BİLGİSAYAR BİLİMLERİ VE TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Araştırma Makalesi

# DtyPAM: Kurumsal Destek Firmaları için Önerilmiş Konteynır Tabanlı Ayrıcalıklı Erişim Yönetim Sistemi

**Hamza Kürşat ŞİMŞEK*[1], Halil ARSLAN[1], Yasin GÖRMEZ[2]**

*[1]Sivas Cumhuriyet Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, Sivas, Türkiye*
*[2]Sivas Cumhuriyet Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri, Sivas, Türkiye*

**Anahtar Kelimeler:**
Ayrıcalıklı erişim yönetim,
Uzaktan destek,
Uzaktan çalışma,
Kod olarak altyapı,
Mikroservis

**ÖZ**

Bilişim alanında önceki zamanlarda da uygulanan uzaktan destek ve uzaktan çalışma kavramları, 2019 yılında başlayan ve tüm dünyayı etkisi altına alan COVID-19 salgını ile hemen hemen tüm sektörler tarafından uygulanmaya başlamıştır. Ölçeği ne olursa olsun bütün girişimler dijital uygulamaları kullanmakta ya da kullanma planı yapmaktadır. Özellikle holding düzeyindeki firmalar, birçok iş sürecini karmaşık kurumsal kaynak planlama uygulamaları üzerinden yürütmektedir. Bu uygulamalar içinse genellikle dış kaynaklardan destek almakta ve bu destekler günümüzde sıklıkla uzaktan yapılmaktadır. Bu aşamada kurumlar güçlü bir erişim yönetim sistemine ihtiyaç duymaktadırlar. Bahsedilen sebeplerden ötürü çalışmamızda, uzaktan bağlantı ve destek süreçlerinin sanal masaüstü ve kod olarak alt yapı teknolojileri kullanılarak otomatik şekilde yapılabileceği bir ayrıcalıklı erişim yönetim sistemi önerilmiştir. Tasarlanan sistem ile kullanıcılara, bağlantı sağlanacak sunucuda yapılacak olan iş için en az düzeyde ayrıcalık verilmesi hedeflenmektedir. Bir sunucuya yapılan bağlantıların geriye dönük takibinin rahatlıkla yapılabilmesi için, çalışma sonucu önerilmiş olan ayrıcalıklı erişim yönetim uygulamasına güçlü bir kayıt defteri sistemi (log) eklenmiştir. Çalışmamızda konteynır teknolojileri kullanılarak mikro-servis tabanlı bir sistem önerilmiş bu sayede platform bağımsız çalışan bir sistem elde edilmesi amaçlanmıştır. Çalışmamız sonucunda elde edilen sistemin kod olarak altyapı ve konteynır teknolojilerini birlikte kullanan ilk ayrıcalıklı erişim yönetim sistemi olduğu değerlendirilmektedir.

# DtyPAM: Container Based Privilege Access Management System for Corporate Consulting Companies

**Keywords:**
Privilege Access management,
Remote support,
Remote work,
Infrastructure as code,
Microservice

**ABSTRACT**

The concepts of remote support and remote work, which have been applied in the field of information technology in the past, began to be implemented by almost all sectors with the onset of the COVID-19 pandemic in 2019, affecting the entire world. Regardless of scale, all enterprises are using digital applications or planning to use them. Especially at the level of holding companies, many business processes are conducted through complex enterprise resource planning applications. These applications often require support from external sources, and such support is frequently provided remotely in today's world. In this context, organizations need a robust access management system. For the reasons mentioned above, in our study, we propose a privileged access management system that can automatically perform remote connection and support processes using virtual desktop and code as infrastructure technologies. The designed system aims to provide the minimum level of privilege to users for the tasks to be carried out on the connected server. To facilitate the retrospective tracking of connections to a server, a strong registry system (log) has been added to the privileged access management application recommended as a result of the study. In our study, a microservices-based system using container technologies is proposed, aiming to achieve a platform-independent system. The system obtained as a result of our study is considered to be the first privileged access management system that uses both code infrastructure and container technologies.

***Sorumlu Yazar**

*(h.kursatsimsek@gmail.com) ORCID ID 0009-0009-5274-8698
(harslan@cumhuriyet.edu.tr) ORCID ID 0000-0003-3286-5159
(yasingormez@cumhuriyet.edu.tr) ORCID ID 0000-0001-8276-2030

**e-ISSN: 2717-8579**
**Geliş Tarihi: 12/07/2023; Kabul Tarihi: 01/12/2023**

## 1. GİRİŞ

Ayrıcalıklı Erişim Yönetimi (Privilege Access Management - PAM), ayrıcalıklı kullanıcıların bir dizi güvenlik işlevi ve süreci aracılığıyla sistemlere veya kaynaklara nasıl eriştiklerini kontrol eden, yöneten ve raporlayan bir kimlik güvenliği çözümüdür. PAM, herhangi bir sisteme erişimi denetlemek için kullanılabilir, ancak genellikle etki alanı denetleyicileri ve üretim sunucuları gibi yüksek değerli kaynaklara daha sık uygulanır (Garbis & Chapman, 2021).

PAM, herhangi bir kuruluşun güvenlik stratejisinin temel bir bileşenidir. Bu sistemler, yalnızca yetkili kullanıcıların belirli görevleri yerine getirebilmesini ve hassas verilere erişebilmesini sağlayarak, kuruluş içindeki ayrıcalıklı hesapların ve erişim düzeylerinin kullanımını kontrol etmek ve izlemek için tasarlanmıştır. Bu amaç doğrultusunda iyi bir PAM çözümü iki faktörlü kimlik doğrulama, belirli eylemler için onay talep etme ve tüm etkinlikler için bir denetim izi sağlama gibi süreçleri de barındırmalıdır. PAM çözümünün en önemli faydalarından biri, sistemlere ve verilere yetkisiz erişimi engellemeye yardımcı olmasıdır. Kurum çalışanları, farklı sistemlere bağlantı için bağımsız üyelikler kullanabilmektedir. Bu durumda işten ayrılan bir personel üyeliklerinin iptal edilmesi karmaşık bir hal almakta, gözden kaçan durumlarda ise kötü niyetli personellerin ihlaller yapabilmesine zemin oluşturulmaktadır. PAM çözümleri üyelik sistemlerini tek bir noktada toplayarak, işten çıkan personellerin tüm sistemlere ve verilere erişiminin hızlı ve kolay bir şekilde iptal edilmesini sağlamaktadır. Bu yapısı sayesinde çalışanların neden olduğu veri ihlallerine ve diğer güvenlik olaylarına karşı korunmaya yardımcı olur. Ayrıcalıklı bir erişim yönetim sisteminin diğer bir yararı ise endüstri düzenlemelerine ve standartlarına uygunluğun sağlanmasına yardımcı olmasıdır. Örneğin, sağlık veya finans gibi denetime tabii sektörlerde, hassas verilere erişimde katı kontroller istenebilmektedir. PAM çözümü işletmeler için ekstra bir güvenlik katmanı sağlarken, hassas veriler için kontrollerin yapılabilmesine yardımcı olmaktadır. PAM, harici saldırganlar ve kazara veri ihlalleri gibi çeşitli tehditlere karşı koruma sağladığı için siber güvenliğin en önemli yönlerinden biri olarak değerlendirilmektedir (Garbis & Chapman, 2021). Tüm bu faydaların yanı sıra iyi bir PAM çözümü;

