ESTUDAM Bilişim Dergisi
Cilt 3, Sayı 1, 11-17, 2022

Journal of ESTUDAM Information
Volume 3, Issue 1, 11-17, 2022

DOI: 10.53608/estudambilisim.1013695

(Geliş Tarihi / Received Date: 23.11.2021, Kabul Tarihi/ Accepted Date: 10.01.2022)

Kurumsal Haberleşme Sistemi

Tolgahan ÇOBANOĞLU*[1], Muammer AKÇAY[2]

[1] Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 43030, Kütahya, ORCID No: https://orcid.org/0000-0001-7939-3801

[2] Kütahya Dumlupınar Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 43030, Kütahya, ORCID No: https://orcid.org/0000-0003-0244-1275

Anahtar Kelimeler:
güvenlik, bilgi,
haberleşme, dağıtık sistemler,
bilgi teknolojileri

Özet: Günümüzde birçok işletme kendi kurumsal ağını oluşturarak bu ağ üzerinden haberleşme sistemlerini kurmakta ve çalışanları ile bu sistemler üzerinden haberleşmektedir. Bilgi güvenliğinin son derece önem kazandığı günümüz çağında işletmeler çalışanları ile iletişimlerini kendi yönetimi ve denetiminde olan platformlar üzerinden gerçekleştirme ihtiyacı duymaktadır. Bu alanda işletmelere sunulan üçüncü parti yazılımlar, kurumsal nitelikte olmaktan ziyade kurumlar için yönetim ve denetimin yapılamayacağı bir paket halinde sunulmaktadır. Bu durum da işletmeye ait bilgi ve belgelerin üçüncü kişilerin eline geçebilme ihtimali oluşmaktadır. Bu çalışma, aynı işletmede çalışanların kendi aralarında güvenli bir şekilde bilgi ve belge paylaşımı yapabilmelerini sağlamakta, yönetim ve denetiminin tamamen işletme tarafından yapılabilme imkânı sunmaktadır. Çalışmanın cep telefonları ve kişisel bilgisayarlar üzerinde çalışabilecek şekilde tasarlanması da ayrıca kullanıcılara platformdan bağımsız kullanabilmeleri sağlanmıştır.

Corporate Communication System

Keywords:
security,
information, communication,
distributed systems,
information technologies

Abstract: Today, many businesses create their own corporate network and establish communication systems over this network and communicate with employees through these systems. In today's era, where information security is of utmost importance, businesses need to communicate with their employees through platforms under their own management and control. Third-party software offered to businesses in this area is presented as a package in which management and auditing cannot be performed for institutions rather than being institutional. This leads to the possibility that the information and documents of the enterprise may be received by third parties. This study ensures that the employees in the same company can share information and documents securely among themselves, and that the management and supervision can be carried out entirely by the enterprise. The study is designed to work on mobile phones and personal computers also gives users independence from the platform

1. GİRİŞ

Toplumsal hayatın sürdürülebilmesi açısından kritik öneme sahip olan iletişim, insanların birlikte yaşayabilmeleri için en temel ihtiyaçlardan biridir. Bu nedenle iletişim, insan ırkının var oluşundan yok oluşuna kadar toplumsal yaşamın bir gereğidir. İnsanlar gibi kurumsal yapıların da varlığının temelini iletişim oluşturmaktadır. Bu nedenle kurumlar, amaç ve hedefleri doğrultusunda yürüttükleri faaliyetler için çeşitli iletişim yöntemleri ve süreçleri geliştirmektedirler.

Kurumsal iletişim, bir kurumun misyon ve vizyonu temelinde, amaç ve hedefleri doğrultusunda iç ve dış tüm iletişim çalışmalarının yönetilmesi sürecidir. İç iletişim sistemi, hedeflere ulaşmak için verilerin toplanması ve yorumlanması hakkında beklentiler ve tutumlar ve koşulları ifade eden kurumsal ortamları, dış iletişim sistemi, dış iletişim kanalları aracılığı ile kurum ile ilgili bilgileri sunmak içim kullanılır [1]. Kurumsal iletişim, kurumu oluşturan tüm bileşenlerin birbirleri ile iletişim kurduğu iletişim sürecidir [2]. Bu yönüyle kurumsal iletişim kurumların kendi vizyon ve misyonlarını gerçekleştirebilmesini sağlayan iletişim organizasyonlarının bütünüdür [3].

