kasım 2021

[3] Özel Hayatın Gizliliği, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf, Erişim Tarihi: Kasım 2021

[4] Ceza Muhakemesi Kanunu Makul Şüphe, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf, Erişim Tarihi: Kasım 2021

[5] Kişisel Verilerin Korunması Kanunu, https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, Erişim Tarihi: Kasım 2021

[6] Metin Y., TEMEL HAKLARIN SINIRLANDIRILMASI VE ÖLÇÜLÜLÜK: Ölçülülük İlkesi Evrensel Bir Anayasal İlke midir?, Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, Cilt.7, sayı.1, Sayfa. 1-74, Aralık 2017.

[7] V. Roussev., Hashing and Data Fingerprinting in Digital Forensics, in IEEE Security & Privacy, vol. 7, no. 2, pp. 49-55, March-April 2009, doi: 10.1109/MSP.2009.40.

[8] J. Wiles, Techno Security's Guide to E-Discovery and Digital Forensics: A Comprehensive Handbook, 1th Edition, Syngress, 2007..

A Password Manager for Post-Quantum Era

Samet Tonyali[1]*, Olemilekan Rasaq Aremu[2], Abdulkadir Köse[2]

[1]*Gümüşhane University, Gümüşhane, TURKEY*
[2]*Abdullah Gül University, Kayseri, TÜRKİYE*

Abstract

Quantum computing poses a threat to our classical cryptographic algorithms especially, key exchange and digital signature algorithms. The rise of this threat has also brought about the rise of solutions and the birth of a new standard called Post-Quantum Cryptography. These algorithms will be resistant against quantum attacks and will be the new standard going forward following the results from the National Institute of Standards and Technology. The goal of this paper is to investigate the progress of post-quantum cryptographic algorithms and how they perform in a pseudo-production environment through the development of a desktop application dealing with highly sensitive data. Specifically, an analysis on the performance of the key exchange and digital signature verification algorithms was conducted, and insights into the viability of these algorithms were given. The findings in this paper would aid the easy adoption of post-quantum algorithms into production environments once they become the new standard.

Keywords: *Post-quantum Cryptography, Key Exchange Algorithm, Key Encapsulation Mechanism, Digital Signature, Post-quantum Digital Signature*

Kuantum Sonrası Dönem İçin Bir Parola Yöneticisi

Özet

Kuantum hesaplama, anahtar değişim ve dijital imza algoritmaları başta olmak üzere geleneksel kriptografik algoritmaların güvenliği için tehdit oluşturmaktadır. Shor algoritmasının yeterince ölçeklenmiş ve verimli kuantum işlemcilerde gerçeklenmesi sonucu bu algoritmaların dayandığı zor matematiksel problemler kolayca çözülebilecektir. Bu tehdidin ortaya çıkması kuantum-dayanıklı kriptografinin ilgi odağı haline gelmesine sebep olmuştur. Bu algoritmalar ABD Ulusal Standartlar ve Teknoloji Enstitüsü'nün çağrısı ile standartlaşma sürecine girmiş bulunmaktadır. Bu çalışma kuantum-sonrası kriptografi algoritmalarının ilerleyişini ve gerçek olmayan bir üretim ortamında yüksek hassasiyetteki verilerle çalışan bir masaüstü uygulaması aracılığıyla başarımının incelenmesini amaçlamaktadır. Özellikle, anahtar değişim ve dijital imza doğrulama algoritmalarının başarım analizi gerçekleştirilmiş ve bu algoritmaların uygulanabilirliğine dair bulgularımız sunulmuştur. Bu çalışmadaki bulgular, kuantum-sonrası kriptografi algoritmaları standartlaştırıldıktan sonra üretim ortamlarında benimsenmesine yardımcı olacaktır.

Anahtar Kelimeler: *Kuantum-sonrası Kriptografi, Anahtar Değişim Algoritmaları, Anahtar Kapsülleme Mekanizması, Dijital İmza, Kuantum-sonrası Dijital İmza*

1 Introduction

With the innovation of more secure methods of transmitting sensitive data, comes more ways of cracking these secure ways. Reminiscing back to World War 2 when the Enigma machine was used for secure communication, computers were subsequently developed which were able to crack this machine.