- Hassas verilere ve kritik sistemlere erişimi yalnızca yetkili kullanıcılarla sınırlayarak, bu bilgilere yetkisiz erişimi ve kötüye kullanımı önlemeye yardımcı olur.
- İçeriden gelen tehditler, genellikle bir kuruluşun sistemlerine ve verilerine yasal erişime sahip oldukları için özellikle zarar verici olabilir. PAM, kullanıcıların erişimini, görevlerini yerine getirebilmek için gereken minimumla sınırlayarak ve çok faktörlü kimlik doğrulama gibi kontroller uygulayarak içeriden gelen tehdit riskini azaltmaya yardımcı olur.
- Dış saldırganlar, oturum açma kimlik bilgilerini çalarak veya tahmin ederek bir kuruluşun sistemlerine ve verilerine erişmeye çalışabilir. Ayrıcalıklı erişim yönetimi, güçlü parolalar ve parola yönetimi çözümleri uygulayarak bu saldırıların önlenmesine yardımcı olur.
- Kazara veri ihlalleri, yetkili kullanıcılar hata yaptığında veya ayrıcalıklarını kasıtlı olarak kötüye kullandığında meydana gelebilir. Ayrıcalıklı erişim yönetimi, kullanıcıların erişimini yalnızca ihtiyaç duydukları kaynaklarla sınırlayarak ve etkinlik izleme gibi denetimler uygulayarak bu ihlallerin etkisini azaltmaya yardımcı olur.

Bu çalışmada PAM çözümlerinin tüm bu özellikleri dikkate alınarak, kurumsal destek sistemlerine entegre olabilen modern ve yerli ayrıcalıklı erişim sistemi içeren, host bağımsız masaüstü altyapısı üzerinden oturumları yönetebilen, kod olarak altyapı (Infrastructure as Code - IaC) ile kullanıcı kurulumlarına gerek kalmadan hazır sistem sunabilen, olası bağlantı sayısının limit sorununu çözebilen, güçlü bir aksiyon kayıt sistemi barındıran, kimlik bilgileri güvenliği sağlayarak yönetim süreçlerinin kolaylaştıran ve sürekli erişilebilir olan bir PAM sistemi önerilmiştir. Önerilen sistemin geliştirilmesi sürecinde konteynır teknolojileri kullanılarak mikro-servis mimarisi kullanılmıştır. Sistemin ana amaçlarından birisi, uzak sunuculara erişim için güvenlik ve ayrıcalık sağlamaktır. Uzak sunuculara erişim için ssh ve rdp gibi farklı ağ protokolleri kullanılmaktadır. Çalışma ile yapılacak uygulamada yerinde ve bulut üzerinde konumlandırılabilen, bilgi güvenliği ihmallerine karşı dirençli, farklı ağ protokolleri ile uyumlu ve ileride çıkabilecek yeni ağ protokollerine uyum sağlayabilecek bir PAM sisteminin tasarlanması amaçlanmaktadır. Sistemin mikro-servis tabanlı geliştirileceği için her bir ağ protokolü için farklı bir mikro-servis geliştirilecektir. Uzaktan erişim için yeni bir ağ protokolünün gerekli olması durumunda sadece o ağ protokolü için bir mikro-servis geliştirilecek, bu sayede sistemin tümünde değişiklik yapmadan yeni ağ protokolleri sisteme eklenebilecektir. Tasarlanan sistem ile kullanıcılara, bağlantı sağlanacak sunucuda yapılacak olan iş için en az düzeyde ayrıcalık verilmesi hedeflenmektedir. Bir sunucuya yapılan bağlantıların geriye dönük takibinin rahatlıkla yapılabilmesi için, çalışma ile tasarlanacak olan PAM uygulamasına güçlü bir kayıt defteri sistemi (log) eklenmesi düşünülmektedir. Eklenecek olan bu kayıt sisteminin, veri madenciliği ve iş zekâsı gibi analizlere de uyumlu olması, platformun ölçeklenebilmesi ve sürekli çalışabilmesi ise çalışmamızın diğer amaçları arasında yer almaktadır.

