

# Genişleyebilir Finansal Raporlama Dilinde Güvenlik (XARL)

Muhsin Çelik<sup>1</sup>, Umut Uyar<sup>2</sup>

<sup>1</sup> Pamukkale Üniversitesi, İşletme Bölümü, Denizli

<sup>2</sup> Pamukkale Üniversitesi, İşletme Bölümü, Denizli

muhsin celik@pau.edu.tr, uuyar@pau.edu.tr

**Özet:** Genişleyebilir Finansal Raporlama Dili (eXtensible Business Reporting Language - XBRL) finansal bilginin internet ortamında değişiminin daha etkin ve hızlı olarak sağlanması amacıyla geliştirilmiştir. İnternetin yaygınlaşması ile elektronik belgelerin iletilmesinde maliyetler düşürülmüş, böylece bilgi tedarikçilerinin bilgiye ulaşmaları oldukça kolaylaşmıştır. İnternetin doğasındaki güvensizlik nedeniyle, iyi bir güvenlik sistemi olmadan XBRL servislerinin hedeflerine ulaşması oldukça güçleşmektedir. Günümüz güvenlik yaklaşımları, kullanıcının kimliğini tanımlanması, şifre ve veri transferinde çeşitli güvenlik önlemleri önermektedir. Genişleyebilir Güvenli Raporlama Dili ise (eXtensible Assurance Reporting Language – XARL) internet ortamında yayımlanan finansal bilgilerin güvenliği ve doğruluğunu güvence altına almak amacıyla tasarlanmıştır. Uygun bir altyapı ile XARL genişleyebilir finansal raporlama dili belgelerinde finansal bilgilerin hazırlanmasındaki güvenliği sağlayabilmektedir. Bu çalışmanın amacı; internet üzerinden genişleyebilir finansal raporlama dili (XBRL) kullanılarak finansal raporların paydaşlara iletilmesinde güvenlik konusunu tartışmaya açmaktır.

**Anahtar Kelimeler:** XBRL, XARL.

## Extensible Assurance Reporting Language (XARL)

**Abstract:** Nowadays computers and internet systems become not only useful things but also a requirement. Companies can declare their financial documents through the internet. Especially, Extensible Business Reporting Language - XBRL which is developing rapidly in the last decades create a continuous data generating process and a paperless system. But there a problem about declaring the financial documents through the internet. First of all the internet is a public network and it is completely indefensible. It is clearly that this situation is dangerous for companies and XBRL users. The software companies found a way for solve this security problem: Extensible Assurance Reporting Language – XARL. With a suitable base, XARL system can secure all the XBRL documents for any hacker attack and also it can encrypt the documents with a private key for unique user. In this paper, we show that how to XARL systems secure the financial documents and users' information.

**Key Words:** XARL, XBRL.

## 1. Giriş

Bilgi çağında yaşadığımız bu günlerde teknolojinin gelişim hızını yakalayabilmek oldukça önemli bir problemdir. Gelişim hızını yakalamayıp geride kalan organizasyonlar, rekabette geri kalma ve unutulma durumuyla karşı karşıya kalmaktadır. Bilgi çağında kuşkusuz en hızlı gelişim internet ve ağ sistemlerinde gerçekleşmektedir. Organizasyonlar bilişim sistemlerini kullanmakta olup, zaman içinde bu sistemlere yeni işlevler eklenmesi talep edilmekte ve mevcut sistemler de daha etkin ve verimli kullanılmaya çalışılmaktadır. Bir kurumun bilgi varlığının büyük bir kısmı bu sistemler tarafından kapsanır hale gelmektedir. Bütün bunların sonucu bilgisayar teknolojilerine olan bağımlılık gittikçe artmaktadır. Teknoloji kullanımı sayesinde kazanılan pek çok yarar olmakla birlikte, bu sistemlerin değişik olumsuz etkileri gözlenmektedir [14]. 1950'li yıllarda bilgisayarların icadından bu yana internet kavramı 1960'ların sonu 1970'lerin başında ARPANET adlı ağ sistemine kadar uzanmaktadır. Ancak modern anlamda internet kavramı 1980'ler ve 1990'larda

internet protokolleri (TCP/IP) ve World wide web (www) konsorsiyumlarının oluşturulması ile başlamaktadır [19]. 2000'li yıllara gelindiğinde ise internet artık hayatın vazgeçilmez bir unsuru haline gelmiştir.

Teknolojinin bu denli gelişimi her meslek alanında olduğu gibi muhasebe mesleğini de kuşkusuz etkilemiştir. Bilgisayarların muhasebe mesleğinde kullanımı sayesinde yoğun iş yükü azalmış, insan faktöründen kaynaklanan hataların önüne geçilmeye başlanmıştır. İnternetin mesleğin yapı taşlarına dahil edilmesi ile de ciddi derecede zaman, maliyet ve iş gücü tasarrufu sağlanmıştır. Sağlanan tasarruf sayesinde daha hızlı, daha esnek ve rekabet açısından daha güçlü organizasyonlar kurulmuş, muhasebe mesleği çalışanları asıl yapmaları gereken stratejik planlama işlemlerine yoğunlaşabilmiştir. 1990'ların sonlarına doğru Genişleyebilir Biçimlendirme Dili'nin - XML (Extensible Markup Language) ve Genişleyebilir İşletme Raporlama Dili'nin (Extensible Business Reporting Language) oluşturulması sayesinde

finansal bilgilerin internette yayınlanması ve ilgili taraflara ulaştırılması olanağı sağlanmıştır.