Today however, we have a similar situation with quantum computers and Shor's algorithm [1]. Modern day cryptographic algorithms are the basis of secure communications and transactions on the

* Corresponding author: samet.tonyali@gumushane.edu.tr

Internet. These algorithms rely on two main problems; the integer factorization problem and the discrete logarithmic problem. As a result of these problems being very difficult to be solved, secure communication can exist, and they can be very difficult to break. However, Peter Shor, a mathematician detailed how these problems can be solved in 1994. This is known as Shor's algorithm. His algorithm was not designed to work on classical computers and instead needed quantum computers [1].

This paper would look to investigate the performance of these algorithms in a pseudo-production environment and delve into the time it takes to encapsulate and decapsulate the shared secrets, create a digital signature and comment on the ease of development.

2 Technical approaches

In this section, we present the technical approaches we used in this work.

2.1 Project information

In order to understand the performance of these post-quantum cryptographic (PQC) algorithms in the context of a production environment, a password manager was developed. This application was developed as a desktop application with the following features.

2.1.1 Client-Side encryption and decryption

Encryption and Decryption responsibility falls to the client which allows the server to be ignorant of these processes. As such, if the server is ever compromised, the encryption key is incapable of being generated.

2.1.2 On-the-Fly key generation

Encryption and Decryption keys are generated on the client and not stored locally. Whenever the key is needed, the key is generated once again and used to either encrypt or decrypt the payload. This prevents attacks that can snoop through memory segments.

2.1.3 Multiple users on a single client

This application supports multiple users on a single client through JSON Web Tokens. It uses JSON Web Tokens to perform authentication and authorization mechanisms.

2.1.4 Post-quantum cryptography

The application would also use post-quantum cryptography to ensure secure communication. It will use key encapsulation and digital signature algorithms. This is one of the first applications to implement these algorithms in a production or pseudo-production environment.

2.2 Technological stack

The technological stack chosen to develop this application was carefully thought out. It involves technology which provided ease of development without reinventing the wheel, provided a performant application and software which interacts well on all layers. The technology chosen for this project were as follows.

2.2.1 JavaScript & TypeScript

This is the language chosen for development on the frontend and the backend. This ensures that the same language can be written on both sides and as a superset of JavaScript, TypeScript provides type-safety which ensures that errors are caught in compile-time rather than during run-time.

2.2.2 Electron

Electron is a framework which allows desktop applications to be built using JavaScript, HTML and CSS. It works by embedding chromium into a desktop application. This ensures that development can be fast at the expense of a larger bundle size during packaging. Electron was used to build desktop applications for Discord, Twitch and Facebook Messenger. It offers a great developer experience.

2.2.3 React.JS

The frontend of the application was written in React to ensure reactive user-interfaces. React is the leading frontend library and was developed by Meta.

2.2.4 NodeJS

The NodeJS JavaScript runtime powers the backend of the application. It allows for JavaScript to be written on the server and ensure the smooth interoperability of the frontend and backend by using the same language.

2.2.5 ExpressJS

Express is a minimalistic framework for creating REST APIs. It provides an intuitive way to build fully equipped API endpoints and as such, the server and the proxy was written using this framework.

2.2.6 MongoDB

MongoDB was the database of choice. The decision was made due to the fact that it was a document

database, easily configurable and features free AWS hosting.

2.2.7 TailwindCSS

The application was styled using TailwindCSS. A utility first CSS framework which provided a great developer experience while ensuring beautiful user-interfaces can be built.

2.2.8 ChakraUI

ChakraUI powered the modals of the application. It provided a clean interface for creating modals and ensuring they looked the best while being performant.

2.2.9 Linux development environment

Linux was the development environment of choice as it allowed the use of Liboqs library [2] which enabled the access to the post-quantum algorithms at a higher level through wrappers.

2.3 Key exchange and digital signature verification mechanism

An important aspect of the application is secure communication which is provided through PQC algorithms. Before passwords are retrieved and transmitted to the client, a secure key must be exchanged between the client and server and used for this communication. This is enabled in the application through Kyber-512 [3] key encapsulation and Dilithium-2 [4] digital signature algorithms.

