MÜHENDİSLİK FAKÜLTESİ

Uluslararası Mühendislik Araştırma ve Geliştirme Dergisi
International Journal of Engineering Research and Development

UMAGD, (2019) 11(1), 64-76.

10.29137/umagd.481464

Cilt/Volume:11 Sayı/Issue:1 Ocak/January 2019

Araştırma Makalesi / Research Article

Sis Bilişim Tabanlı İmza Doğrulama: Senaryoya Dayalı Bir Yaklaşım

Fog Computing Based Signature Verification: A Scenario-Based Approach

Erdal Erdal [1*]

[1]*Kırıkkale Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü, 71450, KIRIKKALE*

***Başvuru/Received**: 11/11/2018* ***Kabul/Accepted**: 16/12/2018* ***Son Versiyon/Final Version**: 31/01/2019*

Öz

Günümüzde teknolojinin gelişmesi hayatımızı her alanda büyük oranda kolaylaştırmaktadır. Ancak internet üzerinden yapılan işlemler güvenlik tehdidini beraberinde getirmektedir. Bu nedenle kişiye özel bir veriye yetkisiz kişiler tarafından erişimin engellenmesi için kontroller ve çalışmalar yapılmaktadır. Bu kontrollerden en önemlilerinden biri kullanıcılardan alınan imza bilgisidir. Ancak imza bilgisi taklit edilebilir ve çalınabilir olduğundan gözle kontrolü yetersiz kalmaktadır. Bu nedenle imzaya özgü karakteristik bilgilerin imzadan çıkarılması, kaydedilmesi ve sonraki imzalarla karşılaştırılması en doğru yaklaşımdır. Bu gibi işlemler bulut bilişim üzerinde yapılmış ve geliştirilmiştir. Geleneksel bulut bilişim mimarisinde tüm veriler internet üzerinden gönderildiği ve paylaşıldığından güvenlik başta olmak üzere bant genişliği, enerji sarfiyatı gibi dezavantajlar barındırmaktadır. Bu nedenle sis bilişim mimarisi geliştirilmiş ve geleneksel bulut bilişimde yer alan eksiklikler büyük oranda giderilmiştir. Bu çalışmada sis bilişim tabanlı imza doğrulama yaklaşımı geliştirilmiştir. Güvenliğin yoğun olarak ele alındığı kurumlardan olan bankalar için bir senaryo geliştirilmiş ve bu senaryo ile değerlendirilmiştir. Çalışmanın sonucunda; geleneksel bulut bilişime kıyasla daha güvenli bir imza doğrulama çerçevesi ortaya konulmuştur. Yapılan çalışma bundan sonra yapılacak çalışmalara öncülük edecektir.

Anahtar Kelimeler

"Sis bilişim, Bulut bilişim, İmza doğrulama, Yazılım çerçevesi"

Abstract

Today, the development of technology greatly facilitates our lives in all areas. However, transactions over the internet bring about the security threat. For this reason, controls and studies are carried out to prevent unauthorized access to personal data. One of the most important of these controls is the signature information received from the users. However, since the signature information can be simulated and played, the visual control is insufficient. For this reason, signature-specific characteristic information is the most accurate approach to be signed out, recorded and compared with subsequent signatures. Such transactions have been made and developed on cloud computing. Since all data is sent and shared over the Internet in traditional cloud computing architecture, it has disadvantages such as bandwidth, energy consumption and security. Therefore, fog information architecture has been improved and the deficiencies in traditional cloud computing have been largely eliminated. In this study, fuzz computing-based signature verification approach has been developed. A scenario has been developed and evaluated in this scenario for banks from institutions where security is handled intensively. As a result of the study; a more secure signature verification framework has been developed compared to traditional cloud computing. The study will lead the studies to be carried out.

Key Words

"Fog computing, Cloud computing, Signature verification, Software framework"

***Sorumlu Yazar: erdalerdal@kku.edu.tr**

1. GİRİŞ

Günümüzde teknolojinin gelişmesiyle gerek çevrimiçi sistemlerde gerek gerçek dünyada güvenliğe verilen önem ve duyulan ihtiyaç her geçen artmaktadır. İnsan tanımlama ve kimlik doğrulama, çevrimiçi güvenlik sistemleri ve gözetim sistemleri için önemli bir unsurdur. Bu alandaki sorunlara biyometri kavramı ortak bir cevap geliştirmiş ve fenomen olarak literatürde de kabul görmüştür.

1.1. Biyometri

Bir insanın kimliği, o kişinin eşsiz olmasıyla tanımlanabilir. Bu anlamda biyometri kavramı ancak bireyin davranış karakteristiğini analiz etmek ve incelemek için kullanılabilir. Günümüzde kullanılan biyometri sistemleri, insanın davranışsal ve fizyolojik özelliklerine dayanmaktadır (Connor & Ross, 2018; Doroz, Kudlacik, & Porwik, 2018; Kekre & Bharadi, 2011; Kekre, Bharadi, & Sarode, 2011).

İnsan vücuduna ait biyometrik özellikler incelendiğinde bunlar arasında göz, parmak izi, insan yüzü, retina, iris ve imza gibi özellikler başta gelecektir. Kullanıcılar tarafından unutulması ya da çalınabilmesi gibi riskleri bulunan token ya da şifre bazlı geleneksel doğrulama sistemleriyle kıyaslandığında biyometrik sistemler kullanıcılara daha verimli, güvenli ve sağlıklı bir alternatif sunabilmektedir. Kişisel tanımlama ve doğrulama için alternatif bir yol olan biyometrik sistemler kullanıcıların hafızasından ya da üçüncü şahıslar tarafından çalınması ihtimallerinden etkilenmezler. Biyometrik özellikler temel olarak iki gruba ayrılırlar, psikolojik ve davranışsal biyometrik özellikler. Psikolojik özellikler, parmak izi, iris, retina, yüz gibi özelliklerin ölçümüdür. Davranışsal biyometrik özellikler denildiğinde ise ses ve imza gibi özellikler sayılabilmektedir. Davranışsal özelliklerden olan imzanın benzersiz olması sayesinde veriler yetkisiz kişilerden korunmaktadır. Biyometrik özellik olarak imza, imza edinimi ve tanıma yöntemleri temelinde çevrimiçi ve çevrimdışı olarak sınıflandırılmaktadır. Çevrimiçi imza doğrulama kullanıcı kimliğinin doğrulanması aşamasında imzanın dinamik özelliklerini kullanmaktadır. Çevrimdışı imza doğrulama yönteminde ise kullanıcı imzası atıldıktan resim olarak saklanır ve kullanılır. Kişisel kimlik doğrulama yöntemi olarak imzanın yaygın kullanımı sayesinde çevrimiçi ve çevrimdışı imza tanıma sistemleri literatürde önem arz eden bir araştırma alanı olmuştur (Ito, Ohyama, Wakabayashi, & Kimura, 2012; Kawazoe, Ohyama, Wakabayashi, & Kimura, 2010; Muramatsu & Yagi, 2013; Radhika & Gopika, 2015).
Biyometrik kimlik doğrulması Şekil 1'de görüldüğü gibi birden fazla adıma sahip bir süreçtir. İşlem adımları sırasıyla imzanın yakalandığı veri edinme aşaması, ön işleme aşaması, sonrasında özellik çıkarma aşaması ve sınıflandırılma işleminin yapılması aşamalarından oluşmaktadır (Radhika & Gopika, 2015).