Tüm bu gelişmeler organizasyonlara ciddi avantajlar sağlasa da bir takım dezavantajları da beraberinde getirmiştir. İnternet temel itibarı ile HTML (HyperText Markup Language) tabanlı çalışan bir ağ sistemidir ve açık kodlu bir yazılım diline sahiptir. Açık kodlu dilden kasıt, istenildiği zaman ek bir takım programlar yardımı ile istenilen bilgilere ulaşmak mümkün kılınabilir. Bu açık kod dili çoğu zaman ilgili tarafların finansal bilgileri istediği gibi görmesini, biçimlendirmesini, raporlamasını sağlarken aynı zamanda finansal bilgilerin güvenliğini de tehdit edebilmektedir. İyi niyetli olmayan kişiler ya da kuruluşlar tarafından finansal bilgilerin değiştirilmesi ya da manipüle edilmesi ihtimali oldukça ciddi bir sorunu ortaya çıkarmaktadır. Sorun, finansal bilgilerin güvenliği, güvenilirliği nasıl sağlanmalı ve nasıl sağlam tutulmalıdır? Bu sorunun cevabı için yine XML tabanlı Genişleyebilir Güvenli Raporlama Dili – XARL (Extensible Assurance Reporting Language) geliştirilmiştir. Bu internet yazılım dili kendi içerisinde oluşturduğu protokoller ve güvenlik önlemleri ile finansal bilgilerin internet üzerinden, kötü amaçlı kişilerin müdahalelerini önleyerek, güvenli bir biçimde ilgili taraflara ulaştırılmasını amaçlamaktadır.

## 2. İnternette Finansal Raporlama: XBRL

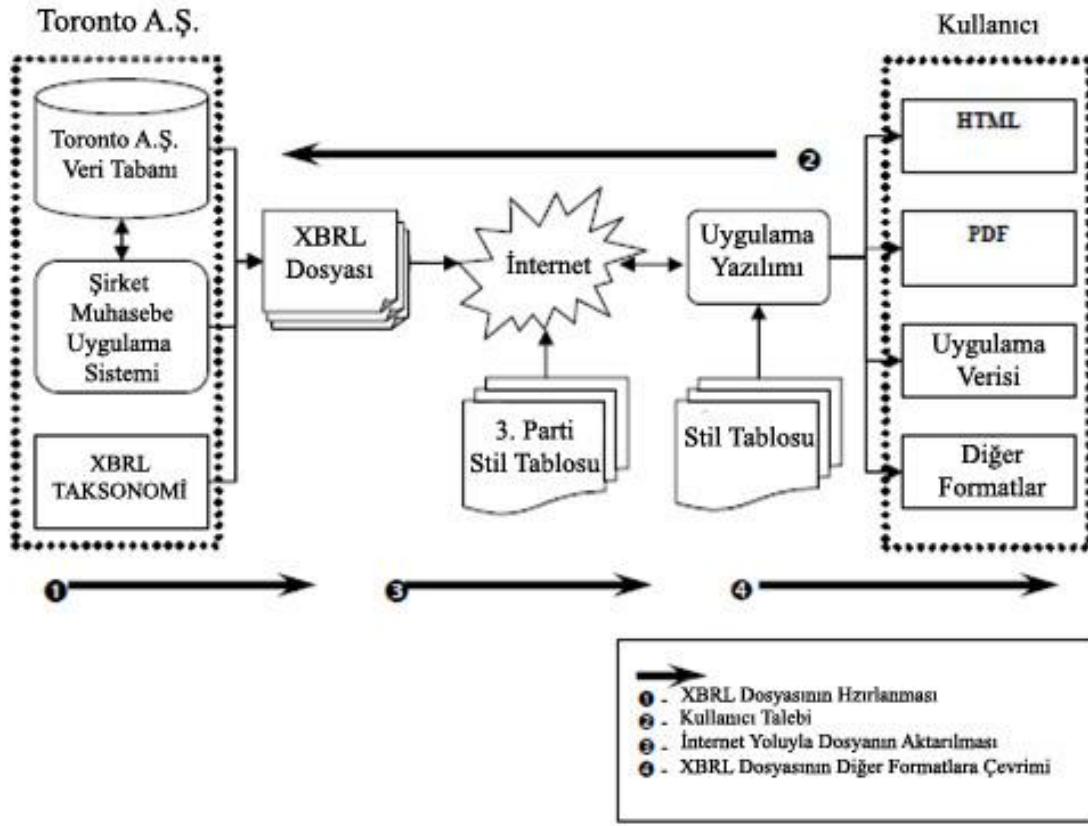
Genişleyebilir Finansal Raporlama Dili (XBRL - Extensible Business Reporting Language), Genişleyebilir Biçimlendirme Dili'nin (XML - Extensible Markup Language) sisteminin finansal raporlama için geliştirilmiş hali olarak ifade edilebilir [7]. Sistem, varlık, sahiplik, sermaye, kar vb. tüm finansal bilgileri etiketler yardımı ile çevrimiçi ortama aktarılmasına dayanmaktadır. Etiketlerden kasıt, verilerin aktarılması için kullanılan bir HTML (Hypertext Markup Language) temel dil kurallarıdır, bu kurallar temel bir internet sayfasının tasarlanmasında kullanılan kurallardır [12]. İlgili taraflar yani kullanıcılar kolaylıkla sisteme ulaşabilir ve istedikleri bilgileri, istedikleri formatta etiketler yardımı ile görebilir, aktarabilir, çeşitli uygulamalar yardımı ile analiz edebilir [13] [5].

XBRL, Amerika Sertifikalı Muhasebeciler Enstitüsü'nün (AICPA) de içinde bulunduğu altı bilgi teknolojisi şirketi ve beş büyük muhasebe şirketi ile oluşturulan bir konsorsiyum tarafından tasarlanmıştır. Konsorsiyum daha sonradan XBRL'nin yaygın kullanımını sağlamak amacı ile 650'den fazla şirketten yardım alarak büyümüştür [2] [8]. Günümüzde XBRL sistemlerini dünya üzerinde 23'den fazla ülke resmi olarak kullanmaktadır [17].