On login from user, the client [5] sends a request to the proxy server [7] which then engages in the key exchange with the server [6] and replies to the client with the shared secret which is used for subsequent communications. In more detail, during the key exchange, the proxy server generates a public key using the key exchange algorithm and signs it using the digital signature algorithm then sends it to the server, the server receives it and then verifies the signature and if valid, encapsulates its secret using the received public key and subsequently generates a shared secret and cipher text. The cipher text is returned to the proxy and is used to decapsulate its secret and generate the same shared secret as the server. This shared secret is then sent back to the client and stored in a database on the server side. The entire data flow is illustrated in Fig.1.

2.4 Comparison of technical approaches

PQC algorithms not only provide quantum-safety, the NIST standards also provide additional security over classical cryptographic algorithms. A comparison between minimum key length and complexity of a successful brute-force attack shows that for key lengths ranging from 80 up until 256 bits, the NIST standards are much more resistant to brute force attacks than the integer factorization problem and discrete logarithm problem algorithms [8].

As shown in Table 1, with increasing key lengths, strength against brute force attacks grow.

Table 1. Comparison of various algorithms: Key lengths and resistance against brute-force attacks [2].

Brute Force	80	112	128	192	256
DLP	160	224	256	384	512
IFP	851	1853	2538	6707	13547
NIST	1024	2048	3072	7680	15360
C-SSI	320	448	512	768	1024
Q-SSI	480	672	768	1152	1536
C-CODE	1438	2013	2301	3451	4602
Q-CODE	2876	4026	4602	6902	9203
C-RLWE	673	921	1058	1541	2045
Q-RLWE	746	1016	1152	1688	2234

2.5 Solution novelties

The proposed solution consists of some novelties to distinguish itself from others out there. Some of these novelties include the fact that this application is one of the first to use post-quantum algorithms in a pseudo-production environment. As these algorithms are still theoretical, applications have not begun to adapt these algorithms.

Another novelty is how the encryption and decryption mechanism are performed. The server is completely kept out of the loop and these mechanisms are only possible on the client side due to the server being unable to generate the key. This approach ensures that should the server or database be compromised, the passwords are still secure.

3 Results

In this section, we present our findings as a result of our experiments.

3.1 Key exchange data and results

Following the development of the application and subsequent implementation of the PQC key exchange and digital signature verification algorithms, readings were taken to understand the performance of the process as well as other

important statistics. The algorithms used are Kyber-512 and Dilithium-2. The results were taken on a computer with an Intel i5-7300hq processor running Ubuntu 20.04 on a virtual machine. The results are given in Table 2.

According to the results, key encapsulation and decapsulation are in acceptable limits. The digital signature generation and verification while taking more time are also acceptable. However, compared to the encapsulated key

Table 2. Performance results of PQC algorithms.

Metric	Recording
Key Encapsulation Time	92 ms
Key Decapsulation Time	0.19 ms
Encapsulated Key Size	32 bytes
Digital Signature Generation Time	22 ms
Digital Signature Verification Time	190 ms
Digital Signature Size	2420 bytes