Şekil. 1. İmza aşamalarının işlenmesi.

1.2. Bulut Bilişim

Bulut bilişim, uzak sunucuların büyük kümelerinin, bilgisayar hizmetlerine ve merkezi veri depolama veya kaynaklarına çevrimiçi erişimi sağlamak için bilgisayarların oluşturduğu ağdır. Bulut bilişim, her zaman kullanıma hazır, isteğe bağlı ağ erişimini, marjinal yönetim çabası veya servis sağlayıcı ara yüzü ile hızlı bir şekilde hazırlanıp serbest bırakılabilen yapılandırılabilir ve paylaşımlı bilgi işlem kaynaklarına yetkilendirmek için kullanılan bir sistemdir (Mell & Grance, 2011).

Bulut bilişimin önemli özelliklerinden bazıları şunlardır:

- İsteğe bağlı kendi kendine servis
- Geniş ağ erişimi
- Kaynak havuzu
- Hızlı esneklik
- Ölçülü servis

Bulut uygulamaları, üç ana hizmet modelinden biri olarak sunulmaktadır.

- Hizmet Olarak Yazılım (Software as a Service – SaaS)
- Hizmet Olarak Platform (Platform as a Service – PaaS)
- Hizmet Olarak Altyapı (Infrastructure as a Service – IaaS)

Bulut kurulumu, aşağıdaki gibi beş farklı dağıtım modelinde dağıtılmıştır.

- Özel Bulut (Private Cloud)
- Topluluk Bulut (Community Cloud)
- Hibrit Bulut (Hybrid Cloud)
- Genel Bulut (Public Cloud)

Özetle, bulut altyapısının beş temel özelliği, üç servis modeli ve dört dağıtım modeli vardır (Ghazouani & Slimani, 2017; Mell & Grance, 2011; Singh & Chatterjee, 2017).

1.3. Bulut Bilişimde Biyometri

Bulut bilişim tarafından ele alınabilecek biyometrik sistemlerin kendilerine özel belirli gereksinimleri bulunmaktadır. Öncelikle, biyometrik sistemlerde büyük öneme sahip olan hesaplama mantığı, biyometrik tanıma sistemlerinde olduğu gibi, bazı yerel işlem birimlerinde değil, bulutta bulunur. Bu özellik, bulut tabanlı biyometrik teknolojiyi geniş ölçüde erişilebilir, kullanılabilir ve uygulanabilir kılar ve diğer tüketici ve güvenlik uygulamalarına entegrasyon için gerekli altyapıyı sağlar.

Bu alanda bir diğer önemli nokta ise depolama konusudur. Biyometrik verilerin bulutta depolanması, sistemi yüksek oranda ölçeklendirebilir ve teknolojinin giderek artan bir kullanıcı tabanına hızlı ve güvenilir bir şekilde uyarlanmasını sağlamaktadır. Getirdiği avantajların yanında bu alanda bazı endişeler de bulunmaktadır. Örneğin, biyometrik verilerin bulutta depolanması gizlilikle ilgili endişeleri artırabilir ve ulusal mevzuata uygun olmayabilir. Son olarak, biyometrik teknolojinin bir bulut uygulamasını kullanması, gerçek zamanlı ve paralel işlem yetenekleri, kullanıma göre faturalandırma gibi bulutun tüm değerlerini bünyesinde barındırmaktadır.

1.4. Sis Bilişim

Bulut bilişim, yüksek hesaplama gücü ve depolama kapasitesi nedeniyle verileri işlemenin verimli bir yolu olarak kullanılmıştır (Armbrust et al., 2010; Fernando, Loke, & Rahayu, 2013). Ancak, bulut bilişim yaklaşımı merkezi bir hesaplama modeli olduğundan, hesaplamaların çoğu bulutta gerçekleşmektedir. Bu yaklaşıma göre, tüm verilerin ve isteklerin merkezi bulutlara iletilmesi gerektiği anlamına gelmektedir. Veri işleme hızı teknolojisi hızla artmış olmasına rağmen, ağ bant genişliği kayda değer ölçüde artmamıştır. Her ne kadar hesaplama ve veri işleme hızı gücü yeterli olsa dahi büyük miktarda veri için ağ bant genişliği problemi bulut bilişimin darboğazı haline gelmektedir. Bu problem uzun gecikmelere neden olabilmektedir. Ancak günümüzde

akıllı taşımada kullanılan trafik ışık sistemleri, akıllı sağlık merkezleri, acil durumlar ve diğer gecikmeye duyarlı uygulamalarda verilerin aktarılmasından kaynaklanan gecikme kabul edilemez (Arkian, Diyanat, & Pourkhalili, 2017; Qiu, Zheng, Song, Han, & Kantarci, 2017; Yu, Songqing, Peng, & Brown, 2015). Ayrıca, bazı kararlar buluta aktarılmak zorunda kalmaksızın yerel alanda yapılabilir. Bazı kararlar bulutta yapılsa bile, tüm veriler karar verme ve analiz için yararlı olmadığından, tüm verilerin işlenmesi ve saklanması için buluta gönderilmesi gerekli değildir hatta efektif değildir. Bir anlamda, gecikme, ağ bant genişliği, güvenlikle ve güvenilirlik ilgili büyük verinin aşırı büyümesinin neden olduğu bu zorluklar, yalnızca bulut modeline bağlı olarak ele alınamaz.

Bu sorunların üstesinden gelmek için, cloudlet tarafından yerel süreç ve depolamayı gerçekleştirmek ve ağ aktarımı ile gecikme miktarını azaltmak için kullanıcılara yakın yerlerde bulunan hesaplama kaynaklarını kullanması önerilmiştir (Min, Yixue, Yong, Chin-Feng, & Di, 2015). Optimal işletim algoritması ile birleştirildiğinde, cloudlet sistemi hesaplama, iletim, depolama ve iletişim maliyetleri düşük bir sistem haline gelmektedir (Y. Zhang, Niyato, & Wang, 2015).

Ağ kenarı aygıtlarını ve bulut merkezini sorunsuz bir şekilde bütünleştiren sis bilişim, bu sınırlamaların ele alınabilmesi için daha etkili bir çözüm olarak sunulmaktadır. Sis bilişim, coğrafi olarak dağıtılmış bir bilgisayar mimarisi olup, ağın kenarındaki çeşitli aygıtlar, her zaman uyumlu bir şekilde, esnek hesaplama, iletişim ve depolama hizmetleri sağlamak için birbirine bağlanmaktadır (Yi, Hao, Qin, & Li, 2015). Sis bilişimin en belirgin özelliği, bulut hizmetinin ağın kenarına genişletilmesidir. Yerel kaynakları bir araya getirerek son kullanıcıya hesaplama, iletişim, kontrol ve depolama imkânı sunmaktadır. Veriler coğrafi olarak dağıtılmış ağ kenar cihazları tarafından yönetilmektedir. Bu sayede, veri aktarım süresi ve ağ aktarımının miktarı büyük ölçüde azaltılabilmektedir (Datta, Bonnet, & Haerri, 2015). Sis paradigması, gecikmeye duyarlı veya gerçek zamanlı uygulamaların taleplerini karşılayabilir ve özellikle ağ bant genişliği darboğazlarını rahatlatabilir.