### 1.1. Literatür araştırması

PAM sistemleri, bir kuruluş içindeki ayrıcalıklı kullanıcıların kritik kaynaklara erişimini güvence altına almak için tasarlanmıştır. PAM çözümleri, kullanıcı erişimi üzerinde ayrıntılı kontrol sağlar, kullanıcı etkinliğini izler ve en az ayrıcalık ilkelerini uygular. Kuruluşlar, iş süreçlerini yürütmek için dijital varlıkları gün geçtikçe daha sık kullanmaktadırlar. Bu doğrultuda ayrıcalıklı hesaplara ve kaynaklara erişimi güvence altına almak, firmaların güvenliğini ve teknolojik değişime uyumunu sürmesi için büyük önem arz etmektedir. Bu bağlamda literatürde PAM çözümleri için birçok çalışma yapılmıştır. Tep ve diğerleri bulut sistem atakları hakkında bir literatür araştırması yaparak temel güncel saldırılar ve bu saldırıları azaltma üzerine önerilerde bulunmuştur. Yaptıkları literatür araştırmasında elde ettikleri bilgileri kullanarak bir PAM çözümü önermiş ve önerdikleri sistemi irdelemişlerdir (Tep, Martini, Hunt, & Choo, 2015). Sindiren ve Ciylan çalışmalarında şirket içi atakları analiz ederek bu tür saldırıların azaltılması için önerilerde bulunmuşlardır. Bunun yanı sıra PAM çözümlerine katkı sağlamak için en az ayrıcalık verme, iş dağılımları ve sosyal mühendislik için personel bilinçlendirme süreçleri için prosedürler geliştirmişlerdir (Sindiren & Ciylan, 2018). Steinhoff yaptığı çalışma ile PAM limitlerini ve gereksinimlerini irdelemiş ve geliştirilen PAM sistemleri için konteynır teknolojilerinin kullanımının getireceği faydaları analiz etmiştir (Steinhoff, 2020). Tabrizchi ve diğerleri çalışmasında bulut bilişim bileşenlerinin güvenlik ve gizlilik açısından analizini yapmış, bu bağlamda karşılaşılan sorunları analiz etmiş ve bu sorunlara çözüm yolları önermişlerdir. Yapılan çalışma sonucu elde edilen çıktıların bulut üzerinde çalışan PAM sistemleri için ciddi fayda sağlayacağı ön görülmektedir (Tabrizchi & Kuchaki Rafsanjani, 2020). Purba yaptığı çalışma ile kuruluşların, kritik bilgi teknolojilerini varlıklarını korumak, uyumluluk düzenlemesini karşılamak ve veri ihlallerini önlemek için PAM kullanmasının önemini vurgulamış ve yayında kuruluşların ISO 27001 kontrolünü karşılayan PAM çözümü elde etmesi için önerilerde bulunmuştur (Anton & Soetomo, 2018). Sindiren ve Ciylan yaptıkları çalışmada imtiyazlı hesapları minimum maliyetle kontrol edebilmek, yönetebilmek ve takip edilebilmek için bir model tasarlamışlardır. Bu uygulama modeli, ayrıcalıklı kullanıcı hesaplarının parolalarının temel bilgi teknolojisi güvenlik ilkelerine uygun olarak belirlenmesinde ve daha güçlü parolaların oluşturulmasını katkı sağlamaktadır (Sindiren & Ciylan, 2019). Ylonen ve diğerleri yaptıkları çalışmada kuruluşların SSH kullanıcı anahtarlarının yönetimine odaklanarak bir kuruluşta SSH etkileşimli ve otomatikleştirilmiş erişim yönetiminin temelleri hakkında bilgi vermişlerdir (Ylonen, Turner, Scarfone, & Souppaya, 2015). D'Silva ve diğerleri yapmış oldukları çalışmada çevrimiçi korumaya ilişkin Sıfır Güven (Zero Trust) ilkesinin başarısını analiz etmişlerdir. Sıfır Güven uygulaması ve araştırması ile ilgili literatürü tarayarak gelecekteki ağ güvenliği için Sıfır Güven ilkesini irdelemiştir. Çeşitli saldırı türlerine yanıt veren mimariyi uygulamak için konteynır teknolojisini kullanmıştır. Açık sistem ara bağlantısı (Open Systems Interconnection) modelinin her katmanında Sıfır Güven Mimarisinin avantaj ve dezavantajlarına odaklanmıştır. Çalışma ile önerilmiş olan sistemin PAM alt yapılarında kullanılan sistemler için ciddi faydaları olacağı ön görülmektedir (D'Silva & Ambawade, 2021). Xu ve diğerleri yapmış oldukları çalışmada konteynır teknolojisini kullanarak dağıtılmış rol tabanlı erişim denetimi tabanlı bir kontrol mekanizması önermişlerdir. Konteynır tabanlı erişim kontrol mekanizmasının avantaj ve dezavantajlarını tartışarak yetki devri nedeniyle oluşabilecek tehlikeleri çözmek için önerilerde bulunmuşlardır (Lang, Jiang, Ding, & Bai, 2019). Alruwies ve diğerleri günümüz dünyasında sistemlere erişim yetki kontrolünün gerekliliğinden ve zorluklarından bahsettikleri çalışmada Active Directory tabanlı bir PAM sistemi önermişlerdir (Alruwies, Mishra, Abdul, & Alshehri, 2021). Ionita, PrivX isimli PAM uygulamasında çalışabilen bir veri tabanı güvenlik eklentisi geliştirmiştir. Geliştirmiş olduğu eklenti sonrasında yapay veri ile yapmış olduğu performans analizi sonucunda gecikme medyan değerinin 304 milisaniye olduğunu hesaplamış ve sağlanan güvenlikten dolayı bu gecikmenin kabul edilebilir olduğunu değerlendirmiştir (Ionita, 2023). Tran yapmış olduğu çalışmada bir sistemden başka bir sisteme erişim için kullanılacak PAM uygulamasının sistem bilgileri tanımlama, sistem protokolleri tanımlama, kimlik bilgileri kurulum sürecini belirleme ve kimlik bilgileri güncelleme olmak dört prosedürünü oluşturmuştur (Tran, 2020). Preuveneers ve Joosen PAM sistemlerini irdeledikleri çalışmalarında açık kaynak kodlu birleşik kimlik ve erişim yönetimi çözümü olan OpenAM kullanılarak sağlık hizmetleri için yeni bir prosedür oluşturmuşlardır (Preuveneers & Joosen, t.y.).

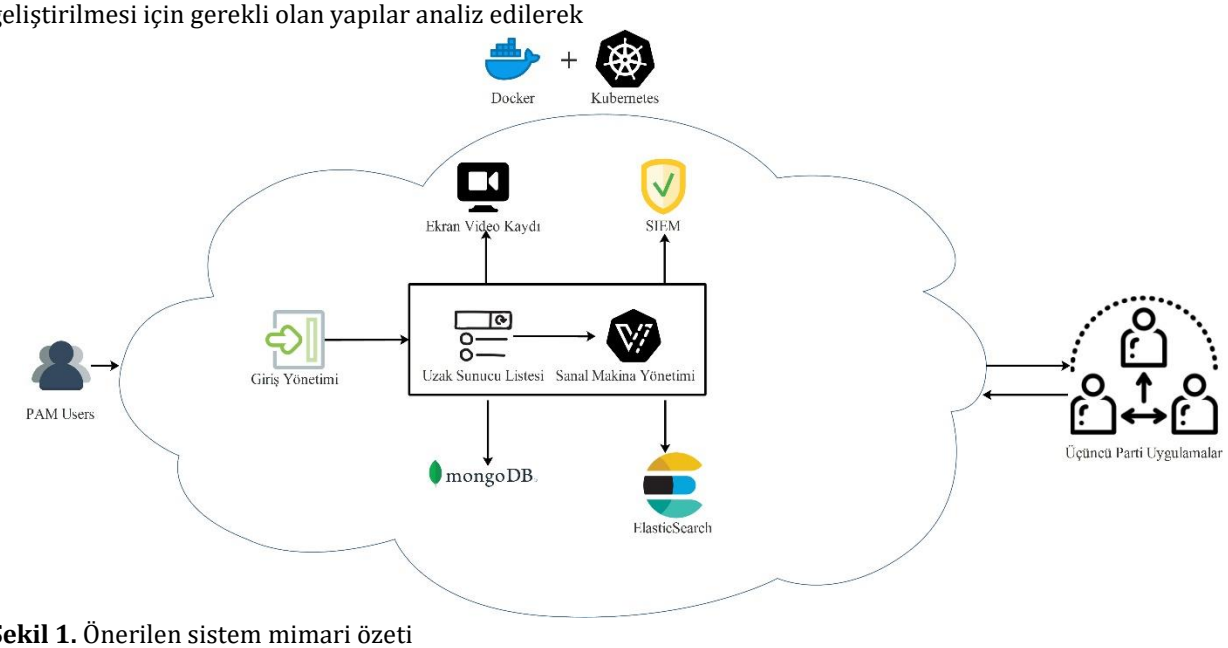
Literatürde var olan çalışmalar incelendiğinde ayrıcalıklı erişim yönetim sistemlerinin modern siber güvenlik stratejilerinin kritik bir bileşeni olduğu kanısına varılmıştır. PAM sistemlerinin, ayrıcalıklı kullanıcıların kritik dijital kaynaklara erişimini kontrol etmek ve izlemek için tasarlandığı ve hassas verilere veya sistemlere yalnızca yetkili kullanıcıların erişebildiğini sağladığı gözlemlenmiştir. Güvenlik gereksinimlerini operasyonel verimlilikle dengelerken, karmaşık ve heterojen ortamlarda çalışabilen kapsamlı ve uyarlanabilir PAM çözümlerinin önemli olduğu literatür araştırması sonucunda anlaşılmıştır.