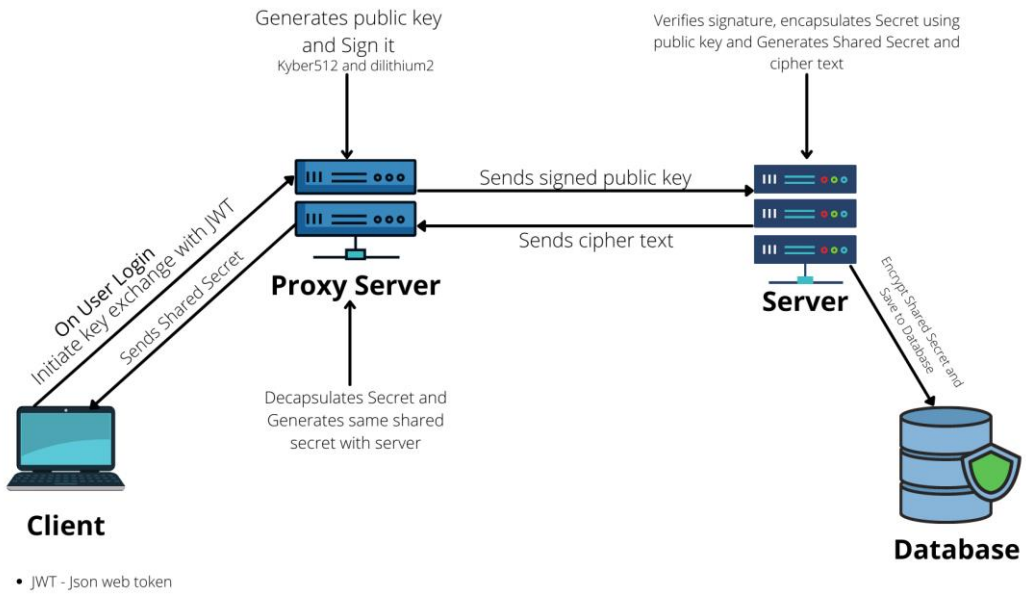


Figure 1. Key exchange flow.

size, the digital signature is much larger, and that might be something to pay attention to. According to these results, these algorithms are completely viable in a production environment and once the standards have been defined, there would be no cause for alarm in terms of performance of applications.

3.2 Advantage of the approach

Developing an application which needs to transfer sensitive data from server to client and vice versa is unavoidable as many applications collect and are responsible for data provided by the user, much of which are very sensitive. This approach provides a guide to these applications and how they can ensure secure communication to avoid security threats and vulnerabilities.

These advantages include;

- **Quantum safety:** This means that using PQC key exchange algorithms protects against attacks from quantum computers. Although these algorithms are still theoretical and a standard has not been decided upon by the relevant authorities, once they are, it will be unwise to not implement them in all applications.
- **User authentication:** The implementation of user authentication ensures that multiple users can coexist on a single client and perform separate key exchanges. User authentication is powered by JSON Web Tokens and transmission is performed with a valid post-quantum key and a valid access token.
- **Ignorant server:** End-to-End secure applications are becoming more popular. This approach was also thought about in the design phase. The server being unaware of the payload means the passwords are secure in case the server or database is compromised.

3.3 Disadvantages of the approach

As with all things, there are some downsides to this approach as well. Being a desktop application, it is susceptible to attacks that can snoop through memory.

3.4 Challenges

Development of an application of this scale is not without its challenges. The main challenge

encountered during this work was the complexity of key flows. As a complex application, a multitude of keys were being exchanged, generated and stored. The complexity steadily grew as more keys were introduced. This complexity was mitigated by detailing the flow and developing a state diagram to visualize the flow before the implementation of any code.

4 Conclusion

This paper investigated the quantum computing threat and looked into how possible post-quantum standards can perform in a production environment. It was discovered that these algorithms are performant and viable and should not be an issue when implemented in a production application. Although the quantum computing threat is not a wide spread issue at the moment, now is the time to start preparing for the period it does become one. The National Institute of Standards and Technology are in the process of developing new cryptographic standards for a quantum-safe future. This process is now in the third round and hopefully once the standards are finalized, the gradual migration to these algorithms can take place.

References

[1] Mone Gregory. "The quantum threat." *Communications of the ACM*, 63.7, 12-14, 2020.

[2] D. Stebila, M. Mosca., "Post-quantum key exchange for the Internet and the Open Quantum Safe project," In Roberto Avanzi, Howard Heys, editors, Selected Areas in Cryptography (SAC) 2016, LNCS, vol. 10532, pp. 1–24. Springer, October 2017. https://openquantumsafe.org.

[3] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G. and Stehlé, D., 2018, April. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS\&P) (pp. 353-367). IEEE.

[4] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G. and Stehlé, D., 2018. Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.238-268.

[5] Olamilekan Aremu, Post Quantum Password Manager, Last accessed on 31 August 2022, https://github.com/Areezy/postquantum-password-manager.

[6] Olamilekan Aremu, Post Quantum Password Manager Server, Last accessed on 31 August 2022, https://github.com/Areezy/postquantum-password-manager-server.

[7] Olamilekan Aremu, Key Exchange Proxy Server, Last accessed on 31 August 2022, https://github.com/Areezy/keyexchange-proxy.

[8] F. Borges, P. R. Reis, and D. Pereira, "A comparison of security and its performance for key agreements in Post-Quantum Cryptography," IEEE Access, vol. 8, pp. 142413–142422, 2020.