*İlgili yazar/Corresponding Author: tolgahancobanoglu@gmail.com

Özellikle Endüstri 4.0 ile birlikte birçok alanda ortaya çıkan yeni rekabet süreçleri kurumların iletişim alanında yeni ihtiyaçları da beraberinde getirmektedir. Bu ihtiyaçları gerçekleştirebilmek maksadıyla doğru ve güvenilir iletişim kanalları kurabilen kurumlar markalaşma yönünde adımlar atmaktadır [3]. Markalaşma sayesinde ise kurumlar ile hedef kitle arasında iletişim sağlanmaktadır [4]. Kurumların hedef kitlelerine yönelik ihtiyaç duydukları ve geliştirdikleri tüm iletişim süreçlerinin temelinde ise çalışanlar arası iletişim faktörü bulunmaktadır. Çalışanları arasında hızlı ve güvenli iletişim kurabilen kurumlar ise, hedef kitleye çok daha kolay ulaşarak, hedef kitlenin beklenti ve ihtiyaçlarına daha kısa sürede cevap verebilmektedir. Rekabette çok daha ileri noktalara ulaşabilmektedir.

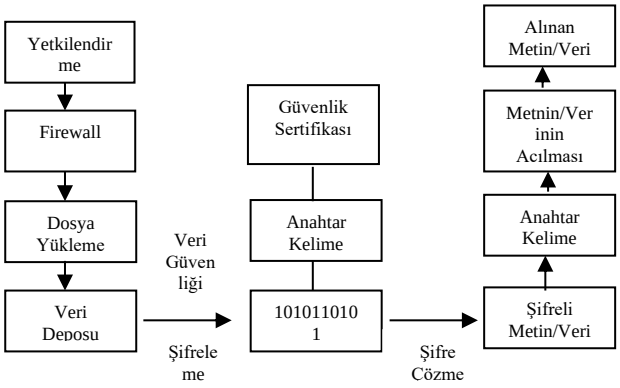
Sağlıklı ve verimli bir kurumsal iletişimin sağlanabilmesi için de ilk olarak sağlanması gereken bilgi güvenliğidir. Rekabet ortamlarının oldukça güçlü olduğu sistemlerde, kurumların iletişim süreçlerine bilgi güvenliği yaklaşımlarını ve standartlarını uygulamaları elzem hale gelmiştir. Bu nedenle bilginin üretimden, saklanmasına ve işlenmesine kadar her ortamda kurumsal bilgi güvenliğinin sağlanması gerekmektedir. Bilgi teknolojililerinin sürekli gelişen ve değişen yapısı nedeniyle de bilgi güvenliğini sağlayan organizasyon ve platformlar sürekli güncellenmeli, ihtiyaçları karşılayabilir durumda olmalıdır [5]. Bunun için kurumun sahip olduğu yazılım, donanım ve insan kaynaklarını oluştururken kurum kaynaklarının bu durumlar göz önünde bulundurularak kullanılması gerekir [6]. IDC gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde çoğu kurum ve kuruluşun 2019 yılında rekor seviyede güvenlik harcaması yaptığı ve IDC firmasının son raporuna göre; 2019 yılında güvenlik harcamaları 106,6 milyar dolar seviyelerine yükselmiştir [7].

Bu çalışmanın amacı; kurumların kendi çalışanları ile dinamik bir şekilde bir web platformu üzerinden iletişim kurmalarını sağlayarak, iletişimlerini güvenli hale getirebilmek ve büyük maliyetlerle satın alınabilecek teknolojilerin asgari düzeyde yapılacak harcamalar ile kurumlara kazandırılmasını sağlamaktır.

Bu amaçla Bölüm 2'de kurumsal iletişimde bilgi güvenliğinin kapsamı verilmiş, Bölüm 3' de ise güvenlikli bir kurumsal iletişim platformunun oluşturulmasına dair geliştirilen uygulama ifade edilmiştir.

2. KURUMSAL İLETİŞİMDE BİLGİ GÜVENLİĞİNİN ÖNEMİ

Ağ üzerindeki verilere erişim ya da işleme esnasında, verilerin bütünlüğünün bozulmadan, üçüncü taraf kullanıcılar tarafından erişilmesini engelleyen yapı bilgi güvenliği olarak adlandırılır [8]. Bilgi güvenliğinin temelini "gizlilik", "bütünlük" ve "erişilebilirlik" olarak tanımlanan unsurlar oluşturmaktadır. Bilgi güvenliğinin sağlanabilmesi için bu üç temel unsurun gereği olarak, bilgide izinsiz erişim ve değişimlerin engellenmesi gerekmektedir. Teknoloji, insan, bilgi, sistem ve yöntem faktörleri ise doğrudan bu üç temel unsura etki ederek güvenliğin sağlanmasında etkendir. Bu faktörler arasında ise insan faktörü bilgi güvenliği sistemini kuran temel ve olmazsa olmaz bileşendir [9]. Bu çalışmanın da konusunu oluşturan bilgi güvenliği Şekil 1'deki akış diyagramı ile sağlanmakta olup, çalışma bu diyagram mantığı ile şekillendirilmiştir [10].