Literatürde var olan çalışmalar incelenerek tasarlanmış olan önerilen sistemde, benzer çözümlerde bulunan özelliklerin bulunmasına dikkat edilmiştir. Bunun yanı sıra literatürde var

olan sistemlerin hiç birinde kod olarak alt yapı teknolojisi kullanılarak otomatik erişim kolaylığı sağlama özelliklerinin bulunmadığı görülmüştür. Önerilen sisteminin özgün yanı ise, uzaktan destek süreçlerinde kullanılmak üzere sanal makine tabanlı sistemlerin kod olarak teknolojisi ile konfigüre edilmesi olarak değerlendirilmektedir. Bu yapısı ile çalışmamızın, PAM araştırmalarına yeni bir vizyon kazandıracağı ön görülmektedir.

## 2. YÖNTEM

Çalışmamızda önerilen PAM sisteminin geliştirilmesi için gerekli olan yapılar analiz edilerek belirlenmiştir. Bu kapsamda sistemimizi geliştirmek için konteynır teknolojisi, konteynır orkestrasyon aracı, kod olarak altyapı geliştirme aracı, dokuman tabanlı veri tabanı, tam metin indeksleme aracı ve sanal makine konfigürasyon teknolojisine ihtiyaç duyulduğu kanaatine varılmıştır. Teknoloji dünyası araştırılarak bu isterileri karşılayacak açık kaynak kodlu yazılımlardan Docker, Kubernetes, IaC mimarisi, MongoDB, ElasticSearch ve Kubevirt çalışmamızda kullanılmak üzere tercih edilmiştir. Önerilen yöntemin mimari yapısı Şekil 1 ile gösterilmektedir.




**Şekil 1.** Önerilen sistem mimari özeti

### 2.1. Docker

Aynı işletim sistemi üzerinde birbirinden izole birden fazla işletim sisteminin çalıştırılabilmesine sanallaştırma denir. Sanallaştırma ile birlikte son zamanlarda konteynır yapısı da teknoloji dünyasında sıkça kullanılmaya başlanmıştır. Sanallaştırma teknolojilerinden farklı olarak daha küçük boyutlara ve bir fonksiyonu çalıştırmak için minimum sistem gereksinimlerine sahip olması, konteynır teknolojisinin sanallaştırmaya alternatif olarak kullanılmasının önemli sebeplerindendir. Önerilen sistemin taşınabilir, diğer sistemlerden yalıtılmış ve buluta dağıtılabilir olması için konteynır yapısından faydalanılmış ve bu kapsamda Docker teknolojisi kullanılmıştır ("Docker Documentation", 200M.S.).

### 2.2. Kubernetes

Konteynır teknolojilerinin kullanım sıklığının artması ile birlikte özellikle yatay ölçekleme yapabilmek, sistemi sürekli ayakta tutabilmek ve sistem sağlığını kontrol edebilmek için konteynır orkestrasyon araçları kullanılmaya başlanmıştır. Konteynır teknolojileri önermiş olduğumuz sistemde de hemen hemen tüm servisleri sanallaştırmak için kullanılacaktır. Bu kapsamda, gelen trafiği ve konteynırları organize edebilmek için kubernetes konteynır orkestrasyon aracından faydalanılmıştır ("Kubernetes Documentation", t.y.).

### 2.3. Kod olarak altyapı (Infrastructure as Code – IaC)

Alt yapının manuel olarak yapılandırılması yerine makine tarafından okunabilir tanım dosyaları aracılığı ile sağlandığı ve yönetildiği sistem Kod Olarak Altyapı (Infrastructure as Code – IaC) denmektedir ("Infrastructure as Code", 2023). Önermiş olduğumuz sistemde farklı ihtiyaçları karşılamak üzere oluşturulmuş birçok sistemin bulundurulması ve zaman içerisinde bu sistemlere ekleme yapılabilmesi hedeflenmektedir. Bu bağlamda önerilen sistemde özelleştirilebilir sanal masaüstü görüntüleri oluşturabilmek ve sunabilmek için IaC mimarisinden faydalanılmıştır ("Infrastructure as Code", 2023).

### 2.4. Dokuman tabanlı veri tabanı

Dokuman tabanlı (NoSQL) veri tabanı, ilişkisel veri tabanından farklı olarak örnekler arasında ilişki kurmak yerine örnekleri bir veri modeli

sayesinde dosya yapısında saklamaktadır. Kullanmış olduğu veri modeli sayesinde hızlı sorgular atabilmekte, yatay ölçeklenebilir şemalar sağlamakta ve diğer veri tabanı tabloları ile ilişkilendirme yapmaya gerek olmadan json ve xml gibi formlarda veri depolayabilmektedir. Çalışmada önerilen sistemde kullanılacak olan uzun vadeli kayıt sistemlerinin saklanması için açık kaynak kodlu ve dokuman tabanlı MongoDB teknolojisinden faydalanılacaktır ("What Is NoSQL?", t.y.).

### 2.5. Elasticsearch

NoSQL veri tabanları, dosya arama, silme ve düzenleme gibi işlemlerde ilişkisel veri tabanlarına göre daha hızlı olsa da gerçek zamanlı veri işlemleri için yeterli hızlara ulaşamamaktadır ("Elasticsearch vs MongoDB - A Detailed Comparison of Document-Oriented Databases | SigNoz", 2023). Bu kapsamda büyük, dağınık ve tek başlarına anlamsız veri topluluklarında hızlı arama yapabilmek için tam metin indeksleme araçlarından faydalanılmaktadır. Çalışmamızda kısa süreli kayıtlara hızlı erişim ve görüntüleme işlemleri için Apache Lucene temelinde Java programlama dili ile yazılmış Elasticsearch teknolojinden faydalanılacaktır ("Elasticsearch", t.y.).