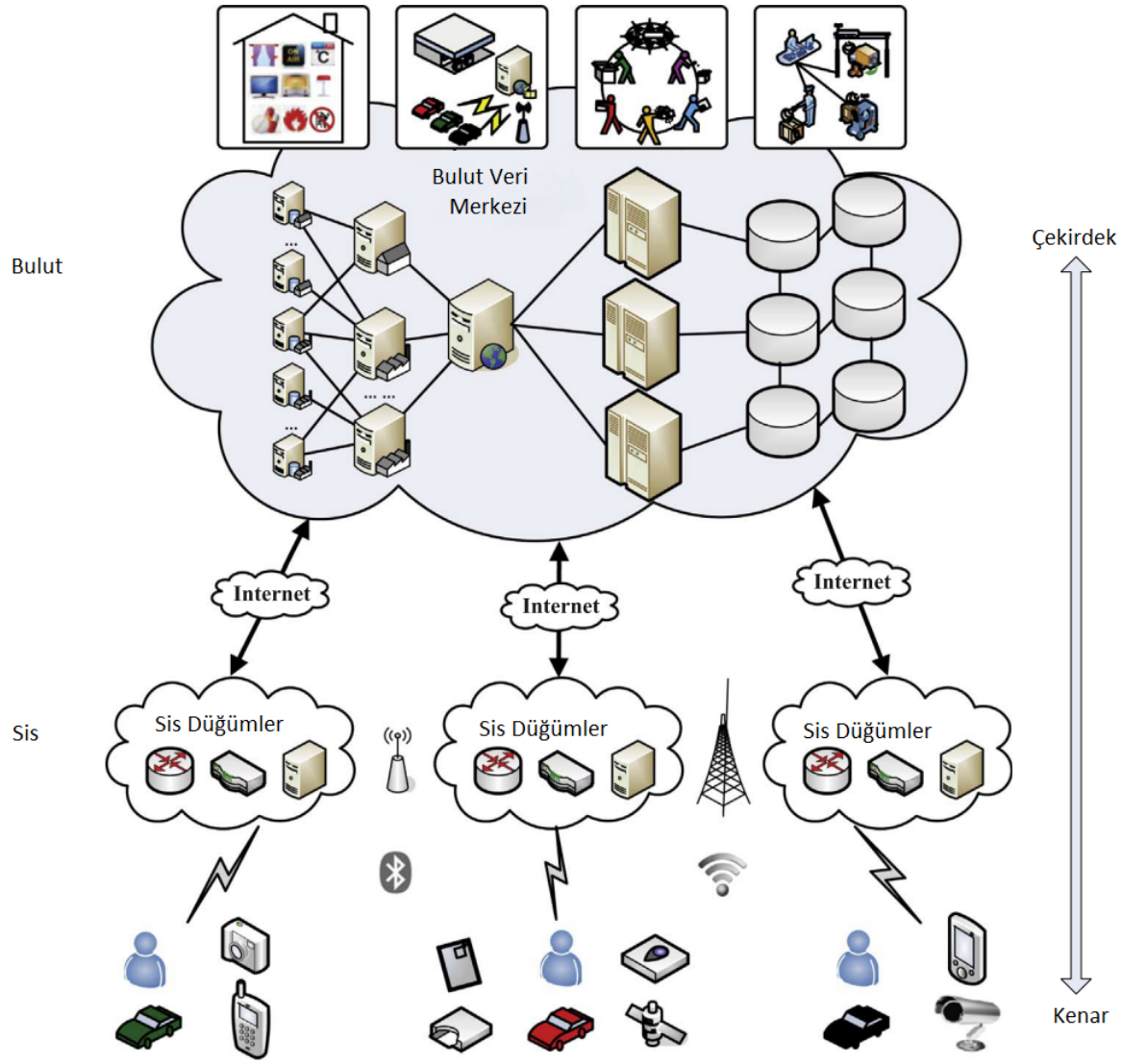
Sis bilişim mimarisi, düşük gecikme, yüksek güvenilirlik ve güvenlik, yüksek performans, hareketlilik ve birlikte çalışabilirlik konularında bu zorlukları karşılamak için uç cihazlar ve bulut arasında ekstra kaynak açısından zengin bir katman eklemektedir (Stojmenovic & Wen, 2014; Yi et al., 2015). Sis platformu, çok sayıda sis düğümlerinden oluşmaktadır. Sis düğümleri, bazı sanal kenarlı veri merkezleri bile dâhil olmak üzere, bu aygıtlardaki çeşitli ağ kenarı aygıtlarını ve yönetim sistemlerini içermektedir (H. Zhang et al., 2016). Sis bilişim, kenar kullanıcılar ile bulutlar arasında köprü görevi görmektedir. Bir yandan sis düğümleri, uç cihazlar ve kullanıcılarla bağımsız olarak bilgi işlem, hesaplama ve depolama hizmetleri sağlamak için mobil internet, bluetooth veya wireless gibi kablosuz bağlantı aracılığıyla bağlantı kurmaktadır. Öte yandan, bulutun zengin bilgi işlem ve depolama kaynaklarını tam olarak kullanabilmek için sis düğümleri de internet ile bulut ile bağlanabilmektedir (Aazam & Huh, 2016). Sis bilişim yaklaşımı, düşük gecikmeli veri analizi ve karar verme becerilerine uygun bir mimariye sahiptir.

Sis bilişimin, bulut bilişiminin yerine bulut bilişimin genişletilmesi ve genişletilmesi olduğu görülmektedir. Sis düğümleri, sensörler ve kenar aygıtları tarafından oluşturulan bu verileri işler ve saklar. Daha sonra kalan değerli veriler depolama veya sonraki işlemler için bulut sunucusuna aktarılmaktadır. Geleneksel bulut bilişim modeli ile iş birliği sayesinde, sis bilişim bulut bilişimin değerini daha etkili bir şekilde oynamasına ve daha yeşil bir bilgi işlem platformu olarak hizmet etmesine yardımcı olmaktadır (Hajibaba & Gorgin, 2014; Yannuzzi, Milito, Serral-Gracia, Montero, & Nemirovsky, 2014).

1.5. Sis Bilişim Mimarisi

Sis bilişim geleneksel bulut bilişimin, özelliklerinin ve imkânlarının ağın kenarına kadar genişletilmesine imkân sağlayan yeni bir hesaplama yaklaşımıdır. Bulut bilişim yaklaşımın aksine ağ kenarında kontrol, iletişim, depolama, hesaplama ve servis yetenekleri sağlamaktadır. Sis bilişim ile geleneksel bulut bilişimin farklarının daha net ifade edilebilmesi için sis bilişim mimarisinin ve özelliklerinin incelenmesi gerekmektedir.

Sis bilişime ait kesin bir referans mimari modelinin ortaya konulmamış olmakla beraber literatürde sıkça çalışmalar yapılan bir araştırma konusu haline gelmiştir. Son yıllarda sis bilişime ait bir dizi referans mimari önerilmiştir. Literatürde sis bilişime ait geliştirilen referans mimari modelleri çoğunlukla üç temel katmandan oluşmaktadır. Sis bilişim mimarisinin temelinde yatan en önemli yaklaşım ağ kenarında bulunan son aygıtlarla bulut arasına bir sis katmanı eklemektir. Sis bilişime ait hiyerarşik mimari Şekil 2'de gösterildiği gibidir (Aazam, Zeadally, & Harras, 2018a; Tang et al., 2017).



Şekil. 2. İmza aşamalarının işlenmesi (Aazam et al., 2018a; Tang et al., 2017).