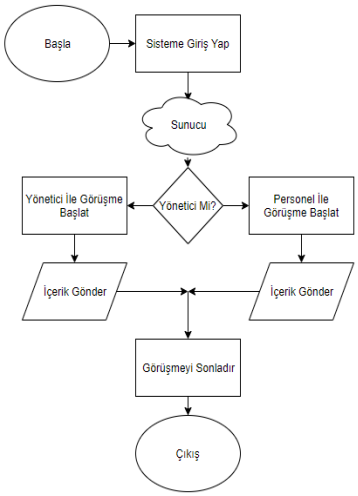


Şekil 1. Bilgi Güvenliği Akış Diyagramı

Kurumsal bilgi güvenliği ise, kurumların kendi ekosistemi içerisinde sahip olduğu bilgiyi korumak amacıyla oluşturdukları mekanizmaları içeren sistemler olarak değerlendirilebilir. Kurumsal bilgi güvenliğinin sağlanması açısından kurumsal iletişim bu ekosistemin en önemli bileşenidir. Kurumsal iletişim, bir kurumun hedef kitlelerine yönelik tüm iletişim çalışmalarıdır [6]. Çalışanlar arasında bilgi ve belge paylaşımı hedef kitleye yönelik iletişim çalışmalarının bir bölümünü oluşturmaktadır. Bu bilgi ve belge paylaşımının güvenli platformlarda yapılması da kurumsal bilgi güvenliğinin oluşturulmasını sağlayacaktır. Bu amaçla geliştirilen çalışmada çalışanların çalışanlar birbirleri ile gerek mobil gerekse de masaüstü ortamlarda bilgi ve belge paylaşımı yapabilecektir.

3. KURUMSAL HABERLEŞME SİSTEMİ

Sistem, temelde istemci-sunucu mimarisi üzerinde PHP - MVC yapısı kullanılarak geliştirilmiştir. Bu bölümde istemci-sunucu mimarisi, PHP - MVC yapısı ve sitemin çalışması açıklanacaktır.

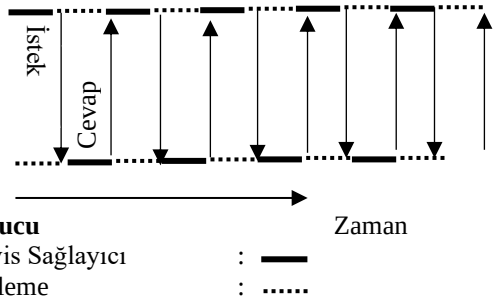


Şekil 2. Uygulama Akış Diyagramı

Kurumsal haberleşme sisteminin çalışma prensibi Şekil 2'de gösterilmiştir. Buna göre sisteme giriş yapılabilmesi için kullanıcı bilgisi sunucuya gönderilmekte, sunucuda bulunan veri tabanındaki bilgiler ile giriş yapılan bilgilerin eşleşmesi durumda kullanıcı sisteme yönetici ya da personel olarak giriş yapabilmektedir. Sisteme giriş yapan kullanıcı, diğer kullanıcıların çevrimiçi ya da çevrimdışı olmasına bakılmaksızın içerik gönderebilmektedir. İçerik gönderimini tamamlayan kullanıcı sistemden çıkış yaparak görüşmeyi sonlandırmaktadır.

3.1. İstemci – Sunucu Mimarisi

Temel istemci-sunucu modelinde, dağıtılmış bir sistemdeki işlemler iki (muhtemelen örtüşen) gruba ayrılır. Bir sunucu, örneğin bir dosya sistemi servisi veya bir veri tabanı servisi gibi belirli bir servisi uygulayan bir işlemdir. İstemci, bir sunucudan hizmet talep eden ve ardından sunucunun cevabını bekleyen bir işlemdir. İstemci ve sunucu arasındaki bu talep – cevap ilişkisi Şekil 2'de gösterilmiştir [11].



İstemci sunucu sistemlerinde istemci, işlemin başlatılmasından sonlandırılmasına kadar sunucuya bir dizi görev bildirir. Sunucu bu görevleri tamamlayarak istemciye haber verir. Bu nedenle işlemin istemci ve sunucu arasında nasıl paylaşılacağı önemlidir. İşlemin istemci ve sunucu arasında nasıl paylaştırılacağına dair beş model mevcuttur:

- Dağıtık kullanıcı arabirimi: Bu modelde sisteme bir kullanıcı arabirimi eklenerek istemcinin kapasitesinin artırılması amaçlanmıştır. İletişim programları aracılığı ile tüm iş istasyonlarının veri tabanına erişimde bulunması sağlanır.