İşleyiş açısından XBRL daha önce de bahsedildiği gibi bir etiketleme sistemine dayanmaktadır. Söz konusu etiketlere XBRL sistemi içerisinde taksonomi adı verilmektedir [3]. Taksonomi mali tabloların içeriğini standart bir biçimde tanımlar ve sınıflandırır. Bu süreçte veri olarak kabul edilen finansal bilgi muhasebe sisteminden alınır ve standart bir formata dönüştürülür. Daha sonra XBRL dokümanları taksonomiler ile tanımlanarak gerçek finansal şekilleri meydana getirmektedir [15]. Bu şekilde çalışarak, işletmenin finansal verileri ile ilgili tüm taraflara hızlı, etkin, düşük maliyetli ve istenilen formatlarda tablolar oluşturabilmektedir.

Boritz ve No [4], XBRL'nin işleyişini Toronto Şirketi örneği ile Şekil 1'deki gibi açıklamışlardır:

1. Toronto Şirketi'nin muhasebe veri tabanı XBRL aracılığı ile internet ortamına aktarılmaktadır. Öncelikle tüm finansal veriler XBRL taksonomileri yardımıyla XBRL dosyaları haline getirilmektedir.
2. İkinci olarak Toronto Şirketi'nin finansal raporları ile ilgilenen kullanıcılar, internet üzerinden belirli bir XBRL uygulaması aracılığı ile şirkete başvurmakta ve XBRL dosyalarını yine internet aracılığı ile talep etmektedir.
3. İstenilen finansal bilgileri içeren XBRL dosyaları kullanıcılara internet yoluyla gönderilmektedir.
4. Son olarak bir XBRL uygulaması aracılığı ile edinilen finansal bilgiler, istenilen rapor şekline ve dosya formatına dönüştürülerek kullanıcıların incelemesine sunulmaktadır.



Şekil 1. XBRL İşleyiş Şeması

Kaynak: Boritz, J. (2004)

### 3. İnternette Finansal Raporlamada Güvenlik: XARL

İnternette güvenlik, işletmeye gönderilen ve işletmenin dışarıya gönderdiğiniz bilgilerin güvenli bir şekilde aktarılabilmesidir. İnternete ilişkin güvenlik konuları internetin güvensiz, güvenilir ve sağlıklı oluşu gerçeğinden hareketle önemlidir. Yapısında bulunan güvenlik problemi nedeniyle internet davetsiz misafir ve hackerlerin saldırısına uğramaktadır. Bununla birlikte XML başlangıçta güvenlik konusuna hitap etmemiştir. Böylece XML tabanlı finansal raporlama hizmetleri ve uzantıları niteliği gereği güvenli değildirler. Finansal raporlama hizmetlerinde güvenliği tehdit eden başlıca konulardan bazıları; mesajları tahrif etme, gizli kalması gereken ya da ulaşmaması gereken yerlere bilginin ulaştırılması veya ifşası, mesajın ikame edilmesi, internet üzerinden bilgisayarları tanımlayan kodların hileli bir şekilde yanlış tanıtılması, hizmetin yalanlanması ve virüs saldırıları şeklinde sıralanabilir.

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden

bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanabilir. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması olarak düşünülebilir [16]. Bilgi güvenliği yönetimi, firmanın elektronik varlıklarının gizlilik, bütünlük ve kullanılabilirlik açılarından baştan sona korunmasını sağlamaktır. Bunun için yönetim ekibinin yüklendiği sorumluluk ve göstereceği liderlik, kurumsal yapı, kullanıcıların farkındalığı ve konuya bağlılığı, kurumsal politikalar, usuller, süreçler, teknolojiler ve yürürlükteki standart ve yasal şartlara uyum mekanizmaları gibi faktörlerin birbirini destekler şekilde çalışmasını sağlamaktır [14]. Finansal raporlama hizmetleri, türdeş olmayan bilgisayar sistemleri tarafından üretilen ve dağıtılan finansal bilgiyi birbiri ile bağlantılı birçok kullanıcıya sağlamalıdır. Bununla birlikte güvenlik gerekleri bu hizmeti sunanların finansal bilgiyi yalnızca yetkili alıcının elde edebilmesine izin verecek şekilde tasarlanmasını ve gerekirse finansal bilgiye kimin erişeceği kararını garanti etmelidir.

İşletmelerin muhasebe kayıtları ve mali tablolarda sunulan bilgilerinin güvenilirliği için ön koşul, muhasebe bilgi sisteminin güvenlik altına

alınmasıdır. Muhasebe verilerinin bilgi teknolojilerinden yararlanılarak hazırlanmasından itibaren, muhasebe bilgi sisteminin güvenliği daha fazla önem kazanmıştır. İşletme yönetiminin muhasebe bilgi sistemlerinin güvenliğinden sorumlu olması nedeniyle; muhasebe verilerinin güvenilirlik derecesini artırmak, gerekli güvenlik tedbirlerini almak, geliştirmek ve uygulamak yükümlülüğü bulunmaktadır. Bilgi teknolojisi sisteminde, aşağıdaki güvenlik ilkeleri uygulandığı zaman, daha güvenilir muhasebe bilgileri üretilebilmektedir. Bu ilkeler IFAC tarafından genel kabul görmüş muhasebe ilkelerine ilaveten yeni güvenlik ilkeleri olarak ortaya konmuşlardır [10]:

**Gizlilik (Confidentiality):** Bu ilke ile üçüncü kişilerden elde edilen bilgilerin yetki olmaksızın başkalarına iletilemeyeceği veya açıklanamayacağı ifade edilir. Şifreleme teknolojisi gibi bazı teknik ölçütler, kişisel bilgilerin üçüncü kişilere transferinin kısıtlanması, şifrelenmiş verilerin yetkili üçüncü kişilere transferinin sağlanması, belgelerin doğruluğunun sağlanması ve kayıtlı kişisel verilerin belli bir zaman dilimi içinde silinmesi ile ilgili talimatları içerir.