### 2.6. Kubevirt

KubeVirt, sanal makinelerin kubernetes üzerinde çalıştırılmasını sağlayan açık kaynaklı bir sanal makine yönetim sistemidir. KubeVirt, bir Kubernetes konteynır orkestrasyon aracı içinde Çekirdek tabanlı Sanal Makine (Kernel-based Virtual Machine - KVM) kullanarak konteynır orkestrasyon aracında yerel sanallaştırma sağlar. KubeVirt ile hem sanallaştırma yönetimini hem de kubernetes konteynır orkestrasyon aracı düzenlemesi yapılabilmektedir. Bu çalışmada kubernetes kümesindeki konteynırların yanında sanal makineleri de tek elden oluşturabilmek ve yönetebilmek amacıyla KubeVirt sisteminden faydalanılmıştır ("Getting to Know Kubevirt", 2018).

## 3. UYGULAMA

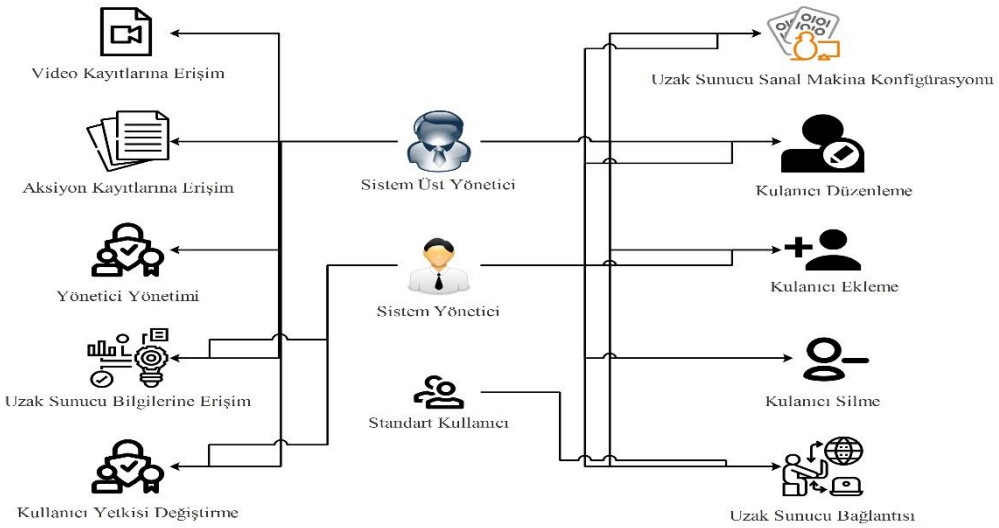
Çalışmamızda, konteynır teknolojileri kullanılarak mikro-servis tabanlı bir PAM sistemi önerilmiştir. Önerilen sistemin güvenliğini artırmak için çok faktörlü doğrulama gerektiren bir giriş sistem geliştirilmiştir. Kod olarak altyapı teknolojisi sayesinde uzak sunucu erişim süreçlerinin, sistem yöneticisi tarafından konfigüre edilmesi sağlanacak bu sayede çalışan eforu azaltılacaktır. Oturum açma ve uzak sunucu bağlantı süreçlerinin tamamı ekran video kayıt sistemi ile tutulacak bu sayede güvenlik ihlalleri rahatlıkla tespit edilebilecektir. Bu sistemin aşamaları Bölüm 3.1, 3.2 ve 3.3'te detaylı olarak anlatılmaktadır.

### 3.1. Önerilen sistem kullanıcı türleri ve sistem giriş adımları

Çalışma kapsamında önerilen sistemde üç farklı tip kullanıcı bulunmaktadır. Söz konusu kullanıcıların yetkileri dahilinde erişebileceği sistemler Şekil 2 de görülmektedir. Kullanıcıların yetki seviyeleri en az yetki seviyesinden en kapsamlı yetki seviyesine doğru; standart kullanıcı, sistem yöneticisi ve sistem üst yöneticisi olarak sıralanmaktadır. Bir üst yetki seviyesindeki kullanıcı alt seviyelerdeki kullanıcıların yetkilerine de sahip olacaktır. Bu kapsamda standart kullanıcı yalnızca uzak sunucu bağlantısı yapabilecektir. Sistem yöneticisi standart kullanıcı yetkisine ek olarak uzak sunucu bilgilerine erişim, kullanıcı yetkisi değiştirme, kullanıcı ekleme, silme ve düzenleme, video kayıtlarına erişim, uzak sunucu sanal makine konfigürasyonu yetkilerine sahip olacaktır. Sistem üst yöneticisi ise tüm yetkilere ek olarak aksiyon kayıtlarına erişim ve yönetici yönetim yetkilerine sahip olacaktır.

Giriş sisteminin temelde dört ana kontrolü yapması hedeflenmektedir. İlk olarak PAM sisteminde kullanıcının aktif olup olmadığı, daha sonra üçüncü parti uygulamalarla (personel bilgi sistemi, kurumsal kaynak planlama uygulamaları vb.) iletişime geçecek servis sayesinde kullanıcının firmadaki durumu, ardından kullanıcı adı ve şifre doğruluğu, son olarak ise ikinci faktör doğrulması kontrol edilecektir. Sisteme giriş sürecinde gerçekleştirilen bütün kontrol aşamaları Şekil 3 de detaylı olarak görülmektedir.

Kullanıcılar PAM kullanıcı ve şifre bilgileri ile sisteme giriş yapabilmek için talepte bulunacaktır. Giriş talebi sonrasında gerçekleştirilen PAM sistemi aktiflik kontrolü sonucunda kullanıcının pasif olması durumunda kullanıcı tekrardan sisteme giriş yapmaya yönlendirilecektir. Kullanıcının aktif olması durumunda ise üçüncü parti sistem aktiflik kontrolü yapılacaktır. Üçüncü parti sistem aktiflik kontrolü sonucunda aktif olmayan kullanıcılar PAM sistemi tarafından pasif kullanıcı olarak değerlendirilip kayıt defteri bildirimi yapılacaktır. Kontrol sonucunda aktif olarak değerlendirilen kullanıcılara ise şifre kontrolü yapılacaktır. Şifre kontrolü sırasında yanlış şifre girilmesi durumunda kullanıcı tekrar sisteme giriş aşamasına yönlendirilecektir. Şifre kontrolü aşamasında üç defa hatalı giriş yapan kullanıcı sistem tarafından pasif kullanıcı olarak değerlendirilip kayıt defteri bildirimi yapılacaktır. Şifre kontrolünü geçen kullanıcılar için ise ilk giriş ya da son şifre değişikliği kontrolü yapılacaktır.