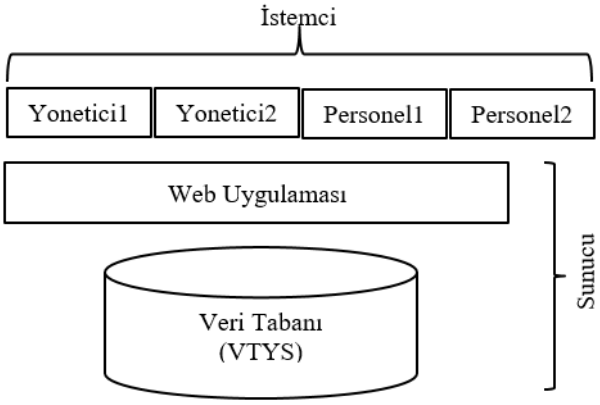
- Son kullanıcı arabirimi: Aynı sunucuya yeni kullanıcı arabirimleri bağlanarak, yönetim ve veri kaynağı istemci tarafından sağlanır.

- Dağıtık işlem modeli: Bu modelde, istemci pek çok işlevi sunucudan bağımsız olarak uygulamaların görevleri istemci/sunucu arasında paylaştırılmıştır. Veri kaynağı sunucu tarafından sağlanır.

- Uç veri tabanı: Bu modelde, kullanıcı arabirimi ve görevler, sunucu üzerinde kalan veri katmanından ayrılır. Bir veri tabanı yönetim sistemi (VTYS) kullanılarak sunucudaki veri katmanından ayrılır. İstemci, sunucuya sorgulama dili komutları göndererek veri talep eder ve sunucu da bu sorgulama sonucundaki veriyi istemciye gönderir.

- Dağıtık veri tabanı: Bu modelde, veri katmanı istemci ve sunucu arasında paylaşılmış olduğundan verinin nerede bulunduğu konusunda uygulamalar bilgi sahibi değildir [12].

Yapılan çalışma ise ilk olarak son kullanıcı arabirimi modeli ile pyhton programlama dili ile benzetim gerçekleştirilmiş ve daha sonra dördüncü model ile PHP-MVC mimarisi kullanılarak geliştirilen yazılım son halini almıştır. Şekil 4'de çalışmanın sistem yapısı gösterilmiştir.



Şekil 4. Sistem Yapısı

Çalışmanın benzetim (simülasyonu) ile ilgili olarak, phyton programlama dili ile geliştirilen uygulamanın sözde kodu ile istemci ve sunucu arasındaki iletişim görülmektedir:

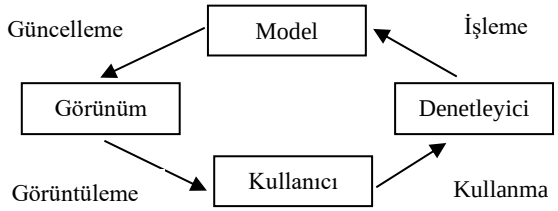
```
istemci.phy:
Sunu ile bağlantıyı kur
Mesaj var ise
Mesajı al
Bağlantıyı kapat

sunucu.phy:
Mesajı gönder
Bağlantıyı kapat
```

Çalışmanın son hali ise dördüncü model ile ifade edilen asıl uygulamanın geliştirildiği kısımdır. Sonraki başlıkta bu konuya değinilecektir.

3.2. Mvc (Model-View-Controller) Yapısı

Çalışma kurum çalışanlarının internete bağlı olduğu sürece sistemi cep telefonu, tablet, pc gibi ortamlardan kullanabilmelerini sağlamak amacıyla duyarlı (responsive) tasarlanmış, test edilebilir ve tekrar kullanılabilir parçalara sahip bir uygulama geliştirmek maksadıyla da çalışma MVC mimarisi kullanılarak geliştirilmiştir. Bu sayede birbirinden ayrı katmanlardan oluşan çalışma programcı tarafından kolay okunabilir ve kontrol edilebilir bir hal almıştır.

MVC (Model-görünüm-denetleyici) yöntemi ilk olarak 1970'lerde Trygve Reenskaug tarafından tanıtılmıştır. Bu yöntem Şekil 5'te görüldüğü üzere birbiriyle bağlantılı, model, görünüm ve denetleyici olmak üzere üç kısma ayrılmıştır [13].



Şekil 5. MVC Yapısı [13]

- Model: Veri tabanı üzerinde ekle, sil, güncelle, ara gibi sorgulama işlemlerinin yapıldığı, sayfa görünümüne dair öğelerin bulunmadığı bölümdür. Bir uygulamanın tüm iş mantığının tutulduğu yerdir. İş mantığı, bir uygulamanın iş gereksinimlerini karşılamak için verileri nasıl sakladığı veya üçüncü taraf hizmetleri nasıl kullandığı belirli bir şey olabilir. Eğer uygulamanın bir veri tabanındaki bilgilere erişmesi gerekirse, bunun için kod modelde tutulur.