**Bütünlük (Integrity):** Bu ilke ile muhasebe verileri ve bilgilerinin tamamlanıp doğrulanması, sistemin işler hale gelmesi ve tüm bu veri, bilgi ve sistemin, yetkisi olmayan kişiler tarafından sisteme girilerek veri değişimi ve manipülasyon yapmasına karşı korunması ifade edilir. Bu üç şartın yerine getirilmesi durumunda, bütünlük ilkesi yerine getirilmiş olur.

**Güvenilirlik (Authenticity):** Bu ilke ile güvenilirlik ilkesini kabul etmiş kişilere işletme işlemleri yetki prosedürleri kullanılarak izlettirilir. Veri ve bilgiler otomatik olarak değiştirildiğinde, karşı tarafın dijital imza prosedürleri kullanılarak tanınması önemlidir.

**Kabul edilebilirlik (Non-repudiation):** Bu ilke, bilgi teknolojisi içeren prosedürlerin arzulan yasal sonuçları da beraberinde getirmesi yeteneği olarak tanımlanır. Bu yeteneğin yerine getirilmesi, işlemlerin yetkisiz kişiler tarafından yapıldığı gerçeğini gizlemek için işlemler yapan personel için imkânsızdır. Genel şifreleme sisteminin kullanımı bu tür olumsuzlukları ortadan kaldıracaktır. Yukarıda anlatılan ilkeler, güvenli bilgi ihtiyacının karşılanmasında yardımcı olur. Bu anlatılan ilkeler elektronik işletme çevresinde, güvenilir bilgilerin yaratılmasında gereklidir. İşletme yöneticileri de bilgi teknolojilerinin kullanıldığı muhasebe bilgi sistemlerinin, bu tip risklerden korunması amacı ile gerekli tüm tedbirleri alması gereklidir. Sonuç olarak, yöneticilerin bilgi güvenliğini sağlamak amacıyla yukarıda sayılan ilkeleri bir yasa gibi tüm ülkede yerleşmesine yardımcı olmaları gereklidir.

**Yetkililik (Authorization) :** Bu ilke, sadece belli kişilerin belli veri, bilgi ve sistemi kullanabilmesi ve sadece yetkili kişilerin bu sistem için tanımlanmış hak ve yetkileri kullanabilmesi anlamına gelmektedir. Bu haklar, elektronik işletme sistemindeki bilgilerin silinmesini, değiştirilmesini, okunmasını ve oluşturulmasını içermektedir. Bunu başarmak için gerekli metodlar ise fiziksel ve mantıksal güvenlik prosedürleridir.

**Uygunluk (Availability):** Bu ilke, yönetimin, işletme faaliyetlerinin sürdürülebilmesi için donanım, yazılım, bilgi ve verilerin sürekli bir şekilde var olmasını ve gerekli bilgi teknolojisi organizasyonunun makul bir zaman dilimi içinde işletilebilir olmasını garantilemeyi ifade eder. Örneğin, acil durumlar için yedekleme prosedürlerinin oluşturulması önemlidir. Yine, dijital kayıt ve defterlerin, kısa bir sürede insanlar tarafından okunabilir hale getirilmesi, önemlidir. Bu dönüşümün, kısa sürede ve güvenli bir şekilde olması gerekir

Söz konusu ilkeler ışığında muhasebe bilgi sisteminde güvenlik yapılandırılması oluşturulması gerekmektedir. Özellikle XBRL belgelerinin açık internet üzerinden yayınlanmaları şirketlerin sadece kendi çıkar grupları ile paylaşmaları gereken belgelerin bir takım tehditlerle karşı karşıya kalmalarına neden olmaktadır. Bu tehditler Bosworth ve Kabay'ın [9] çalışmalarında yedi grupta toplanmıştır. İlk olarak belgelerde değişiklik yapılma tehdidi mevcuttur ki istenmeyen kişiler internet aracılığı ile XML kodlarına fazladan bilgiler ekleyebilir, değiştirebilir veya silebilir. İkinci olarak, kötü niyetli kişiler veri transferi sırasında kullanıcının kişisel bilgilerini ifşa edilmektedir. Bir diğer tehdit de istenmeyen kişilerin Örneğin bir XBRL dosyasını kendi oluşturduğu başka bir dosya ile değiştirme tehlikesi yani bilgilerin tamamen manipüle edilmesidir. İnternet aracılığı ile IP adresleri taklit edilen kullanıcılar adına XBRL bilgileri çalınabilmektedir. Başka önemli bir tehdit ise sunucuların tahribata uğramasıdır. Kullanıcıların bilgilere erişimlerini engelleyen bu yöntem bilgilerin çalınması ya da değiştirilmesi gibi bir tehdit içermezken, kullanıcıları zaman, para ya da itibar kaybına uğratabilmektedir. Veri takibi sonucu finansal verileri talep edenlerin kullanıcı adlarının ve şifrelerinin ele geçirilmesi de olası bir tehdit olarak karşımıza çıkmaktadır. Son olarak en ciddi tehdit olan bilgisayar virüsleri gelmektedir. Bilgisayar virüsleri gerek sağlayıcıları gerekse istemci bilgisayarları etkileyerek, bilgi kayıplarına, sistem göçmelerine ya da başka istenmeyen kişilerin saldırılarına neden olmaktadır.