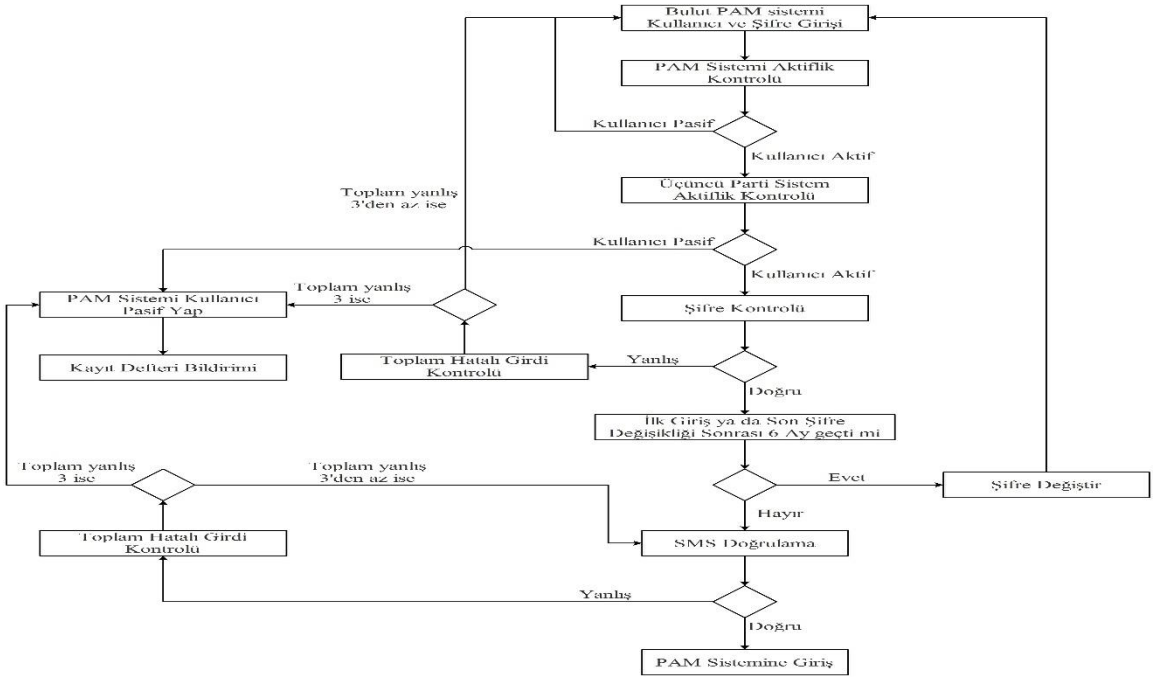

**Şekil 2.** Kullanıcı durum diyagramları

Kullanıcıların sisteme ilk kez girmesi veya son şifre değişikliği üzerinden altı ay geçmesi durumunda kullanıcıların şifrelerini değiştirerek tekrardan sisteme giriş talebinde bulunması gerekmektedir. Şifre değiştirmesine gerek olmayan kullanıcılar ise SMS doğrulama aşamasına yönlendirilecektir. SMS doğrulaması sırasında hatalı giriş yapan kullanıcıların tekrar doğrulama yapması istenecektir. Üç defa hatalı giriş yapan kullanıcılar sistem tarafından pasif kullanıcı olarak değerlendirilip kayıt defteri bildirimi yapılacaktır. SMS doğrulamasını geçen kullanıcılar ise PAM sistemine giriş yapacaktır.

### 3.2. Önerilen sistem fonksiyonları

Bu çalışmada PAM sisteminde uzak sunuculara bağlanmak için sanal masaüstüler oluşturulmuş ve bağlantılar bu sanal masaüstüler üzerinden yapılmıştır. Uygulama sistemini özetleyen teknik mimari yapımız Şekil 1 de gösterilmiştir. Tasarlanan sistem üzerinden bağlantı yapmış her bir kullanıcı için farklı sanal masaüstü oluşturulacak ve uzak erişim istenen sunucu için bağlantı gereksinimlerini (vpn, rdp, ERP bağlantısı, ayar dosyası vb.) bu sanal masaüstünde otomatik olarak oluşturulmuştur. Aynı sunucuya yapılmış olan her bir bağlantı için, kullanıcı bilgileri ile ilgili sanal masaüstü çalıştırılmıştır. Bu kapsamda sistem için bir sanal masaüstü yöneticisi olan, açık kaynak kodlu kubernetes, konteynır ve VDI teknolojilerinden faydalanılmıştır.

Tasarlanan PAM sistemi tek bir noktadan yönetilmiştir.




**Şekil 3.** Önerilen sistem girişi akış diyagramı

Erişim aşamalarında sanal masaüstü kullanılmış olduğu ve bağlantının kişisel bilgisayar yerine sanal masaüstü üzerinden yapılmış olduğu göz önüne alındığında fiziki kaynaklardan ötürü aynı anda yapılabilecek bağlantı sayısının bir limiti olacağı saptanmıştır. Bunun yanı sıra aynı anda yapılabilen bağlantı sayısı, erişim istenen sunucuların gereksinimlerine göre istediği kaynak miktarına bağlı olarak değişiklik göstermiştir. Çalışma kapsamında sistem alt yapısı için dinamik olarak ölçeklenebilir bir mimariye ihtiyaç duyulmuştur. Bu amaçla sistem kaynaklarını ve istek gereksinimlerini yönetebilen açık kaynak kodlu, çalışma başlatmak, çalışma yürütmek gibi işlevleri olan ve bekleyen işlerin sırasını yönetebilen kaynak yönetim yazılımı kubernetes vdi kullanılmıştır.

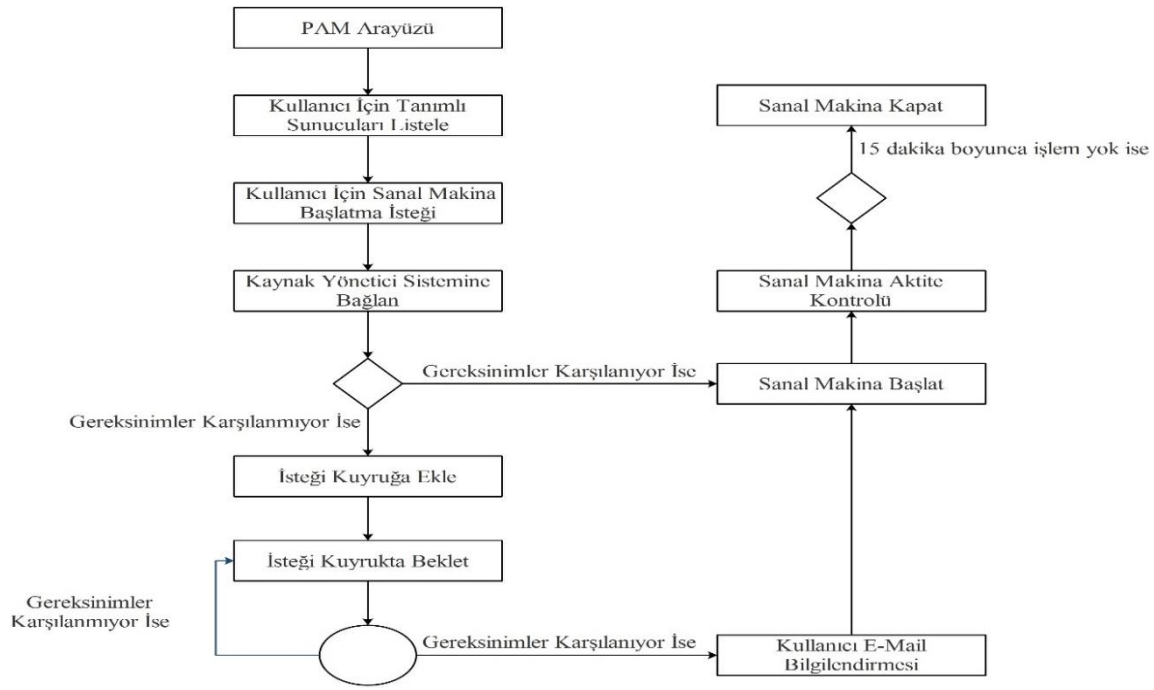
Sistemin güçlü bir kayıt defteri sisteminin olması ve ihlal durumlarının tespit edilebilmesi için Güvenlik Bilgileri ve Olay Yönetimi (Security Information and Event Management - SIEM) teknolojisinden faydalanılmıştır.