Şekil 2'de gösterilen sis bilişime ait referans mimari modeli aşağıdaki üç katmandan oluşmaktadır.

- Terminal Katmanı : Terminal katmanı sis bilişimin fiziksel ortama ve son kullanıcıya en yakın olduğu katmandır. Cep telefonları, akıllı kartlar, sensörler gibi son kullanıcıda bulunan cihazların bu alanda yer almaktadır. Bu katmanda bulunan cep telefonu ya da tabletler kendilerine ait işlem gücüne sahip olsa da bu gücü sadece kendi amaçları doğrultusunda kullanmaktadırlar. Bu katmanda bulunan cihazların temel görevi olayların veya fiziksel nesnelerinin algılanması ve bu işlem sonucu elde edilen verilerin depolama ve işlem için mevcut mimaride bulunan üst katmana gönderilmesinden sorumludurlar.

- Sis Katmanı : Bulut ile terminal katmanı arasında bulunan sis katmanı ağın kenarında bulunmaktadır. Sis katmanı genellikle erişim noktaları, ağ geçitleri, yönlendiriciler, temel istasyonları, sunucular gibi cihazları içeren çok fazla sayıda sis düğümlerinden oluşmaktadır. Bu sis düğümleri bulut ile son cihazlar arasında dağılmış olarak alışveriş merkezleri, kamu kurumları, sokaklar, kafeler, caddeler gibi alanlarda barındırılmaktadırlar. Sis düğümler sabit bir yer olabileceği gibi hareketli bir taşıyıcıda mobil olarak da bulunabilirler. Son kullanıcıda bulunan cihazlar hizmet almak için sis düğümlerine bu yöntemlerle rahatça bağlantı kurabilirler. Sis düğümler son kullanıcıdan aldıkları verileri iletmek, geçici olarak depolamak ve işleme gibi yeteneklere sahiptirler. Gerçek zamanlı işlem yapmak zorunda olan gecikme toleransı bulunmayan uygulamalar bu katmanda işlemlerini yapmaktadırlar. Bahsedildiği gibi bu katmanda bulunan sis düğümleri IP ağı üzerinden buluta bağlanabilmektedir ve daha güçlü depolama ve veri işleme gücü gerektiğinde bu bağlantı üzerinden bulutla iletişime geçme çalışma gibi yetenekleri bulunmaktadır.

- Bulut Katmanı : Bulut katmanı bünyesinde birden fazla depolama cihazı ve yüksek performanslı sunucu aygıtlarından oluşmaktadır. Yüksek işlem kapasitesi ile başarılı hesaplama analizi ve güçlü depolama aygıtları ile büyük veriyi saklama gibi yetenekleri bünyesinde barındırmaktadır. Ancak sis bilişimde geleneksel bulut bilişimin yaklaşımının aksine tüm işlem ve depolama görevleri bulut bilişim tarafında yürütülmez.

Sis bilişim mimarisinde, her son cihaz bir kablosuz veya kablolu erişim altyapısı ile sis düğümlerine bağlanmaktadır. Kablosuz erişimde özellikle WiFi, 4G, 3G, Bluetooth gibi kablosuz erişim teknolojilerinden faydalanılmaktadır. Yine mimari sonucu olarak sis düğümleri de kendi aralarında bağlantı kurabilme yetisine sahiptirler ayrıca her bir sis düğüm IP ağı üzerinden buluta bağlanmaktadır. Bulut tabanlı uygulamalarda buluttan gelecek cevap işlem gücüne, ağ hızına veya sunucu yüklerine bağlı olarak uzun sürebilmektedir. Bulut bilişim ile sis bilişimin detaylı karşılaştırılması Tablo 1'de sunulmaktadır (Aazam et al., 2018a; Aazam, Zeadally, & Harras, 2018b; Díaz, Martín, & Rubio, 2016; Mahmud, Srirama, Ramamohanarao, & Buyya, 2018; Nobre et al., 2019; Salman, Elhajj, Chehab, & Kayssi, 2018).

Tablo 1. Bulut bilişim ile sis bilişimin karşılaştırılması.

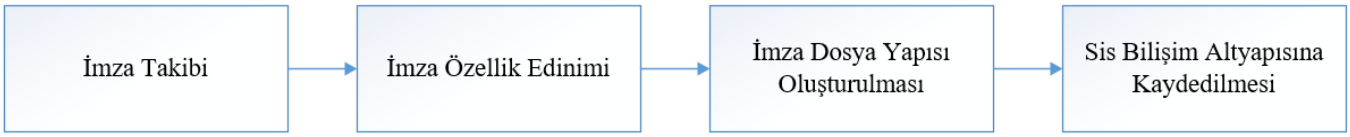
	Bulut Bilişim	**Sis Bilişim**
Gecikme	Yüksek	Düşük
Gerçek zamanlı etkileşim	Destekli	Destekli
Yer farkındalığı	Kısmen destekli	Destekli
Hesaplama ve depolama yetenekleri	Güçlü	Zayıf
Bant genişliği maliyetleri	Yüksek	Düşük
Sunucu düğüm sayısı	Az	Çok
Coğrafi dağılım	Merkezi	Merkezi olmayan ve dağıtılmış
Enerji tüketimi	Yüksek	Düşük
Son cihazlara olan mesafe	Uzak	Yakın
Hizmet yeri	Internet ile	Lokal ağ kenarında
Çalışma ortamı	Özel veri merkezi	Dış ya da iç mekân
İletişim yöntemi	IP ağı	Kablosuz ya da kablolu bağlantı
Mobilite	Sınırlı	Destekli

Tablo 1'de görüldüğü üzere geleneksel bulut bilişimde bulunan kimi aksaklıklar veya eksiklikler sis bilişim ile giderilmiş ve daha efektif ve stabil yaklaşım geliştirilmiştir.

Bu çalışmada servis tabanlı bir imza doğrulama yöntemi geliştirilmiştir; geliştirilen yöntem bir senaryo üzerinde test edilmiş ve sonuçları tartışılmıştır.