Tüm bu ilkeler ve tehditler çerçevesinde, konuya getirilebilecek en önemli çözüm önerisi şifreleme

olarak karşımıza çıkmaktadır. Şifreleme, verinin sayısal ortama geçmeye başlamasıyla güvenlik konusu ön plana çıkmış, işletmelerin özenle topladıkları verilerin, kötü niyetli kişilerce ele geçirilip kullanılabilme olasılıkları hep bir soru işareti olarak kalmıştır [11]. Güvenlik yapılandırılmaları öncelikle bir takım ağ üzeri protokollerle sağlanmaya çalışılmıştır. Bu ağ üzeri çözümler kullanıcı şifreleri ve internet veri akışını şifreleyen SSL/TLS<sup>1</sup>, S-HTTP<sup>2</sup> ve VPN<sup>3</sup> gibi protokollerdir (Boseorth ve Kabay 2002). SSL/TLS, güvenli soket katmanı/aktarım katmanı güvenliği olarak tanımlanabilen ağ üzerindeki mesaj iletişiminin güvenliğinin yönetimi oluşturulmuş bir şifreleme protokolüdür. S-HTTP, güvenliği artırılmış HTTP sistemi olarak tanımlanabilir. Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilmektedir. İnternette sunucular ve son kullanıcılar arasında bilgilerin başkaları tarafından okunamayacak şekilde nasıl aktarılacağına dair kurallar ve yöntemleri düzenleyen bir sistemdir. VPN ise, güvenli ve özel veri aktarımını sağlayan sanal özel ağ teknolojisi olarak tanımlanabilir. Özel telekomünikasyon şirketlerinin topluma açık ağ kapasitesinin bir kısmını özel kuruluşlara tahsis etmesi veya kiralaması şeklinde, kişiye özel ağ olarak tasavvur edilebilir.

Veri transferlerinde önemli bir güvenlik seviyesi sağlamalarına rağmen SSL/TLS, S-HTTP, VPN bazı özellikleri açısından XBRL belgelerinin aktarımları için yeterli güvenlik ölçüsü vermemektedir [7]. İlk olarak bu güvenlik protokolleri sunucu ve istemci arasında direkt bir şifreleme modeline sahiptirler, ancak XBRL dosyaları birden fazla aracı arasında hareket etmektedir. Böyle bir trafikte noktadan noktaya bir güvenlik ağı kurmak hem oldukça zor hem de oldukça pahalı bir yol olacaktır. İkinci olarak ağ sisteminin şifrelenmesi XBRL dosyalarının şifreleme mantığı ile örtüşmemektedir. Kullanıcı finansal bilgi içeren dosyanın sadece bir kısmını görmek için şifre aldıysa, tamamı şifrelenmiş bir ağdan gelen dosyayı açmakta zorlanacaktır. Özetle söz konusu ağ şifreleme modelleri, hem sunucu hem de istemci tarafında yapılarak notadan noktaya bir güvenlik sistemi oluşturduğu ve sunucu-istemci trafiğinde eksikliklere sahip olduğu açılarından eleştirilmektedir.

---

<sup>1</sup> Secure Sockets Layer(SSL)/Transport Layer Security(TLS)

<sup>2</sup> Secure Hypertext Transfer Protocol (S-HTTP)

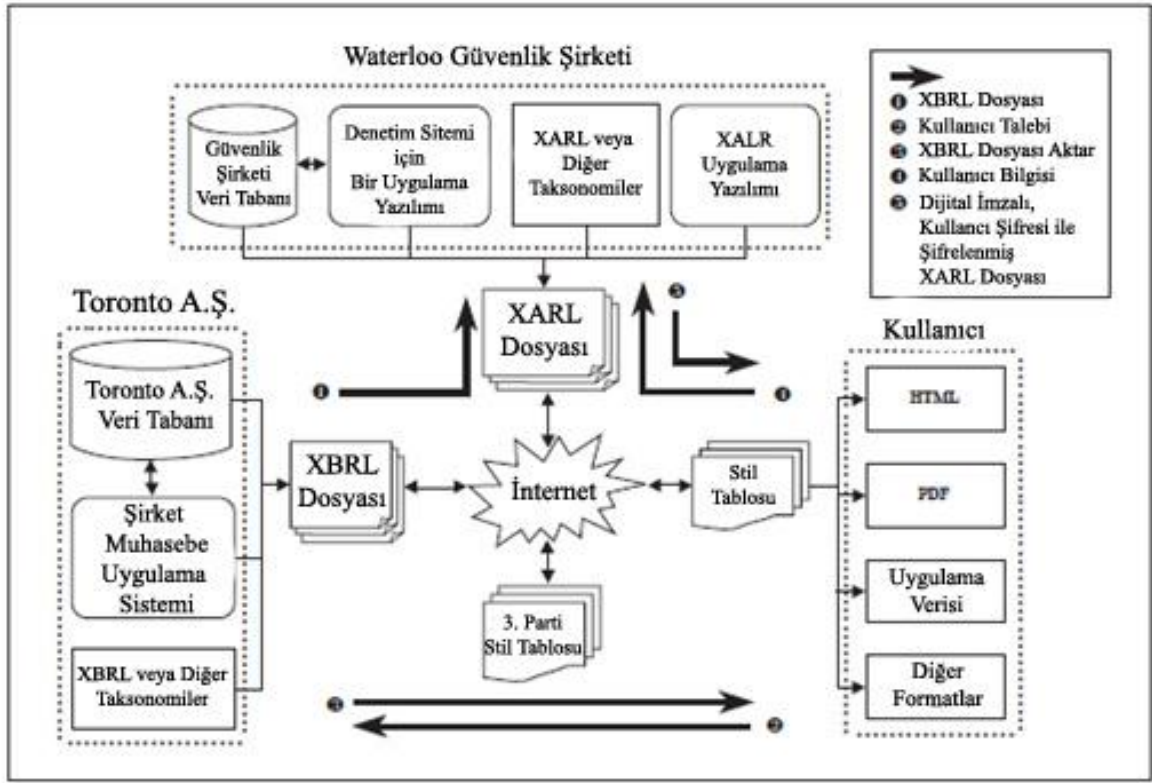
<sup>3</sup> Virtual Private Network (VPN)

Genişleyebilir Güvenli Raporlama Dili – XARL (Extensible Assurance Reporting Language) tüm bu eleştirilere ve eksikliklere karşı başka bir çözüm olarak tasarlanmıştır. XML tabanlı ve XBRL'nin uzantısı olarak, finansal bilgilerin internet yoluyla dağıtımı aşamasında güvenliği sağlamak ve kullanıcılara bu finansal bilgilerin doğruluğu hakkında garanti vermek amacı ile oluşturulan XARL, belirli bir şirkete ait finansal bilgilerin başka bir güvenlik ve denetim şirketi aracılığı ile kontrol edilerek şifrelenmesi ve XARL taksonomileri ile yazılması şeklinde işleyen bir düzene sahiptir.