Tasarlanan sistemde kısa ve uzun vadeli olmak üzere kayıt işlemlerinin iki farklı şekilde tutulması planlanmıştır. Kısa vadeli kayıt işlemleri son birkaç günün aksiyonlarının tutulduğu sistemi temsil etmektedir. Bu kayıtlarda arama ve görüntüleme işlemlerinin kolay yapılabilmesi için açık kaynak kodlu tam metin indeksleme aracı olan ElasticSearch teknolojisinden faydalanılacaktır. Uzun vadeli kayıt işlemleri ise, aksiyonların daha uzun süreli zaman dilimlerinde tutulduğu sistemi temsil etmektedir. Elasticsearch gibi tam metin indeksleme araçlarının fazla kaynak tüketiminden ötürü, uzun süreli zaman diliminde tutulan aksiyonlar için dokuman tabanlı veri tabanı olan açık kaynak kodlu MongoDB teknolojisinden faydalanılacaktır.

Bu çalışmada olay takip edilebilme kabiliyetini artırmak için, kayıt defterinin yanı sıra ekran videoları da alınmaktadır. Bu kapsamda Java tabanlı "Robot" kütüphanesinden faydalanılmıştır. Bu kütüphanelerden erişimin ve kullanımlarının kolay olması ve video kayıt için isteklerimizi karşılaması nedeniyle yararlanılmıştır. Oluşturulacak video kaydının optimizasyonu için mpeg, h264 vb. sıkıştırma teknolojilerinden faydalanılmıştır.

### 3.3. Önerilen sistem üzerinden oturum başlatma süreci

Oturum başlatma süreci kullanıcının PAM ara yüzüne giriş yapmasıyla başlar. İlk olarak sistem tarafından kullanıcı için tanımlı sunucular listelenir ve sanal makine başlatma isteğinde bulunulur. Sonrasında otomatik olarak kaynak yönetim sistemine bağlanılır ve sanal makine başlatılması için gereksinimlerin karşılanıp karşılanmadığı kontrol edilir. Gereksinimler karşılanıyor ise sanal makine başlatılır. Aksi durumda sanal makine başlatma isteği kuyruğa alınır ve gereksinimler karşılanana kadar kuyrukta bekletilir. Gereksinimler karşılandığında ise kullanıcıya e-mail yoluyla bilgilendirme yapılarak sanal makine başlatılır. Devam eden süreçte sanal makine aktivite kontrolü yapılarak oturum başlatılır. Oturumun başlatılmasından itibaren kullanıcının on beş dakika herhangi bir işlem yapmaması durumunda sistem tarafından sanal makine kapatılır. Önerilen sistemde kullanıcı oturum başlatma süreci şekil 4 de detaylı olarak gösterilmiştir. Sanal makineler kullanıcı spesifik olarak özelleştirildiğinden IaC alt yapısından faydalanılmıştır. Kullanıcıya özel sanal makineler sunmak için ise terraform konteynır şablonundan faydalanılmıştır.




**Şekil 4.** Önerilen sistem üzerinden oturum başlatma akış diyagramı

## 4. SONUÇLAR

Bu çalışmada, yenilikçi yaklaşımlar kullanılarak bir PAM sistemi önerilmiştir. Önerilen bu sistemde platform bağımsız çalışma için konteynır teknolojisinden faydalanılmıştır. Yatay olarak büyümeye olanak sağlamak ve düğümler arası yük dengesi sağlaması amacıyla konteynır orkestrasyon araçları kullanılmıştır. Sistem kullanıcılarının ihtiyaç duyduğu araç setlerinin otomatik olarak sağlanması amacıyla kod olarak alt yapı mimarisi ile geliştirilmiştir. Bu sistemi kullanan kullanıcıların kısa süreli aksiyon kaydı verilerine hızlı ulaşabilmek için tam metin indeksleme aracı, uzun süreli aksiyon ve video kayıtlarının saklanması için doküman tabanlı veri tabanı kullanılmıştır. Sistem aksiyon kayıtlarının raporlanması ve analizi için Güvenlik Bilgileri ve Olay Yönetim sistemi kullanılmıştır. Bu sisteme güvenli giriş yapılabilmesi amacıyla çok faktörlü giriş yönetim sistemi tasarlanarak sisteme entegre edilmiştir. Tüm bu teknolojilerden faydalanılarak uzak sunucu bağlantısı yapacak kullanıcıların, erişim ayarlarının be bağlantı süreçlerinin yönetilmesi için ayrıcalıklı erişim yönetim sistemi geliştirilmiştir.