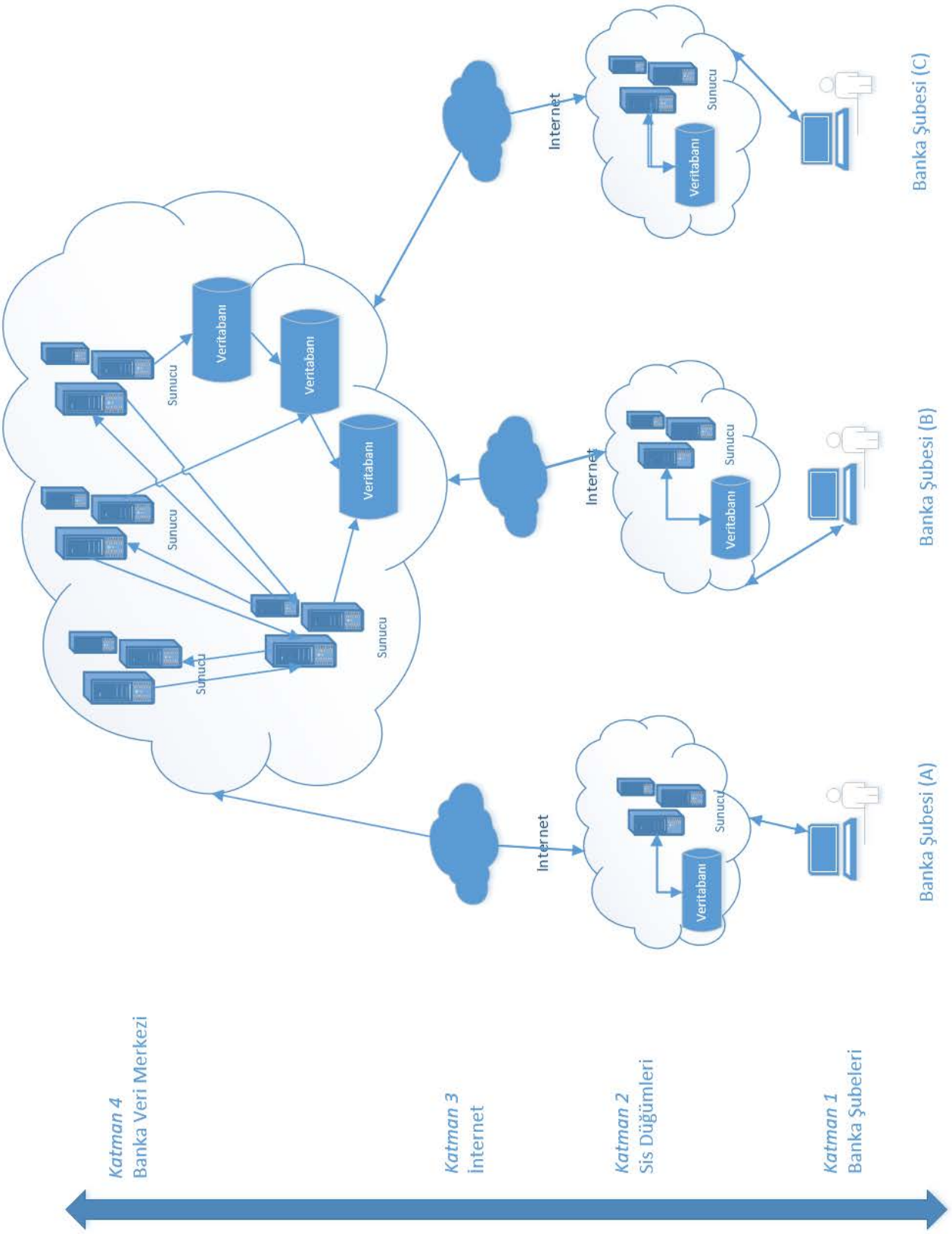
2. ÇALIŞMANIN KAPSAMI

Çalışmaya ait adımlar Şekil 3'te gösterilmektedir. Öncelikle kullanıcıların imzaları takip edilerek kayıt altına alınmaktadır. Kayıt edilen imza literatürde kullanılan imza özellik edinim yöntemleri ile dijital hale getirilmektedir. Elde edilen verilerle imza dosya yapısı oluşturulmaktadır. Çalışmaya özel oluşturulan imza dosya yapısı sis bilişim alt yapısına kaydedilmektedir.



Şekil. 3. Çalışmanın adımları

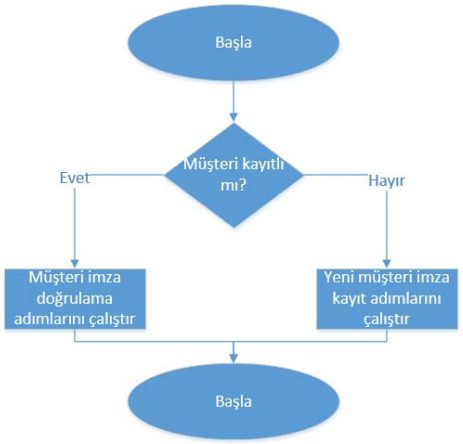
Literatürde bulunan imza doğrulama yöntemleri bulut bilişim alt yapısına uygulanmıştır ancak sis bilişim alt yapısına uygun bu tarz bir uygulamaya rastlanmamıştır. Ayrıca geliştirilen sistemin kullanımının ve uygunluğunun tartışılması için bir senaryo oluşturulmuştur. Şekil 4'te gösterilen senaryo bir bankaya ait olup geliştirilen yöntem bu senaryo üzerinde değerlendirilmiştir.



Şekil. 4. Banka senaryo tasarımı

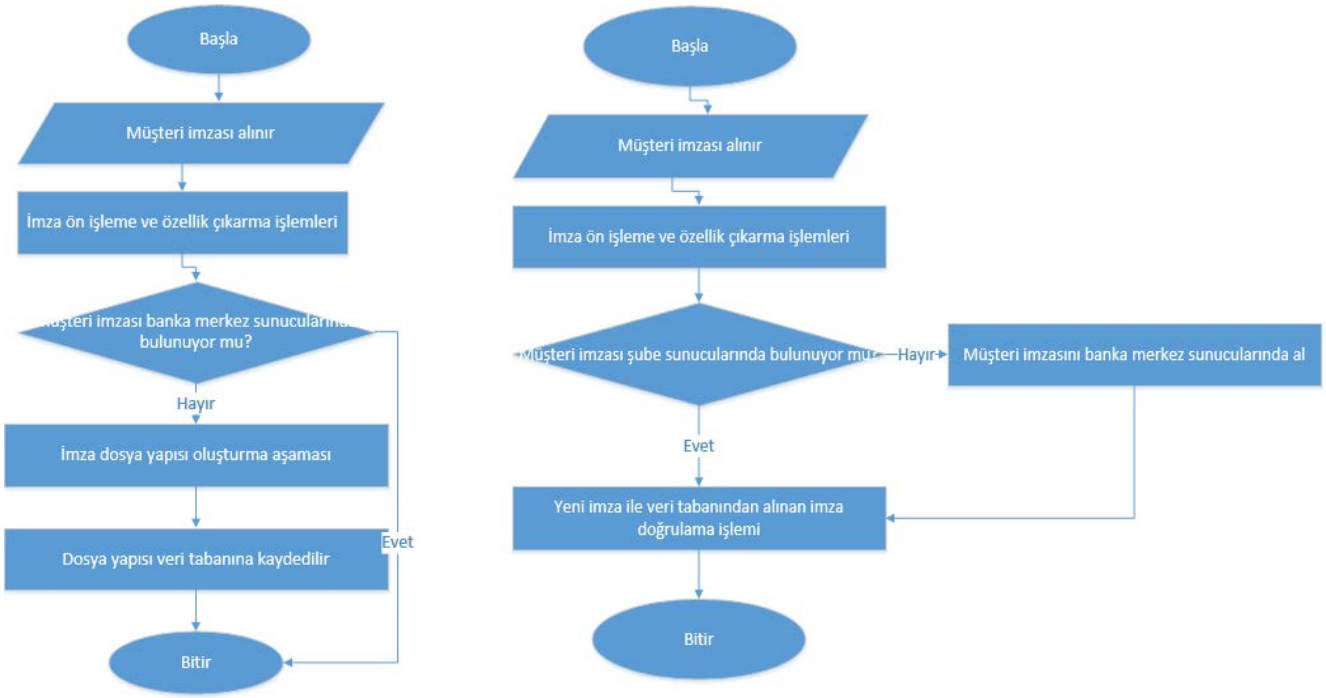
Şekil 4'te gösterilen senaryo 4 katmandan meydana gelmektedir. Senaryoda bulunan katmanlar ve katmanlarda bulunan görevler sırasıyla aşağıdaki gibi tanımlanmaktadır.