#### 4. XARL İşleyişi

XALR çalışma şekli olarak XBRL'ye oldukça benzemektedir. Bir takım etiketler yardımı ile finansal bilgilerin doğruluğunu ve güvenilirliğini garanti altına almaktadır. Bu etiketlerde güvenlik tipi, garantiye alınma zamanı, bilgiyi giren kişinin elektronik imzası vs. bilgiler bulunmakta ve kullanıcının belgelere güvenilirliğini arttırmayı amaçlamaktadır [6]. ZBoritz ve No [6], XARL'nin işleyişini aynı XBRL'de olduğu gibi, Şekil 2'de Toronto Şirketi, Waterloo Güvenlik Şirketi ve kullanıcı örneği ile anlatmışlardır. Buna göre XARL şu şekilde çalışmaktadır:

1. İlk olarak aynen XBRL çalışma sisteminde olduğu gibi, işletme finansal bilgilerini XBRL taksonomileri aracılığı ile gruplara ayırmaktadır. Toronto Şirketi'nin veri tabanındaki muhasebe verileri XBRL dosyalarına dönüşmektedir. Ancak XBRL'de olduğu gibi bu dosyalar doğrudan internet ortamına verilmektense, Waterloo Güvenlik Şirketi gibi bir güvenlik sağlayıcısının şirket veri tabanına gönderilmektedir.
2. Waterloo Güvenlik Şirketi, XBRL kullanıcısı işletmelere şifreleme sistemleri sayesinde güvenlik hizmeti veren şirketlerden biridir. Bu noktada, Toronto Şirketi'nden aldığı XBRL dosyalarını kendi veri tabanında depolama ve bunları XARL taksonomileri ile tekrar yazma işlemlerini yerine getirmektedir. XARL taksonomileri ile yeniden yazılan Toronto Şirketi'ne ait veriler, yine şirkete özel tasarlanmış güvenlik ve garanti bilgilerin içeren XARL dosyalarına dönüşmektedir. Güvenlik sağlama işlemi ayrıca finansal verilerin doğru taksonomilerle yazılıp yazılmadığını da denetleyerek, verilerin doğruluk sağlamasını da yapmaktadır.
3. Toronto Şirketi'nin finansal raporlarına ihtiyaç duyan kullanıcılar verileri şirketten XBRL dosyası olarak internet aracılığı ile talep etmektedir. Ancak şifrelenmemiş XBRL



Şekil 2. XARL İşleyiş Şeması

Kaynak: Boritz, J., No, W.G. (2003b)

dosyaları, dolandırıcılığa, kötü amaçlı değiştirmelere ve çalınmalara karşı savunmasız haldedir. Bu nedenle kullanıcıların finansal bilgilere erişim talepleri, Toronto Şirketi tarafından, daha güvenli olan XARL dosyalarını edinme amacıyla Waterloo Güvenlik Şirketi'ne yönlendirilir. Güvenlik şirketi öncelikle, Toronto Şirketi tarafından kendisine yönlendirilen kullanıcılara, internet aracılığı ile ya da elden bir "kurumsal anahtar (şifre)" sağlamaktadır.

4. Kurumsal anahtarın kullanıcıya ulaşmasının ardından Waterloo Güvenlik Şirketi, internet aracılığı ile XARL dosyalarını kullanıcıya aktarmaktadır. XARL dosyaları Waterloo Güvenlik Şirketi tarafından dijital olarak imzalanmış ve kurumsal anahtarın açabileceği şekilde şifrelenmiş belgelerdir.
5. XARL dosyaları kullanıcının eline ulaştıktan sonra kurumsal anahtar yani şifre kullanılarak açılır. Bu noktadan sonraki kısım aynen XBRL'de olduğu gibi istenilen bilgiler, istenilen formattaki raporlara dönüştürülerek kullanılabilir.

Tüm bu işleyiş sonucunda, kullanıcıların finansal bilgilerin yanlışlığına dair şüpheleri ortadan kaldırılmış olmaktadır. Çünkü finansal veriler güvenlik şirketleri tarafından hem doğru kodlama açısından denetlenmiş, hem de güvenlik açısından şifrelenmiş XARL dosyaları şeklinde kullanıcılara

ulaşmaktadır. XARL taksonomileri, finansal bilgileri şifrelerken aynı zamanda da etiketlemektedir. Söz konusu etiketler güvenlik bilgilerinin yanı sıra, XBRL dosyalarında olduğu gibi içerik hakkında da bilgi vermektedir. Temel bir XARL dosyası oluşturulurken şu etiketler standart olarak dosyada yer almaktadır:

- Kaynak şirket bilgileri
- Güvenlik şirketinin adı
- Rapor başlığı
- Adresler
- Açıklayıcı bilgiler
- Kullanım kısıtlama bilgileri
- Oluşturulma tarihi

XARL ham dosyaları içerisinde yer alan bu etiket bilgiler kullanıcıların doğrudan görebileceği bir biçimde tasarlanmamıştır. Söz konusu belgeler HTML formatında kodlardan oluşmakta ve kullanıcı tarafından okunabilmesi için yardımcı uygulamalara gerek duyulmaktadır. Bu uygulamalar kimi zaman bir internet tarayıcısı olabilirken kimi zaman özel nitelikli bir program da olabilmektedir. XARL dosyalarının içerisinde şifrelenmiş biçimde saklanan şirket finansal bilgilerini çoğu zaman günlük kullanımdaki bir internet tarayışı ile

okumak, incelemek mümkün olmamaktadır. Özel tasarlanmış programları kullanarak daha verimli bir inceleme yapmak mümkün olmaktadır. Zira Amerika Birleşik Devletleri 2005 yılında Menkul Kıymetler Komisyonu'nda (SEC), EDGAR programı kullanılmaya başlanmıştır [20].