Tasarlanan sistem, üçüncü parti sistemlerle entegre çalışabilen bir giriş sistemine sahip olması, uzun ve kısa vadeli kayıt sistemleri sayesinde güçlü bir aksiyon analizine olanak tanıması, sanal masaüstü alt yapısından faydalanarak her erişimde izole bağlantı açabilme kapasitesi, anlık ihlal tespitlerine uyumlu olması, erişim süreci boyunca ekran kaydı alabilmesi, sunucu erişim ayarlarının otomatik kurulu olduğu sanal masaüstüler sayesinde kullanım kolaylığı sağlaması ile literatürde tasarlanmış ayrıcalıklı erişim yönetim sistemlerine yeni bir bakış açışı kazandırmaktadır. Tüm bunların tanı sıra konteynır ve kod olarak altyapı teknolojileri sayesinde uzak sunucuya erişimde kullanılabilecek sistemlerin yönetici tarafından oluşturulabilmesi sağlanacak ve oluşturulan bu sistemleri kimlerin kullanabileceği belirlenecektir. Yönetici tarafından oluşturulan bu sistemler kullanılarak, ilgili sunucuya bağlanmak ve o sunucuda işlem yapmak için gerekli olan tüm kurulumlar yönetici tarafından yapılacak, ilgili sunucuya bağlantı için kullanılacak şifreler ise sadece yönetici tarafından bilinecek ve erişimi sağlayacak kişi tarafından bilinmeyecektir. Çok faktörlü doğrulama gerekmesi durumunda ise bu doğrulama önerilen sistem tarafından otomatik olarak yapılacaktır. Örneğin, bir kullanıcının SAP Logon kullanarak bir müşterinin sistemine bağlanması gerektiğini ve bu bağlantı için ise çok faktörlüğü doğrulama barındıran proxy kullanılacağını varsayalım. Önermiş olduğumuz PAM uygulamasında sistem yöneticisi, içerisinde SAP Logon ve ilgili müşterinin giriş bilgilerini barındıran bir sanal makina konfigürasyonu gerçekleştirecektir. Uzak bağlantı yapmak isteyen çalışan, SAP Logon ve proxy kurulumu gibi hiçbir süreçle uğraşmadan sistemi kullanarak bağlantı yapabilecektir. Birçok çalışanın aynı firmaya destek vereceği düşünüldüğünde bu kurulumların normal koşullarda tüm çalışanlar tarafından yapılması gerekmektedir. Bir çalışanın ise farklı firmalara destek verdiği durumlarda, destek verilen firmaların gereksinimlerine bağlı olarak farklı kurulumlar yapması gerekmektedir. Önerilen sistem kullanılarak tüm bu durumlar sistem yöneticisi tarafından tek seferde yapılacaktır. Bu sayede yazılım danışmanlığı yapan firmaların aynı anda birçok kurumun farklı sistemlerine uzaktan destek verme sürecindeki uzak sistemlere bağlanma, bağlantı süreçlerini yönetme, şifre güvenliği ve erişim düzeylerinin belirlenmesi işlemlerinin en az efor ile yapılabilmesini sağlamıştır.

Bu çalışma sonucunda kuyrukta bekletilen kullanıcıların gereksinimleri karşılandığında hangi öncelik sırasına göre iş kuyruğuna ekleneceği noktasında yapay zekâ destekli dinamik bir ölçekleme sistemi ihtiyacı doğmuştur. Bir sonraki çalışmamızda, tasarlanmış olan sistem tarafından toplanan veriler analiz edilecek ve yapay zekâ destekli bir ölçekleme sistemi geliştirilecektir.

## BİLGİLENDİRME/TEŞEKKÜR

Bu çalışma, Detay Teknoloji Yazılım Danışmanlık Bilgisayar Hizmetleri Tic. San. A.S Ar-Ge Merkezi bünyesinde yürütülen çalışmaların sonucudur. Desteklerinden dolayı Merkeze teşekkür ederiz.

## KAYNAKÇA

Alruwies, M., Mishra, S., Abdul, M., & Alshehri, R. (2021). Identity Governance Framework for Privileged Users. Computer Systems Science and Engineering, 40. https://doi.org/10.32604/csse.2022.019355

Anton, P., & Soetomo, M. (2018). Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control. 5, 65-76. Annual Conference on Management and Information Technology.

Docker Documentation. (200M.S., 42:25 + +0200). Geliş tarihi 02 Ekim 2023, gönderen Docker Documentation website: https://docs.docker.com/

D'Silva, D., & Ambawade, D. D. (2021). Building A Zero Trust Architecture Using Kubernetes. 2021 6th International Conference for Convergence in Technology (I2CT), 1-8. https://doi.org/10.1109/I2CT51068.2021.9418203

Elasticsearch: The Official Distributed Search & Analytics Engine. (t.y.). Geliş tarihi 02 Ekim 2023, gönderen Elastic website: https://www.elastic.co/elasticsearch

Elasticsearch vs MongoDB - A detailed comparison of Document-Oriented Databases | SigNoz.

(2023, Ocak 20). Geliş tarihi 08 Ekim 2023, gönderen https://signoz.io/blog/elasticsearch-vs-mongodb/

Garbis, J., & Chapman, J. W. (2021). Privileged Access Management. Içinde J. Garbis & J. W. Chapman (Ed.), Zero Trust Security: An Enterprise Guide (ss. 155-161). Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-6702-8_12

Getting to Know Kubevirt. (2018, Mayıs 22). Geliş tarihi 02 Ekim 2023, gönderen Kubernetes website: https://kubernetes.io/blog/2018/05/22/getting-to-know-kubevirt/

Infrastructure as code. (2023). Içinde Wikipedia. Geliş tarihi gönderen https://en.wikipedia.org/w/index.php?title=Infrastructure_as_code&oldid=1176394945

Ionita, V. (2023). Privileged access management for databases. Geliş tarihi gönderen https://aaltodoc.aalto.fi:443/handle/123456789/122872

Kubernetes Documentation. (t.y.). Geliş tarihi 02 Ekim 2023, gönderen Kubernetes website: https://kubernetes.io/docs/home/

Lang, D., Jiang, H., Ding, W., & Bai, Y. (2019). Research on Docker Role Access Control Mechanism Based on DRBAC. Journal of Physics: Conference Series, 1168(3), 032127. https://doi.org/10.1088/1742-6596/1168/3/032127

Preuveneers, D., & Joosen, W. (t.y.). Federated Privileged Identity Management for Break-the-Glass: A Case Study with OpenAM.

Sindiren, E., & Ciylan, B. (2018). Privileged Account Management Approach for Preventing Insider Attacks.

Sindiren, E., & Ciylan, B. (2019). Application model for privileged account access control system in enterprise networks. Computers & Security, 83, 52-67. https://doi.org/10.1016/j.cose.2019.01.008

Steinhoff, M. (2020). Using Software Containers for Privileged Access Management in Cloud Environments: A Novel Approach to Handle Access Management for Cloud-based Networks. Nordic and Baltic Journal of Information & Communications Technologies, 297-310. https://doi.org/10.13052/nbjict1902-097X.2020.013

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. The Journal of Supercomputing, 76(12), 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management. 2015 IEEE Trustcom/BigDataSE/ISPA, 1, 1073-1080. https://doi.org/10.1109/Trustcom.2015.485

Tran, L. (2020). Privileged Access Management for System to System communications. Geliş tarihi gönderen https://aaltodoc.aalto.fi:443/handle/123456789/46232

What Is NoSQL? NoSQL Databases Explained. (t.y.). Geliş tarihi 02 Ekim 2023, gönderen MongoDB website: https://www.mongodb.com/nosql-explained

Ylonen, T., Turner, P., Scarfone, K., & Souppaya, M. (2015). Security of Interactive and Automated Access Management Using Secure Shell (SSH) (Sy NIST IR 7966; s. NIST IR 7966). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7966