CAFTSY: Yüz Tanıma Tabanlı Ulaşım Sistemi

Furkan Ayakdaş[1]*, Erdem Demiroğlu[2], Nurullah Sevinçkan[3] ,Gülsüm Akkuzu Kaya[4]

[1]Isparta Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Isparta, Türkiye
[2,3]Recep Tayyip Erdoğan Üniversitesi, Mühendislik-Mimarlık Fakültesi, Rize, Türkiye
[4]Kırşehir Ahi Evran Üniveristesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Kırşehir, Türkiye

Özet

Teknolojik gelişmeler sayesinde günlük hayatı kolaylaştıracak birçok uygulama geleneksel uygulamaların yerini almıştır . Yüz tanıma sistemleri bu yenilikçi uygulamalar arasındadır ve birçok alanda güvenliği artırmak için kullanılmaktadır . Bazı bankacılık sistemleri müşterilerinin kimlik doğrulaması işlemiş için yüz tanıma sistemlerini kullanmaktadır . Teknolojinin ve uygulamalarının yaygın kullanımına karşın hala , geleneksel yöntemlerin kullanıldığı sistemlerin varlığı günümüzde söz konudur . Bunlardan bir tanesi toplu taşıma sistemleridir . Toplu taşıma sistemlerinde kullanılan yöntemler trafikte kaza, vakit kaybı veya hırsızlık gibi problemlere yol açmaktadır . Bu çalışma toplu taşıma düzeyinde güvenliği arttırmak için yüz tanıma tabanlı bir ödeme sistemi önermektedir . Önerilen çalışma güvenilirlik, güvenlik ve uygulanabilirlik kriterleri ile değerlendirilmektedir.

Anahtar Kelimeler: *Yüz tanıma, Güvenlik, Temassız, Akıllı trafik, Ödeme sistemi, Yenilik*

CAFTSY: Face Recognition Based Transportation System

Abstract

Thanks to technological developments , many applications that will facilitate daily life have replaced traditional applications . Facial recognition systems are among these innovative applications and are used to increase security in many areas . Some banking systems use facial recognition systems to authenticate their customers . Despite the widespread use of technology and its applications , there are still systems in which traditional methods are used today . One of them is public transport systems . The methods used in public transportation systems cause problems such as traffic accidents , loss of time or theft . This study proposes a face recognition based payment system to increase security at the level of public transport . The proposed study is evaluated with the criteria of reliability, safety and applicability.

Keywords: *Face detection, Security, Contactless, Intelligent traffic, Payment system, İnnovation*

[1]* İletişim e-posta: gulsum.akkuzukaya@ahievran.edu.tr

1 Giriş

Sanayi Devrimi merkezli dünyaya uyum sağlamak için çeşitli alanlarda yeni teknolojiler uygulanmaktadır. Yeni teknoloji uygulamalarının amacı hayatı kolaylaştırmak ve oluşabilecek sorunları en aza indirmektir. Günümüzde yaşamın farklı alanlarında teknolojik gelişmelerin uygulamalarına rastlamak mümkün olsa da halen geleneksel uygulamaları kullanan sistemler mevcuttur. Örneğin, otomatik ödeme sistemlerinin varlığı söz konusu olmasına rağmen yerel otobüsler ve/veya ortak taksiler sorunlara neden olan nakit ödeme sistemini kullanmaya devam etmektedir [1] . Finlandiya, dünyanın ilk yüz tanıma ödeme sistemi olan "Uniqul" ile ödemenin sadece kamera üzerinden yüzün tanınması ile yapılabilmesinin mümkün olduğunu kanıtlamıştır.

Geleneksel ödeme sistemlerinin başlıca sorunları şöyledir;

- Mevcut toplu taşıma araçlarında halen salgın hastalıkların yayılmasına neden olabilecek nakit ödeme yapılması.
- Sürücünün parayı alırken ve verirken yola olan dikkatini kaybederek trafik kazalarına neden olabilmesi.
- Para bozdurma veya kart ödemeleri, müşteri ve sürücüler için zaman kaybına neden olabilecek bekleme kuyruklarına neden olması
- Toplu taşıma ödemelerinde her şehir farklı kart uygulamaları kullanıyor; farklı kart gereksinimleri.
- Toplu taşıma kartlarında yolcuların rol değişiklikleri (öğrenci, asker, çocuk, yaşlı, normal vatandaş).