- Görünüm: Uygulamanın tüm kullanıcı arabirimi öğelerinin tutulduğu yerdir. Bu, HTML, biçimlendirme, CSS stil sayfaları ve JavaScript dosyaları kodlarını içerebilir. Bir kullanıcının gördüğü veya etkileşimde bulunduğu her şey görünümde tutulabilir ve bazen kullanıcının gördüğü şey aslında aynı istekte birçok farklı görünümün birleşimidir. Bu bölümden model bölümüne doğrundan erişim bulunmamaktadır. Öyle ki bu bölümde genelde HTML kodlama yapısı kullanılarak web sayfasının şablonu oluşturulmaktadır.

- Denetleyici: Modelleri ve görünümleri birbirine bağlayan bileşendir. Görünüm bölümündeki sayfalar ile model arasında bir köprü işlevi gören öğelerin bulunduğu bölüm olup, denetleyici metotlar ile kullanıcıdan istek ve verileri alarak uygulamanın ne işleyeceğini belirler [14].

MVC kullanımı tasarım desen geliştirmeyi ve korumayı daha kolay hale getirir. Bu sayede uygulamanın görünümü veri yapılarını ve iş mantığını değiştirmeden büyük ölçüde değiştirilebilir ve uygulama, birden fazla dil veya farklı kullanıcı setleri gibi farklı ara yüzleri kolayca koruyabilir [2].

3.3. Sistem Tasarım ve Yapısı

Kurumsal haberleşme sistemi PHP kodlama dili kullanılarak MVC mimari ile geliştirilmiştir. Bu mimari ile ilgili olarak ilk bahsedilecek bileşen, görünümdür. Çünkü bu bileşen kullanıcıya hitap eden ara yüzdür. Sistem kullanıcıları bu ara yüzü kullanarak birbirleri ile etkileşime geçerler. Burada kullanıcılara mesaj oluşturabilecekleri ve dosya paylaşımı yapabilecekleri bir ekran gösterilmektedir.

İlk olarak sistem kullanıcı bilgilerinin veri tabanından çekilerek görünüm sayfasında bu bilgilerin görüntülenmesini sağlayan tanımlar `UserModel.php` sayfası içerisinde aşağıdaki gibi tanımlanmıştır:

```
<?php
      $obj->load->model('UserModel');
      $user=$obj->UserModel-
>GetUserData();
 ?>
```

Sayfada yer alan metin girişi alanına metin ya da dosya ekleyen kullanıcı karşı tarafa bu bilgi ve belgeleri aşağıdaki denetleyici sayfasında yer alan kodlar vasıtasıyla gönderebilmektedir. Bu aşamada metin gönderimi için aşağıdaki metot denetleyici sayfasında tanımlanmıştır.

```
public function send_text_message(){
$messageTxt=
reduce_multiples($post['messageTxt'],'
');
}
```

Karşı tarafa dosya gönderimi için ise aşağıda görüldüğü gibi `ChatAttachmentUpload()` fonksiyonu kullanılmıştır. Bu fonksiyon içerisinde kullanılan `$config` değişkenine gönderilen dosyanın sahip olduğu parametreler (dosya konumu, dosya türü gibi) atanmıştır. `$config` değişkeninin tuttuğu değerler CodeIgniter'ın upload kütüphanesi aracılığı ile dosyanın sunucu ya da istemci bilgisayara gönderilmesini sağlamıştır.

```
public                          function
ChatAttachmentUpload(){
$config['upload_path']=
./uploads/attachment';
$config['allowed_types']='jpeg|jpg|png
|txt|pdf|docx|xlsx|pptx|rtf';
$this->load->library('upload',
$config);
}
```

Kullanıcıların sohbet geçmişlerini içeren bilgiler ise; `public function get_chat_history_by_personel()` metodu ile sunucudan alınmaktadır.

Tüm bu yukarıdaki işlemler `ChatController.php` sayfası içerisinde tanımlanmıştır.

Kullanıclar arasındaki tüm bu yazışmalar, bilgi ve belge gönderimleri;

```
$this->OuthModel-
>Encryptor('encrypt',$row->id)
```

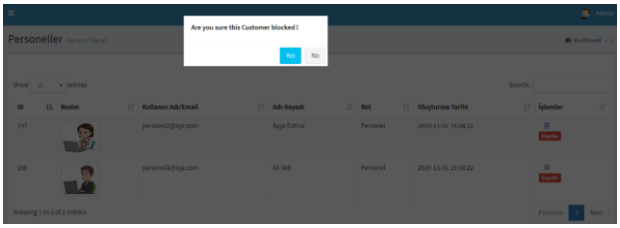
metodu ile veri tabanına şifrelenerek kaydedilmekte ve

```
$this->OuthModel->Encryptor('decrypt',$row->id)
```
metodu ile de veri tabanından alınmaktadır.