- Katman 1 : Senaryonun ilk katmanı olan bu katman banka ile müşterinin temas sağladığı katmandır. İlk defa gelen müşteriye ait imzanın tanıtıldığı ve müşteriye ait verinin ilk defa okunduğu ya da daha önce kayıtlı olan müşterinin yaptığı işlemde imza doğrulama işleminin kontrol edildiği katmandır. Bu katmana ait detaylı akış diyagramı Şekil 5'te görülmektedir.



Şekil. 5. Banka senaryo katman 1 akış diyagramı

- Katman 2 : Senaryonun ikinci katmanı bankanın ya da bankanın bağlı olduğu bir üst şubenin verilerinin işlendiği ve tutulduğu sunucuların barındırıldığı katmandır. Bu katmanda müşteriden alınan veriler sunucu aracılığıyla işlenir ve imzaya ait özellikler elde edilir. Bu edinim işlemi sonrasında imza dosya yapısı oluşturulur ve sonraki işlemler için veri tabanına kaydedilir. Bu işleyişe ait akış şeması Şekil 6a'da gösterilmektedir. Bu sisteme daha önce kaydedilmiş ve banka sisteminde var olan müşteri için imza doğrulama aşamasında sorgulamanın yapıldığı ve imza doğruluğunun kıyaslandığı aşama bu katmanda yer almaktadır. Bu işleyişe ait akış şeması Şekil 6b'de gösterilmektedir.
-



Şekil. 6(a). Banka senaryo katman 2 yeni müşteri akış diyagramı **(b).** Banka senaryo katman 2 var olan akış diyagramı

- Katman 3 : Senaryonun bu katmanında banka şubelerine ait küçük sis düğümleri ile bankanın büyük veri merkezi arasındaki iletişim sağlanmaktadır. İnternet üzerinden sağlanan bu iletişim servis tabanlı oluşturulmuş. Ancak bu iki nokta arasında yapılacak tüm iletişim güvenli şekilde yapılması gerekmektedir. Bu nedenle servis tabanlı sistem

üzerinde yapılan tüm haberleşme ve kurulan mimari güvenli hiper metin aktarım iletişim protokolü üzerinden yapılacak şekilde tasarlanmıştır.

- Katman 4 : Senaryonun dördündü katmanı bankanın tüm verilerinin tutulduğu banka veri merkezinden oluşmaktadır. Burada bankaya ve bankanın hizmet verdiği müşterilere ait tüm bilgiler tutulmakta ve tüm sistemlerin üzerinde çalıştığı sunucular bu katmanda barındırılmaktadır.

3. METODOLOJİ

3.1. İmza Edinim Aşaması

Çalışmanın bu aşamasında giriş verisi olan kullanıcı imzasını aldıktan sonra yapılacak adımlar tanımlanmaktadır. Bu adımda giriş verisini daha hassas ve işlenebilir hale getirmek için bir ön işlem uygulanmaktadır. Ön işlem adımında otsu algoritması, normalizasyon, morfolojik operasyonlar ve medyan filtresi uygulanmaktadır. Bir sonraki adımda özellik edinimi yapılmaktadır. Bu işlemde her imzanın dikey ve yatay özellikleri yerel ve global özellikler olarak belirlenmektedir. Bu aşamada belirtilen global özellikler en boy oranı, genişlik, yükseklik, imza alanı, normalizasyon işlemi uygulanmış imza yüksekliği gibi özelliklerdir. Yerel özellikler ise imzanın ağırlık merkezi, açı, mesafe ve eğim gibi temel özelliklerini barındırmaktadır. Bu aşamada kullanılacak yola ait algoritma adımları Tablo 2'de gösterilmektedir.

Tablo 2. İmza edinim aşaması algoritma adımları.

Adım	İşlem
Adım 1:	Başla
Adım 2:	Giriş imzası görüntüsünü oku
Adım 3:	Resmi ikili sisteme dönüştür
Adım 4:	Resme normalizasyon işlemi uygula
Adım 5:	Resmi daha kullanışlı hale getirmek için morfolojik işlemleri uygula
Adım 6:	Medyan filtre ile görüntüdeki gürültüyü kaldırın
Adım 7:	Yatay ve Dikey özellikleri ayıkla
Adım 8:	Eğim, mesafe ve açıyı ayıkla
Adım 9:	Genel özellikleri ayıkla
Adım 10:	Bitir

Kullanıcı imzasını kâğıt üzerine alındıktan sonra bir tarayıcı aracılığıyla görüntü sayısal veri haline dönüştürülür. Bu aşamada gerçekleştirilen ilk işlem giriş verisi olan imzanın ikili resmi almak ve imza özelliklerinin edinimi için Otsu segmentasyonu algoritması uygulanır. Elde edilen ikili görüntü sonraki aşamalarda ya da işlemlerde kullanılmak üzere 256 x 256 boyutlarında yeniden boyutlandırılırlar. Ardından görüntüdeki verimin artırılması için morfolojik işlemler uygulanırlar. Ancak bu işlem sırasında görüntü üzerinde gürültü oluşabilmektedir. İmzayı daha kullanışlı kılmak, oluşan gürültüyü ortadan kaldırmak ve doğrulama oranını artırmak için medyan filtreleme uygulanmaktadır. Adımlara ait detaylar çalışmanın bu aşamasında sunulmaktadır.

3.1.1. Otsu segmentasyonu

Görüntü bölümleme adımında, giriş verisi olan imza görüntüsü uygun bilgiyi elde etmek için ikili görüntüye ayrılır. Bu segmentasyonun en önemli özelliği imzanın arka plandan ayrılmasıdır yani ön planda duran imzanın arka plandan ayrılarak kullanılabilir hale dönüştürülmesidir. Bu amaçla en sık kullanılan algoritma Otsu segmentasyonudur. Otsu segmentasyonunun hesaplanması için, ilk olarak, gri ölçekli görüntüdeki her yoğunluk seviyesine ait histogramı ve olasılık hesaplanmaktadır (Otsu, 1979). Her yoğunluk seviyesinin başlangıç ağırlıkları, ortalama ve ölçeklendirme parametresi sıfıra ayarlanır. Maksimum yoğunluk değerinin elde edilmesinde bir eşik değeri tanımlanmıştır. Eşik değeri yinelerse de toplam yoğunluk değerleri sayısı yürütülür. Tüm tekrarlarda ağırlıklar ve ölçeklendirme parametresi değerleri güncellenir. Eşik değeri, maksimum yoğunluk değeri olarak seçilir.

3.1.2. Normalizasyon işlemi

Otsu segmentasyonu sonrasında elde edilen çıktı olan ikili imza görüntüsü bu aşamanın giriş parametresidir. Bu adımda bölümleme işlemi uygulanmış görüntü 256 x 256 olarak yeniden boyutlandırılmaktadır. Yeniden boyutlandırılmış görüntüye çıkarma işlemi uygulanır. Bu işlemin amacı, bölümlere ayrılmış görüntünün maksimum yoğunluk değerini elde etmektir. Bu alan resimde imzalı bölgeyi barındırmaktadır.