Bu çalışma listelenen problemlere çözüm üretmek için yüz tanıma sistemi tabanlı bir uygulama geliştirerek günümüz dünyasında uygulanan akıllı trafik sistemlerine bir katkı sağlamayı amaçlamaktadır.

Çalışmanın diğer bölümlerinin genel yapısı şu şekildedir, İkinci bölüm, yüz tanıma sistemleri ve kullanım alanları tartışılmıştır. Üçüncü bölümde, bu çalışmanın tamamlanması için izlenen metot tartışılmıştır. Bölüm 4'te bu çalışma sonucundan beklenen sonuçlar sunulmuştur.

2 Literatür Taraması

Yüz tanıma teknolojisi, görüntü veya video içeriklerinde var olan bir yüz alanının otomatik olarak algılanarak bu yüzün analizi ile bu yüzün hangi insana ait olduğunu belirler [2]. Yüz tanıma işlemi, bir kişinin yüzü kamera ile tarama işlemi yapıldıktan sonra göz , kulak ve ağız yapısı gibi yüz özellikleri çıkarılarak gerçekleştirilir [3]. Yüz tanıma sistemleri bugün birçok alanda kullanıldığı gibi ödeme sistemlerinde de kullanılmaktadır . Bu sistemlerden bir tanesi ülkemizde birçok bankanın mobil bankacılık uygulamalarında kimlik doğrulama işlemi için kullanılan yöntemdir . İnsan yüzünün şifre yerine kullanılması sistemi olarakta bilinen sistemdir [4]. Diğer ödeme sistemi platform-tabanlı ödeme sistemi , Uniqul uygulaması bu sistemi kullanmaktadır. Bu sistemde ödeme işlemi yapılmak istendiğinde kişinin sadece kameraya bakması yeterli olur.

Platform tabanlı ödeme sistemi ve mobil ödeme sistemleri sayesinde insanların cüzdan , nakit para , banka veya kredi kartı taşımlarına gerek kalmadan ödemelerini biometrik verilerini kullanarak kolayca yapabilmektedir . Sistem kalitesine yönelik çalışmalarda yüz tanıma tabanlı ödeme sistemlerinin kolaylık , güvenilirlik , güvenlik ve tepki hızı faktörlerinden dolayı ödeme sistem kalitesini artırdığı gözlemlenmiştir [5].

Yüz tanıma tabanlı ödeme sistemi karakteristik özelliklerine göre şöyle incelenir; Hareket kolaylığı, zaman kolaylığı ve kullanım kolaylığı avantajları ile geliştirilen sistemlerde ayırıcı özellik olan **kolaylık** faktörünü karşılar [6]. Yüz tanıma tabanlı ödeme sistemlerinde hizmetten duyulan memnuniyet ve hizmeti sürekli kullanma isteği sistemin **güvenilirlik** faktörünü karşılar [7]. **Güvenlik** geliştirilen sistemde ödeme yapılırken finansal ve kişisel bilgilerin sızdırılmadan gerçekleştirilmesi işlemidir [8]. **Temassız** ödeme kriteri, fiziksel herhangi bir etkileşim olmaksızın ödeme işleminin gerçekleştirilmesidir.

Bizim çalışmamızın amacı yukarıdaki çalışmalarda sözü geçen yüz tanıma tabanlı ödeme sisteminin ülkemizde toplu taşımalarda kullanımını sağlamak için gerekli sistemi geliştirmektir. Geliştirdiğimiz uygulama sistem gereksinimleri baz alınarak değerlendirme işlemi gerçekleştirilecek.