Son olarak, oluşturulan bu sayfalar ve veri tabanı kiralanan bir sunucuya yüklenerek çalışma yayınlamıştır. Sistem kullanıcıları yönetici ve personel olarak belirlenmiştir. Yöneticiler personeli aktif ya da pasif yapabilme yetkisine sahiptir. Bu yetki ile engellenen personel sitemde pasif duruma geçecek ve kendisi ile herhangi bir yazışma yapılamayacaktır. Bunun için jQuery kodlarından faydalanmış olup, `yönetici_lisy_template.php` görünüm sayfasında kullanılan bu yapı aşağıdaki gibidir:

```
<script>
      function block(id,durum){
      if(durum == 2){
      Kullanıcıyı engelle
      }if(durum == 1){
      Kullanıcı engelini kaldır
      $('#durumDegiskeni').val(durum);
      $('#durumNo').val(id);
      }
      }
</script>
```

Yukarıdaki işlem ile Şekil 6'da görüldüğü gibi ekrana kullanıcının engellenip engellenmeyeceğine dair uyarı mesajı görüntülenmektedir. Bu mesaja verilen cevap durum değişkeninde saklanarak veri tabanına bu değişkendeki değer gönderilmektedir.



Şekil 6. Kullanıcı Engelleme İşlemi

Çalışmanın bir diğer önem arz eden kısmı ise sistem kullanıcılarının yetkilendirilmesini sağlayan bölümüdür. Bu bölümde, hangi sistem kullanıcısı sistemi hangi yetki ile kullanacak bunu sağlayan yapıların oluşturulması sağlanacaktır. Bu sayede kullanıcılar arasında bir hiyerarşi gerçekleşecek, sistem kullanıcılarının yetkisiz işlemler yapmalarının önüne geçilebilecektir. Örneğin, yönetici kullanıcısı çalışanlar arasındaki konuşmaları izleyebilecek ve sisteme çalışan ekleme yetilerine sahip olacaktır. Personel kullanıcıları ise yalnızca sistemi mesajlaşma için kullanabilecektir. Bunun için Log kaydı tutma ve yetkilendirme konularına değinilecektir.

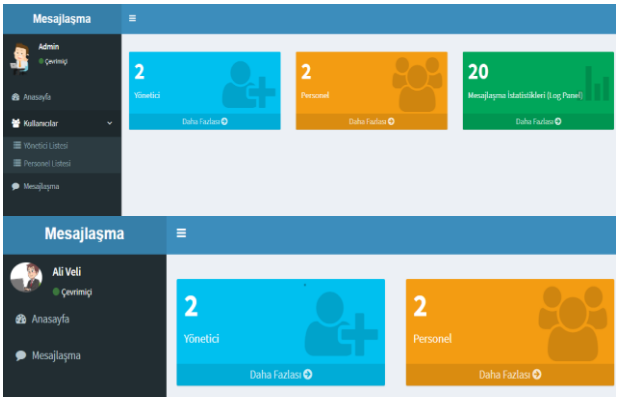
3.4. Log Analizi ve Yetkilendirme

Kurumsal bilgi güvenliğini sağlayarak çalışanlar arasında mesajlaşma sistemi kurmayı amaçlayan bu çalışmada, kurumsal bilgi güvenliğini sağlamak maksadıyla geliştirilen iki bölüm daha mevcuttur. Bunlardan birincisi Log analizinin yapıldığı, Log Panel ve kullanıcı yetkilendirme işlevinin gerçekleştirildiği, Yetkilendirme sayfalarıdır. Bu sayfalar sadece yönetici panelinde mevcuttur. Dolayısı ile yetkisiz erişimlere kapalı olacak ve yalnızca sistem yöneticisi tarafından kullanılacaktır.

Log, bir kuruluşun sistemlerinde ve ağlarında meydana gelen olayların bir kaydıdır. Log kayıtları, log girdilerinden oluşur; her girdi, bir sistem veya ağda meydana gelen belirli bir olayla ilgili bilgiler içerir. Başlangıçta, log kayıtları temel olarak sorun giderme için kullanıldı, ancak artık çoğu kuruluşta sistem ve ağ performansını optimize etme, kullanıcıların eylemlerini kaydetme ve kötü amaçlı etkinlikleri araştırmak için yararlı veriler sağlama gibi birçok işleve hizmet etmektedir [16].

Bu çalışmada yönetici panelinde bulunan Log Panel (Mesajlaşma İstatistikleri) bölümü, kullanıcı eylemlerini yöneticiye sunarak kurumsal bilgi güvenliğine katkı sağlamaktadır. Bu sayede kullanıcılar arasında güvenli ve kontrollü bir veri akışı sağlanmaktadır. Bunun için bir denetleyici sayfası oluşturularak, veri tabanındaki birbiri ile ilişkili tablolar arasında join komutu aracılığı mesaj gönderen ve mesajı alan kişilerin verileri ilgili tablolardan çekilmiştir. Bu veriler bir datatable ile yöneticiye ait görünüm sayfasında ekrana bastırılmıştır. Aşağıda bu işlemin temelini oluşturan denetleyici içerisinde tanımlı fonksiyon gösterilmiştir:

```
public function grid_data()
{
  $query = $this->db->query($sql);
  $queryqResults = $query->result();
  $totalData = $query->num_rows();
  $totalFiltered = $totalData;
  $where = " WHERE u.id = c.sender_id
";
  $sql = "SELECT ".$fields;
  $sql.=" FROM ".$table . $where;
}
```