3.1.3. Morfolojik işlemleri

Normalizasyon aşamasından sonra, normalize edilmiş görüntüde incelme ve kapama olarak adlandırılan iki morfolojik işlem uygulanır. Morfolojik işleme, bir görüntüdeki özelliklerin şekli veya morfolojisi ile ilgili doğrusal olmayan işlemlerin bir koleksiyonudur. Morfolojik operasyonlar sadece piksel değerlerinin göreceli olarak sıralanmasına dayanır bu nedenle özellikle

ikili görüntülerin işlenmesi için uygundur. Morfolojik teknikler, bir yapı elemanı olarak adlandırılan küçük bir şekle veya şablona sahip bir görüntüyü işler. Yapılandırma elemanı, görüntüdeki tüm olası konumlara yerleştirilir ve ilgili piksel komşusuyla karşılaştırılır. İkili bir görüntü üzerinde morfolojik bir işlem, pikselin sadece sıfırdan büyük bir değere sahip olduğu yeni bir ikili görüntü oluşturur (Efford, 2000).

3.1.4. Medyan filtreleme

Normalizasyon işlemi uygulanmış görüntüye morfolojik işlemler uygulanması aşamasında görüntüye gürültü eklenmesi ihtimali meydana gelmektedir. Bu gürültünün görüntüden çıkartılması bir zorunluluktur, bölümlere ayrılmış görüntüye 3 x 3 medyan filtresi uygulanmaktadır (Zhou & Zhang, 1999). Bu işlem sonrasında görüntüde oluşan gürültü giderilmiş olur.

3.2. Özellik çıkarımı

Çalışmanın özellikler çıkarma aşamasında imzaya ait global özellikler elde edilmektedir. İmza görüntüsüne ait özellikler ve denklemleri Tablo 3'te gösterilmektedir.

Tablo 3. Global özellikler ve eşitlikleri.

Özellik	Eşitlik
En boy oranı	$\frac{Width}{Height}$
Siyah piksel alanı	$\sum_{i}^{w}\sum_{j}^{h} I\,(i,j)$
İmzanın saf genişliği	$\max(sum(I,1)$
İmzanın saf yüksekliği	$\max(sum(I,2)$
Normalleştirilmiş imza yüksekliği	$\frac{Saf\ genişlik}{Saf\ yükseklik}$
Alan	$\emptyset^{A} = \sum_{i=1}^{n}\sum_{j=1}^{m} A[i,j]$

3.3. İmza Dosya Yapısının Oluşturulması

Elde edilen tüm özelliklerin veri tabanına kaydedilmesi ve sorgulama aşamasında kullanılabilmesi için probleme özel bir dosya yapısı geliştirilmiştir. Dosya yapısında yer alan bilgiler ve kapladıkları alan Şekil 7'de gösterilmektedir.

Banka Numarası	Müşteri Numarası	Şube Numarası	Şube Server Numarası	Dosya Oluşturulma Tarihi	En boy Oranı	Siyah piksel alanı	İmzanın saf genişliği	İmzanın saf yüksekliği	Normalleştirilmiş imza yüksekliği	Alan
long	long	long	long	datetime	float	float	float	float	float	float
8 byte	8 byte	8 byte	8 byte	8 byte	4 Byte	4 Byte	4 Byte	4 Byte	4 Byte	4 Byte

Şekil. 7. İmza dosya yapısı

Tasarlanan dosya yapısında aramaya imkân vermek ve arama performansını geliştirmek için bölümlere ayrılarak tasarlanmıştır. Aranan dosyanın hangi bankaya ait dosya olduğunu ilk aşamada tespit edebilmek için dosyanın ilk bilgisi olarak banka numarası belirlenmiştir. Bankaya ulaşıldıktan sonra şube bilgileri yerine Müşteri numarası bilgisi eklenmiştir. Bu yaklaşım kendi içerisinde iki nedene sahiptir. Bunlardan ilki, her müşteri imzasını kendi şubesinde vermiş olamayabileceğinden müşterinin şubesine gitmek imzanın bulunmamasına sebep olabilir. Bu nedenle banka bilgisinden sonra müşteri numarası bilgisine yer verilmiştir. İkinci neden ise banka numarası bilgisine erişildikten sonra, o bankaya ait müşteri numarası tekil değer olmaktadır. Bu nedenle banka ve müşteri numarasına öncelik tanınmıştır. Geliştirilen dosyada yer alan bir diğer bilgi şube numarasıdır. Burada belirtilen şube bilgisi müşterinin bağlı bulunduğu banka şubesi değildir, müşterinin ilgili imzayı verdiği şube numarasıdır. Şube sunucu numarası geliştirilen dosya sisteminde barındırılan bir diğer bilgidir. Sis bilişim yapısında gösterildiği üzere her bankanın kendisine ait bir sunucusu bulunmaktadır, aranan imzanın hangi sunucuda barındırıldığının bilinmesi büyük önem taşımaktadır. Ayrıca imza dosyasının ilk oluşturulma tarihi veri bütünlüğünün sağlanması için dosya yapısına eklenmiştir. Tablo 3'te gösterilen global değişkenler dosya yapısına sırasıyla eklenmiştir. Şekil 7'de gösterilen dosya yapısı imza dosyasının başlığı niteliğinde geliştirilmiş olup sonrasında imza dosyası bulunmaktadır.

3.4. Sis Bilişim Altyapısı

Müşteri imzasına ait Tablo 3'te gösterilen özellik edinilmiştir. Şekil 7'de gösterilen probleme özgü geliştirilen imza dosya yapısı ile imzaya ait bilgiler ve imza dosyası oluşturulmuştur. Müşterinin imzasının alındığı şube sunuculara kaydedilmiştir. Bu sayede sonraki sorgulama ve güncelleme aşamalarında internet üzerinden buluta erişmeye gerek kalmaksızın şubenin kendi sunucularında tüm işlemler yapılabilecektir. Ayrıca geliştirilen imza dosya yapısı buluta gönderilerek kayıt edilmesi sağlanmaktadır. Bu yaklaşım sayesinde müşteriler başka bir şubeden ve hatta bankadan dahi işlem yapsalar tüm detaylar bulutta da tutulduğundan herhangi bir problem olmaksızın en hızlı şekilde erişim sağlanacak ve müşteri imzası kontrol edilecektir.

4. SONUÇ

Bu çalışmada literatürde yoğun çalışmalar yapılan sis bilişim alt yapısı kullanılarak bir imza doğrulama yaklaşımı geliştirilmiştir. Geliştirilen yazılım çerçevesi imzaların sıklıkla kullanıldığı kurumlardan olan bankalara özel bir senaryo üzerinde kurgulanmıştır. Sunulan çerçeve, imza ön işleme süreçlerini, probleme özel geliştirilen imza dosya yapısının oluşturulması ve sis bilişime kayıt edilmesinden oluşan üç ana aşamadan oluşmaktadır. Çalışma ile geliştirilen mimari, imza doğrulama kullanan kurum ve kuruluşlara sis bilişim mimarisi konusunda rehberlik etmektedir. Yapılan çalışma ile elde edilen tespitler, sonuçlar ve öneriler aşağıda listelenmiştir.

- Bulut bilişim, güncel teknolojiler arasında popülerliğini korumaya devam etmektedir.
- Bulut bilişim, maliyetleri azaltan ve genişlemeye uygun bir yaklaşıma sahiptir.
- Sis bilişim, bulut bilişimde yer alan eksiklikleri ya da açıklıkları kapatmaktadır. Bulut bilişim mimarisini güçlendiren ve daha güvenli hale getiren bir yaklaşımdır.
- Sis bilişim, bant genişliği konusunda bulut bilişimden daha hassastır ve veri giriş veya çıkış işleminin yoğun olduğu bankalar, üniversiteler gibi yerel sunucular ile çalışmaları mümkün olan daha kritik kurumlara ya da şirketlere uygundur.
- Biyometrik yöntemler arasında yer alan imza halen en sık kullanılan güvenlik araçları arasındadır.
- İmza gibi biyometrik verilerin doğrulanması aşamasında gözle kontrol yerine bilgisayar tabanlı kontroller hataları önleyerek güvenliği artıracaktır.
- Sis bilişimin kritik güvenlik önemine sahip sistemlerde bulut bilişim yerine kullanılması uygun görülmektedir.