XARL dosyalarının işleyişi esnasında sağladığı bir diğer hizmet ise dijital imzalama teknolojisidir [6]. XBRL ve XARL gibi dijital ortamdaki finansal belgeler bilindiği üzere basılı belgelere dayalı muhasebe sisteminin artık kullanılmamasına neden olmuştur. Bu durumun bağımsız denetçi kuruluşların finansal tabloları ve bilgileri denetimden geçirerek belirttikleri raporların da dijital ortama taşınmasını sağlamıştır. XARL dosyaları üzerinde "Denetlenmiştir" şeklinde ibarelerin yer alması, bu bilgilerin doğruluğunu ve güvenilirliğini bir kat daha arttırmaktadır. Kullanıcının istediği takdirde söz konusu şeklin üzerine basarak denetim raporunu dijital olarak görebilmesi de XARL'nin diğer bir işleyiş modülüdür.

#### 4.1. XBRL ve XARL Arasındaki Farklılıklar

XBRL ve XARL arasındaki farklar Tablo 2'de özetlenmektedir [6].

	<b>XBRL</b>	<b>XARL</b>
<b>Güvenlik Elementleri</b>	XBRL taksonomisinin bir parçası	Dosyadan ayrı bir güvenlik taksonomisi
<b>Bilgi</b>	Sadece muhasebeci raporlarına ilişkin bilgiler içerir	Güvenlik amaçlı kapsamlı bilgi içerir
<b>Güvenlik Aralığı</b>	Tüm finansal bilgilerin güvenliği	Sadece finansal bilgiler değil standartlarla belirlenen tüm bireysel finansal bilgilerin, araçların, sistemlerin güvenliği
<b>Bölümlendirme</b>	Güvenlik bilgisi XBRL dosyasının bir parçası olarak oluşturulur	Güvenlik bilgisi her kullanıcıya özel oluşturulur ve ayrı bir dosyada ulaştırılır
<b>Elemanlar</b>	-Hesap bilgileri -Rapor bilgileri elemanlarından oluşur	-Güvenlik bilgileri -Rapor bilgileri -Açıklayıcı bilgiler -Güvenlik içeriği -Kullanıcı bilgisi elemanlarından oluşur.

**Tablo 2.** XBRL ve XARL Karşılaştırması

Kaynak: Boritz, J., NO, W.G. (2003b)

Karşılaştırma beş ana başlık altında yapılmıştır. Sonuç olarak, XBRL kendi içerisinde temel anlamda bir güvenlik alt yapısına sahiptir. Ancak internetin korunmasız ortamı içerisinde güvenliğin önemi ciddi derecede artmaktadır. XARL ise, kapsadığı güvenlik alanı ve işleyişi açısından XBRL'ye göre oldukça yüksek bir güvenliğe sahiptir. Kullanıcıların kendine özel bilgileri kullanarak şifreleme yapması en önemli ve aşılması zor güvenlik önlemi olarak karşımıza çıkmaktadır.

#### 5. Sonuç ve Öneriler

Günümüz finansal raporlama işlemlerinde artık internet büyük önem taşımaktadır. 1990'lı yıllarda yeni yeni kullanılmaya başlayan internet; şirketlerin kendi resmi sitelerinden finansal raporlarını yayınlamaları fikri ile muhasebe bilgilerinin raporlanması ve iletilmesinde önemli bir çığır açmıştır. Her şirketin finansal raporlarını standart bir biçimde görme ve karşılaştırma ihtiyacı önce XML'in muhasebe bilgilerinin iletilmesinde kullanılmasına daha sonra da XBRL'nin geliştirilmesine neden olmuştur. Tüm bu gelişmeler, şirket bilgileri ile ilgili tarafların bu bilgilere en hızlı, en az maliyetli ve istedikleri formatta ulaşmalarını sağlamıştır. Bu yararlar ciddi maliyet ve emek tasarrufu sağlamış, şirketler daha az iş yükü sayesinde stratejilerle daha çok ilgilenme olanağı kazanırken; yatırımcılar, analistler ve diğer ilgili taraflar daha hızlı bir biçimde şirketlerin finansal yapılarını inceleme imkanı bulmuşlardır.

İnternet sayesinde ulaşılabilen tüm bu yararların yanında, internetin bir takım sakıncaları da yeni sorunlar doğurmuştur. Bu sorunlardan en önemlisi ve ciddi olanı güvenlik sorunu olarak karşımıza çıkmaktadır. XBRL dosyalarının, kamuya ve dolayısıyla tüm saldırılara açık internet ağı yoluyla kullanıcılarına gönderilmesi, bu dosyaların kötü niyetli kişilerce değiştirilmesi veya manipüle edilmesine davetiye çıkarmaktadır. Sorun karşısında birçok çözüm önerisi de ortaya atılmıştır. Önerilerin başında internet protokolleri ile oluşturulmuş güvenlik sistemleri yer almaktadır. Bu sistemler bilgilerin oluşturulduğu noktada şifrelenmesi ve ulaştığı noktada da şifresinin çözülmesi şeklinde işlemektedir. Ancak noktadan-noktaya oluşturulan bu güvenlik sistemi XBRL dosyalarının nitelikleri gereği güvenlik sağlamada yetersiz kalabilmektedir. XBRL dosyalarının ve dolayısıyla finansal bilgilerin güvenilirliği ve güvenliğini sağlamak amacıyla daha bütün uçtan-uca şifreleme sistemlerinin kullanılması gerekmektedir. Bu amaçla XARL dosyaları geliştirilmiş ve uygulamaya konulmuştur. XARL şifreleme işlemini ayrı bir güvenlik şirketi yardımı ile gerçekleştirmektedir. Böylece finansal bilgilerin hem doğruluğu denetlenmekte, hem de şifreleme sayesinde uçtan-uca bir güvenlik sağlanmaktadır.