Şekil 7. Yönetici ve Personel Sayfalarından Görünüm

Çalışmanın süper yönetici sayfasında farklı kullanıcı rolleri için yetkilendirme işlemleri bulunmaktadır. Bu rol tanımları kurum çalışanlarının rolleri göz önünde bulundurularak oluşturulmuştur. Buna göre personel rolüne sahip kullanıcı yalnızca sayfasında diğer kurum çalışanları ile mesajlaşma paneline sahip olacak, yönetici rolüne sahip kullanıcı ise mesajlaşma panelinin yanı sıra

log kayıtlarını görebileceği bir panele sahip olacaktır. Bu rol tanımları Şekil 7'de görülmektedir.

Kullanıcılara rol tanımlaması işlemleri CodeIgniter geliştiricileri tarafından hazırlanan `ion_auth` kütüphanesi aracılığı ile çok kolay ve basit bir biçimde gerçekleştirilmiştir. Öncelikle aşağıda görülen `grupOlustur` metodu ile `ion_auth` kütüphanesinin `create_group` metodu üzerinden kullanıcı rollerinin bulunduğu gruplar tanımlanmıştır. Bu komut satırları süper yönetici sayfasına ait olup yalnızca sistem yöneticilerinin kullandığı sayfa ile ilişkilidir. Oluşturulan gruplara göre grup izinleri kullanıcıların sistem üzerindeki kısıtlarını içermektedir.

```
public function grupOlustur() {
if (grupAdi değeri girildi ise) {
      grup oluştur
if(grup oluşturulamadı ise)
{
   Ekranda hata göster
}
else
{
   Sayfayı yenile
 }
      grup izinlerini ayarla
}}
```

4. TARTIŞMA VE SONUÇ

Çalışma, duyarlı tasarımı ile işletme ya da kurum çalışanları arasında bilgi ve belge paylaşımının platformdan bağımsız ve güvenli bir şekilde yapılabilmesine imkân sağlamaktadır. Bilgi güvenliğinin her geçen gün daha da önem arz ettiği günümüzde kurum ya da işletmelerin çalışanları ile güvenli ortamlarda iletişim kurabilmeleri imkânı doğmaktadır. Postini güvenlik şirketi tarafından yayınlanan rapora göre anlık mesajlaşmayı hedefleyen tehditlerin %90'ının oldukça yıkıcı olduğunu belirtilmiştir [17]. Öte yandan, birçok kamu kurumu ve işletme sunucuları ülke dışındaki yabancı yazılımları kullanarak çalışanları ile iletişim kurmaktadır.

M. Özel [18] 1200 çalışanlı bir Perakende Grubu firması ile yaptığı araştırmada, firma çalışanları arasında iletişim aracı olarak kullanılan Cluster isimli sosyal medya uygulamasının çalışanlar üzerindeki etkilerini incelenmiştir. Çalışanların bilgi ve içerik paylaşımı, yorum tavsiyesi amacıyla kullandıkları uygulamanın güvenlik konusunda kaygılar taşıdığını belirtmiştir.

Tamamen yerli imkanlar ile üretilen bu çalışma ile çalışmayı kullananların tüm verilerinin ülke içerisindeki sunucularda saklanması sağlanacak böylelikle işletme ya da kurumlar için kritik bilgilerin üçüncü tarafların eline geçmesi ve hatta ülke dışına çıkması engellenecektir. Aynı zamanda işletme ya da kurum yöneticileri çalışanları ile uzaktan toplantı ya da görüşme yapabilmeleri sağlanacaktır.

Bu çalışmaya benzer şekilde TÜBİTAK BİLGEM tarafından tamamen milli imkanlar ile geliştirilmiş Güvenli Mesajlaşma Sistemi (GMS), askeri ve kurumsal kullanıma uygun olarak geliştirilmiş güvenilir ve güvenli anlık mesajlaşma sistemidir [18].

Şekil 8'de bazı anlık mesajlaşma sistemleri ile bu çalışmada gerçekleştirilen uygulamalara dair karşılaştırmalara yer verilmiştir.