REFERANSLAR

Aazam, M., & Huh, E.-N. (2016). Fog Computing: The Cloud-IoT\/IoE Middleware Paradigm. IEEE Potentials, 35(3), 40-44. doi:10.1109/mpot.2015.2456213

Aazam, M., Zeadally, S., & Harras, K. A. (2018a). Fog Computing Architecture, Evaluation, and Future Research Directions. IEEE Communications Magazine, 56(5), 46-52. doi:10.1109/mcom.2018.1700707

Aazam, M., Zeadally, S., & Harras, K. A. (2018b). Offloading in fog computing for IoT: Review, enabling technologies, and research opportunities. Future Generation Computer Systems, 87, 278-289. doi:10.1016/j.future.2018.04.057

Arkian, H. R., Diyanat, A., & Pourkhalili, A. (2017). MIST: Fog-based data analytics scheme with cost-efficient resource provisioning for IoT crowdsensing applications. Journal of Network and Computer Applications, 82, 152-165. doi:10.1016/j.jnca.2017.01.012

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., . . . Rabkin, A. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50. doi:10.1145/1721654.1721672

Connor, P., & Ross, A. (2018). Biometric recognition by gait: A survey of modalities and features. Computer Vision and Image Understanding, 167, 1-27. doi:10.1016/j.cviu.2018.01.007

Datta, S. K., Bonnet, C., & Haerri, J. (2015). Fog Computing architecture to enable consumer centric Internet of Things services. 1-2. doi:10.1109/isce.2015.7177778

Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications, 67, 99-117. doi:10.1016/j.jnca.2016.01.010

Doroz, R., Kudlacik, P., & Porwik, P. (2018). Online signature verification modeled by stability oriented reference signatures. Information Sciences, 460-461, 151-171. doi:10.1016/j.ins.2018.05.049

Efford, N. (2000). Digital Image Processing: A Practical Introduction using Java (1 edition ed.): Pearson.

Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. Future Generation Computer Systems, 29(1), 84-106. doi:10.1016/j.future.2012.05.023

Ghazouani, S., & Slimani, Y. (2017). A survey on cloud service description. Journal of Network and Computer Applications, 91, 61-74. doi:10.1016/j.jnca.2017.04.013

Hajibaba, M., & Gorgin, S. (2014). A Review on Modern Distributed Computing Paradigms: Cloud Computing, Jungle Computing and Fog Computing. Journal of Computing and Information Technology, 22(2), 69. doi:10.2498/cit.1002381

Ito, T., Ohyama, W., Wakabayashi, T., & Kimura, F. (2012). Combination of Signature Verification Techniques by SVM. 430-433. doi:10.1109/icfhr.2012.192

Kawazoe, Y., Ohyama, W., Wakabayashi, T., & Kimura, F. (2010). Improvement of On-line Signature Verification Based on Gradient Features. 410-414. doi:10.1109/icfhr.2010.70

Kekre, H. B., & Bharadi, V. A. (2011). Dynamic signature pre-processing by modified digital difference analyzer algorithm, New Delhi.

Kekre, H. B., Bharadi, V. A., & Sarode, T. K. (2011). Dynamic signature using time based vector quantization by Kekre's median codebook generation algorithm, New Delhi.

Mahmud, R., Srirama, S. N., Ramamohanarao, K., & Buyya, R. (2018). Quality of Experience (QoE)-aware placement of applications in Fog computing environments. Journal of Parallel and Distributed Computing. doi:10.1016/j.jpdc.2018.03.004

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. U.S. Department of Commerce Computer Security Division Information Technology Laboratory: NIST.

Min, C., Yixue, H., Yong, L., Chin-Feng, L., & Di, W. (2015). On the computation offloading at ad hoc cloudlet: architecture and service modes. IEEE Communications Magazine, 53(6), 18-24. doi:10.1109/mcom.2015.7120041

Muramatsu, D., & Yagi, Y. (2013). Silhouette-based online signature verification using pen tip trajectory and pen holding style. 1-8. doi:10.1109/icb.2013.6612958

Nobre, J. C., de Souza, A. M., Rosário, D., Both, C., Villas, L. A., Cerqueira, E., . . . Gerla, M. (2019). Vehicular Software-Defined Networking and fog computing: Integration and design principles. Ad Hoc Networks, 82, 172-181. doi:10.1016/j.adhoc.2018.07.016

Otsu, N. (1979). A Threshold Selection Method from Gray-Level Histograms. IEEE Transactions on Systems, Man, and Cybernetics, 9(1), 62-66. doi:10.1109/tsmc.1979.4310076

Qiu, T., Zheng, K., Song, H., Han, M., & Kantarci, B. (2017). A Local-Optimization Emergency Scheduling Scheme With Self-Recovery for a Smart Grid. IEEE Transactions on Industrial Informatics, 13(6), 3195-3205. doi:10.1109/tii.2017.2715844

Radhika, K. S., & Gopika, S. (2015). Online and Offline Signature Verification: A Combined Approach. Procedia Computer Science, 46, 1593-1600. doi:10.1016/j.procs.2015.02.089

Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). IoT survey: An SDN and fog computing perspective. Computer Networks, 143, 221-246. doi:10.1016/j.comnet.2018.07.020

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115. doi:10.1016/j.jnca.2016.11.027

Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. 2, 1-8. doi:10.15439/2014f503

Tang, B., Chen, Z., Hefferman, G., Pei, S., Wei, T., He, H., & Yang, Q. (2017). Incorporating Intelligence in Fog Computing for Big Data Analysis in Smart Cities. IEEE Transactions on Industrial Informatics, 13(5), 2140-2150. doi:10.1109/tii.2017.2679740

Yannuzzi, M., Milito, R., Serral-Gracia, R., Montero, D., & Nemirovsky, M. (2014). Key ingredients in an IoT recipe: Fog Computing, Cloud computing, and more Fog Computing. 325-329. doi:10.1109/camad.2014.7033259

Yi, S., Hao, Z., Qin, Z., & Li, Q. (2015). Fog Computing: Platform and Applications. 73-78. doi:10.1109/HotWeb.2015.22

Yu, C., Songqing, C., Peng, H., & Brown, D. (2015). FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation. 2-11. doi:10.1109/nas.2015.7255196

Zhang, H., Xiao, Y., Bu, S., Niyato, D., Yu, R., & Han, Z. (2016). Fog computing in multi-tier data center networks: A hierarchical game approach. 1-6. doi:10.1109/icc.2016.7511146

Zhang, Y., Niyato, D., & Wang, P. (2015). Offloading in Mobile Cloudlet Systems with Intermittent Connectivity. IEEE Transactions on Mobile Computing, 14(12), 2516-2529. doi:10.1109/tmc.2015.2405539

Zhou, W., & Zhang, D. (1999). Progressive switching median filter for the removal of impulse noise from highly corrupted images. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 46(1), 78-80. doi:10.1109/82.749102