Kullanıcılara özel şifreli taksonomilerle yazılan XARL dosyaları, yine kullanıcıya has bir kurumsal anahtar yardımı ile güvenli bir biçimde internet aracılığı ile aktarılmaktadır.

Tüm bu gelişmeler göstermektedir ki, muhasebe mesleği gelecekte oldukça fazla ilerleme kaydedecektir. Özellikle bilgilerin hızlı ve güvenli bir biçimde aktarımı sayesinde, finansal piyasalar “Etkin Piyasa Hipotezi” deki etkin piyasa kavramına daha da yakınlaşılması kaçınılmazdır. İnternet aracılığı ile finansal raporlama açısından gelecek süreçlerin daha da kısaltılması aşamasında olması muhtemeldir. XARL dosyalarının oluşturulması oldukça uzun bir süreçtir ve teknolojik gelişmeler sayesinde bu sürecin daha hızlı, daha kısa ve daha güvenilir hale gelmesi kaçınılmazdır.

## 6. Kaynaklar

- [1] Altunsöğüt, Ö. ve Uçar, E. (2006) “Veri Tabanı Bağlantı Ayarlarının Şifrelenerek XML Dosyasında Saklanması” **Pamukkale Üniversitesi Bilgi Teknolojileri Kongresi IV Akademik Bilişim Kongresi 2006 Bildiriler Kitabı**: 484-487.
- [2] Arndt, H. K. ve diğerleri (2006) “Sustainability Reporting Using the eXtensible Business Reporting Language (XBRL)” [http://bauhaus.cs.uni-magdeburg.de:8080/miscms.nsf/4E5CEFA594537DF5C125743E00705200/17ADD1D1EDD598E4C12574D500296459/\\$FILE/IFU06.pdf](http://bauhaus.cs.uni-magdeburg.de:8080/miscms.nsf/4E5CEFA594537DF5C125743E00705200/17ADD1D1EDD598E4C12574D500296459/$FILE/IFU06.pdf), (10.04.2011)
- [3] Blundell, W.A. (2007) “Continuous Auditing Technologies and Models” **Yayınlanmamış Yüksek Lisans Tezi**, Nelson Mandela Metropolitan University, South Africa.
- [4] Boritz, J. E. (2004) “Managing Enterprise Information Integrity - Security, Control and Audit Issues” USA: **IT Governance Institute**.
- [5] Boritz, J.E. ve No, W.G. (2003a) “Business Reporting with XML: XBRL (Extensible Business Reporting Language)” The Internet Encyclopedia, **John Wiley**, New York.
- [6] Boritz, J.E. ve No, W.G. (2003b) “Assurance reporting for XBRL: XARL (Extensible Assurance Reporting Language)” Trust and Data Assurances in Capital Markets: The Role of Technology Solutions
- Research Monograph sponsored by **PricewaterhouseCoopers**: 17-31.
- [7] Boritz, J.E. ve No, W.G. (2005) “Security in XML-based financial reporting services on the Internet” **Journal of Accounting and Public Policy**, No: 24:11-35.
- [8] Bovee, M. (2005) “Financial Reporting and Auditing Agent with Net Knowledge (FRAANK) and Extensible Business Reporting Language (XBRL)” **Journal of Information Systems**, 19 (1): 19-41.
- [9] Bosworth, S., Kabay, M.E., (2002) “Computer Security Handbook” 4 Ed. **John Wiley & Sons Inc.**, New York.
- [10] Dinç, E. ve Varıcı, İ. (2008) “E- İşletme Olgusunun Muhasebe İlke ve Uygulamaları Üzerine Etkisi” **Sosyal Bilimler Dergisi**, X (1): 191-211.
- [11] Feitsma, P. A. W. (2008) “Security in the XBRL Business Information Supply Chain An explorative study on integrity and authentication issues in the XBRL Business Information Supply Chain” **Master’s thesis**, Erasmus University Rotterdam Erasmus School of Economics Economics & Informatics Economics and ICT programme.
- [12] Garthwaite, C. (2000) “The Language of Risk: Why the Future of Risk Reporting is Spelled XBRL” **Balance Sheet**, 8 (4): 18-20.
- [13] Hoffman, C. ve Strand, C. (2001) “XBRL Essentials” **AICPA**, New York.
- [14] Kuyumcuoğlu, M. ve Başoğlu, A.N., (2008) “Bilişim Sistemlerinde Risk Yönetimi Benimseme Modeli” **Yönetim**, 19 (61): 143-164.
- [15] Uyar, S. ve Çelik, M. (2006) “Sürekli Kamuyu Aydınlatma ve İnternet Ortamında Finansal Raporlama Sürecinde Kullanılan Diller” **Ege Akademik Bakış Ekonomi, İşletme, Uluslararası İlişkiler ve Siyaset Bilimi Dergisi**, 2 (6): 93-104.
- [16] Vural, Y. ve Sağiroğlu, Ş. (2008) “Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme”, **Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi** 23 (2): 507-522.
- [17] [www.xbrl.org](http://www.xbrl.org), Erişim Tarihi: 15.04.2011

[18] Zarowin, S. ve Harding, W.E. (2000) "Finally, Business Talks The Same Language"  
**Journal Of Accountancy**, August: 25-30.

[19][http://en.wikipedia.org/wiki/History\\_of\\_the\\_Internet](http://en.wikipedia.org/wiki/History_of_the_Internet), Eriřim Tarihi: 30.04.2011

[20]<http://www.sec.gov/info/edgar.shtml>, Eriřim Tarihi: 17.10.2011