3 Metot

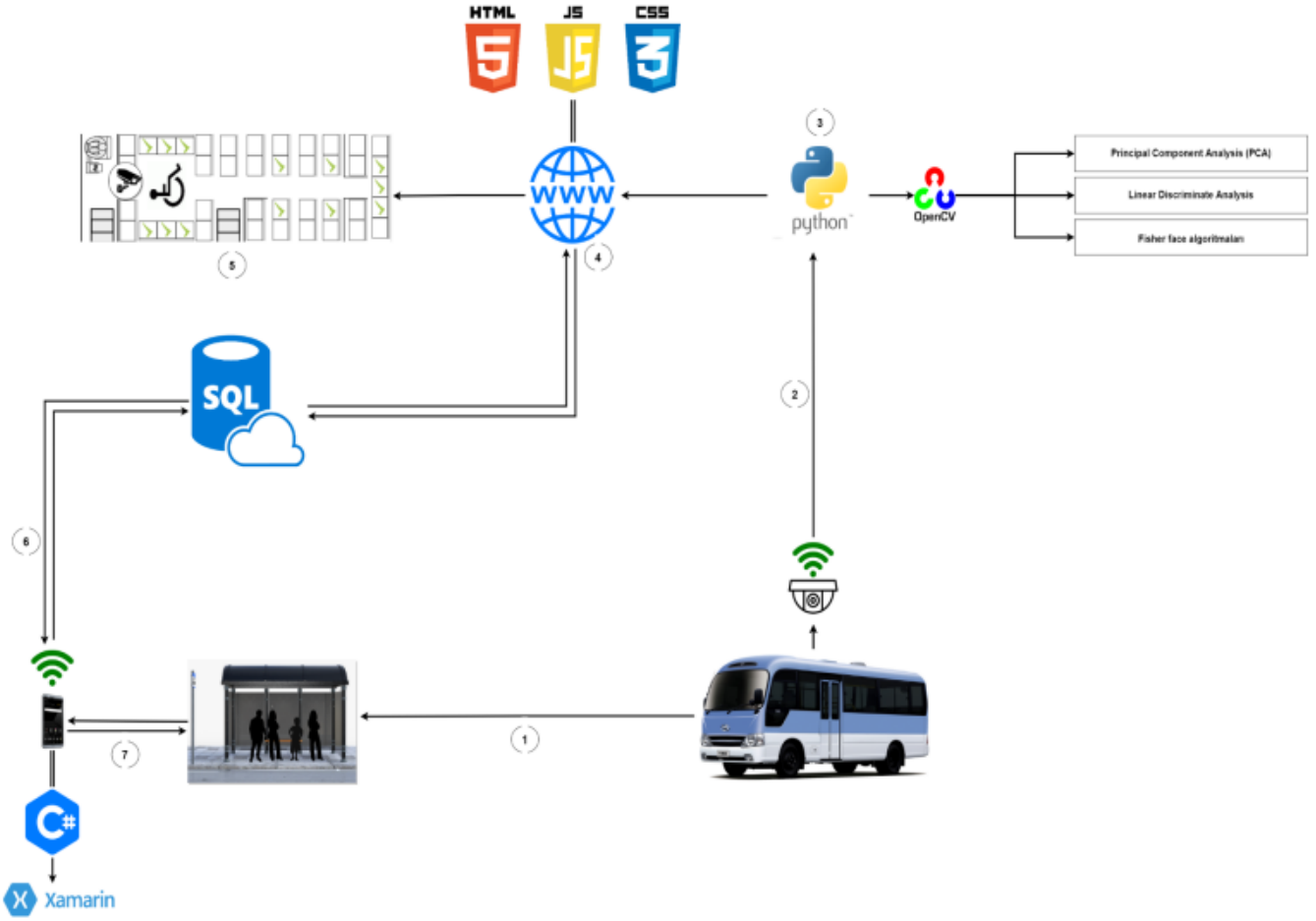
Bu bölümde çalışmamızın genel mimari yapısı açıklanmıştır . Şekil 1'de sistemimizin ilk adımdan son adıma kadar nasıl çalıştığı genel bir yapı ile verilmiştir . Adımlar şu şekilde açıklanmıştır;