Platform / Özellik	Bip	WhatsApp	Telegram	Signal	Kurumsal Haberleşme Sistemi
Yazılımı Yapan Ülke	Türkiye	ABD	Rusya	ABD	Türkiye
Verilerin Saklandığı Ülke	Türkiye	ABD	Rusya	ABD	Türkiye
Şifreleme	Var Uçtan uca şifreleme yakında	Var Uçtan uca şifreleme	Var Gizli mesajlar uçtan uca şifreli	Var Uçtan uca şifreleme	Var Uçtan uca şifreleme
Açık Rıza Olmadan Veri Paylaşımı	Yok	Var	Yok	Yok	Yok

Şekil 8. Anlık Mesajlaşma Sistemleri Güvenlik Karşılaştırması [19]

Mevcut durumda yalnızca internet bağlantısı ile çalışabilen bu uygulama, kısmen de olsa internet üzerinden iletişim kurulabilmesi nedeniyle güvenlik zafiyeti taşıdığı söylenebilir. Ancak kurumların kendi iç özel ağlarını (intranet) kurdukları ya da kendilerine ait bir sunucu satın aldıkları takdirde bu sorun da tamamen ortadan kalkacaktır.

Çıkar çatışması

Çalışma ile ilgili olarak, herhangi bir kişi veya kurumla çıkar çatışmasının bulunmadığını Yazarlar olarak onaylıyoruz.

KAYNAKÇA

[1] R. J. Varey ve J. White, The corporate communication system of managing. Corporate Communications: An International Journal, c. 5, s.11, ss. 5–12, 2000.

[2] G. Murat ve B. Öksüz, Çalışanların Kurumsal İtibar Sürecine Katılımlarında İçsel İletişimin Rolü, Jounal Of Yaşar University, c. 4, s. 16, ss. 2637–2660, 2009.

[3] M. Batu ve Ş. Kayacan, Kurumsal İletişim Projelerinin, Kurumların Marka Algısı İle İlişkisi: Belediyelere Yönelik Bir Analiz, Erciyes İletişim Dergisi, c. 5, s. 4, ss. 749–769, 2018.

[4] H. Alan ve O. Yeloğlu, Markalaşma ve Yenilikçilik, İktisadi Yenilik Dergisi, c. 1, s. 1, ss. 13-26, 2013.

[5] Y. Vural ve Ş. Sağıroğlu, Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, c. 26, s. 1, ss. 89-113, 2011.

[6] Y. Vural ve Ş. Sağıroğlu, Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, c. 23, s. 3, ss. 507-522, 2008.

[7] M. Shirer, K. Massey ve J. Goepfert, New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services. https://www.idc.com/getdoc.jsp?containerId=prUS45591619. (Erişim Tarihi: 21.01.2020)

[8] B. N. Akilotu, Z. Kadiroglu, ve A. Sengur, Information Security and Related Machine Learning Applications, 1st International Informatics and Software Engineering Conference, Ankara, Türkiye, Kas. 6-7, 2019.

[9] D. Aksu ve M. A. Aydin, Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms, International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), ss. 77–80, 2019.

[10] Macrovector, Data Security Flowchart. https://www.canstockphoto.com/data-security-flowchart-32723100.html. (Erişim Tarihi: 21.07.2020)

[11] A. S. Tanenbaum ve M. Van Steen, Distributed Systems, CreateSpace Independent Publishing Platform, c. 3, 2017.

[12] C. S. Sütçü, İstemci/Sunucu Bilgisayar Sistemleri, Marmara İletişim Dergisi, c. 10, s. 10, ss. 79–86, 2014.

[13] M. R. Mufid, A. Basofi, M. U. H. Al Rasyid, I. F. Rochimansyah, ve A. Rokhim, Design An MVC Model Using Python For Flask Framework Development, IES 2019 - International Electronics Symposium: The Role of Techno-Intelligence in Creating an Open Energy System Towards Energy Democracy, Surabaya, Indonesia, Indonesia, Eyl. 27-28, 2019, ss. 214–219.

[14] C. Pitt, Pro PHP MVC, Germanuy: Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2012.

[15] A. Leff ve J. T. Rayfield, Web-Application Development Using the Model/View/Controller Design Pattern. http://domino.watson.ibm.com/library/CyberDig.nsf/home (Erişim Tarihi: 02.08.2020)

[16] K. Kent ve M. Souppaya, Guide to Computer Security Log Management, Recommendations of the National Institute of Standards and Technology, 2006.

[17] A. T. Kabakus and R. Kara, “Survey of Instant Messaging Applications Encryption Methods,” Eur. J. Sci. Technol., vol. 2, no. 4, pp. 112–117, 2015

[18] M. Özel, “Kurum İçi Sosyal Medya Uygulamaları ve Çalışan Katılımı İlişkisi Üzerine Bir Araştırma,” Halkla İlişkiler ve Rekl. Çalışmaları E-Dergisi, vol. 1, no. 2, p. 1, 2018.

[19] Türkiye Bilişim Derneği, “Anlık İleti Hizmetleri Değerlendirme,” 2021. https://www.tbd.org.tr/pdf/tbd-anlik-ileti-hizmetleri-degerlendirme-raporu.pdf.