1. Yolcu gitmek istediği güzergâh doğrultusunda ulaşım aracına biner.
2. Otobüste bulunan yüz tanıma sistemi kameralar aracılığı ile yolcuların yüzünü tarar . Alınan veriler geliştirdiğimiz algoritmalar kullanılarak kategorize edilir.
3. Kişilerin yüz verileri geliştirdiğimiz sistemin veri tabanında saklanır . Veri tabanında bulunan ve yolcu yüz profili ile eşleşen kişi kaydı bulunup halihazırda elde edilen güncel veriler ile güncelleme yapılır.
   Bu veriler;
   - Kişinin Önceki bakiyesinden hizmetten yararlandığı takdirde bakiye düşürme.
   - Kişinin yeni kullanmış olduğu rotayı veri olarak kaydetme.
     Kişinin istenildiği takdirde güncel konum bilgisini zaman destekli kaydetme.
     Kişinin yeni yüz verisi veritabanında halihazırda bulunan yüz verisi eskimiş olması veya doğruluk oranını arttırmak için yeni yüz verisi filtre kullanılması için veritabanına eklenecek veya güncellenecek.
4. Python aracılığı ile işlenen verilerin SQL veritabanında güncellenmesi sağlanarak son kullanıcı (yolcu) için Web sayfasında bulunan yolcunun kendi profiline yansıtılır . Bu bilgiler arasında;
   - Yolcunun bulunduğu rota
   - Eğer Ulaşım aracını hali hazırda kullanıyorsa , ulaşım aracının rotasını
   - Yolcunun mevcut bakiyesini
   - Yolcunun geçmişte bulunduğu rotaları
   - - Yolcunun rolü (öğrenci , yaşlı, çocuk, vb)

   bilgiler içerir ve bu bilgiler Web kullanıcı arayüzünde gösterilir.
5. İşlenen veriler ile ulaşım aracının anlık durumu, rota, ulaşım ücreti gibi bilgileri görselleştirerek

yolcuya sunulmak üzere web uygulama ve mobil uygulamaya gönderilir.

6. Mobil uygulamayı kullanan kişi kendisi ulaşım aracı ve güzergah hakkındaki bilgiler kullanıcıya sunulur.



Şekil 1. Genel Yapı

4 Beklenen Sonuç

Geliştirilmekte olan CAFTSY ödeme sistemi tamamlandığında beklenen sonuçlar şöyledir;

- Geliştirilen sistem kullanımı kolay ve güvenilir olmalı
- Toplu taşım aaraçlarını kullanan kişilerin sistemin kullanımı ile ilgili düşünceleri toplanarak, sistemin kullanıcılar tarafından benimsenirliği test edilecektir.
- Kullanıcıların gizlilik ve mahremiyetleri korunmalıdır

Limitasyon:

Sistem henüz geliştirilme aşamasında olduğu için herhangi bir sonuç elde edilememiştir.

Kaynaklar

[1] Zhang, L. L., Xu, J., Jung, D., Ekouka, T., & Kim, H. K. (2021). The Effects of Facial Recognition Payment Systems on Intention to Use in China. Journal of Advanced Researches and Reports, 1(1), 33-40.

[2] Kim, H. I., Moon, J. Y., & Park, J. Y. (2018). Research Trends for Deep Learning-Based High-Performance Face Recognition Technology. *Electronics and Telecommunications Trends*, *33*(4), 43-53.

[3] Lee, J. (2020). Changes in Society According to Facial Recognition Technology. *Magazine of the SAREK*, *49*(3), 90-91.

[4] Zhang, L. L., Xu, J., Jung, D., Ekouka, T., & Kim, H. K. (2021). The Effects of Facial Recognition Payment Systems on Intention to Use in China. *Journal of Advanced Researches and Reports*, *1*(1), 33-40.

[5] Choi, S., & Song, G. (2018). A study on the influence of system quality characteristics of mobile payment service on discontinuance intention. *Journal of the Korean Society for Quality Management*, *46*(3), 625-640.

[6] Choi, S., & Song, G. (2018). A study on the influence of system quality characteristics of mobile payment service on discontinuance intention. *Journal of*

the Korean Society for Quality Management, *46*(3), 625-640.

[7] Zhang, L. L., Xu, J., Jung, D., Ekouka, T., & Kim, H. K. (2021). The Effects of Facial Recognition Payment Systems on Intention to Use in China. *Journal of Advanced Researches and Reports*, *1*(1), 33-40.

[8] Zhang, Y. N., Ma, J., & Park, H. J. (2019). Factors Affecting the Usage of Face Recognition Payment Service. *The Journal of the Korea Contents Association*, *19*(8), 490-499.