Avrupa Bilim ve Teknoloji Dergisi
Sayı 16, S. 267-274, Ağustos 2019

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
No. 16, pp. 267-274, August 2019

Research Article

Büyük Veride Hadoop Mimarisi ile VoIP Güvenliği Önerisi

Atınç Yilmaz[1*]

[1] Beykent Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0003-0038-7519)

(İlk Geliş Tarihi 26 Mart 2019 ve Kabul Tarihi 25 Mayıs 2019)

(**DOI:** 10.31590/ejosat.544829)

ATIF/REFERENCE: Yilmaz, A. (2019). Büyük Veride Hadoop Mimarisi ile VoIP Güvenliği Önerisi. *Avrupa Bilim ve Teknoloji Dergisi*, (16), 267-274.

Öz

Günümüzde kuruluşların birçoğu, siber saldırıyı etkisiz hale getirmek için anomalileri tanımlamak, tehditleri algılamak, alarmları doğrulamak ve güvenlik olaylarını belirlemek adına güvenlik istihbaratında büyük veri teknolojisini kullanmaktadır. Büyük veride hadoop benzeri mimariler anlık tehditleri rasyonel bir bakış açısı ile hesaplayabilme yeteneğine sahiptir. Bu açıdan büyük verinin mantıksal çözümlemesinden yararlanan kuruluşlar öncelikle gizlilik ve güvenlikle ilgili sorunları halletmek istemektedirler. Büyük veri mimarileri ağ üzerinden yapılan anomali ve sahtekarlık girişimlerinin tespiti için sistemlere destek olmaktadır. Hadoop mimarisi gibi anlık izleme yapabilen gelişmiş Büyük Veri teknolojileri, çok büyük ve karmaşık verilerin depolanmasını ve analiz edilmesini benzeri görülmemiş bir ölçekte ve hızda doğrulamaktadır. Bu çalışmada çok hızlı veri trafiğinde VoIP (Voice Over IP) paketlerinin tespit edilerek, VoIP güvenliğinin sağlanması incelenmiştir.

(Minimum 250 – Maksimum 400 kelime ve içeriğinde amaç, materyal-metot, bulgular ve sonuç kısımlarını içerecek şekilde yazılmalıdır.)

Anahtar Kelimeler: Büyük Veri, Hadoop, VoIP, Ağ Güvenliği.

Proposed VoIP Security with Hadoop Architecture in Big Data

Abstract

Today, many organizations use large data technology in security intelligence to identify anomalies, detect threats, verify alarms, and identify security incidents to neutralize cyber attacks. In large data, hadoop-like architectures are capable of calculating instant threats with a rational perspective. In this respect, organizations that take advantage of the logical analysis of large data primarily want to handle privacy and security issues. Large data architectures support systems to detect anomalies and fraud attempts over the network. Enhanced Big Data technologies, such as the Hadoop architecture, can instantly monitor storage and analysis of very large and complex data on an unprecedented scale and speed. In this study, VoIP packages were determined in very fast data traffic and the security of VoIP was investigated.

(Minimum 250 - Maximum of 400 words and content should be written in a way to include material, method, findings and results.)

Keywords: Big Data, Hadoop. VoIP, Network Security.

[*] Sorumlu Yazar: Beykent Üniversitesi, Mühendislik-Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye, ORCID: 0000-0003-0038-7519, atincyilmaz@beykent.edu.tr

1. Giriş

IP(internet protocol) ağı altyapısı ile haberleşmenin birlikte çalışması mantığı, e-posta servisleriyle başlayarak hızlı mesaj servisi (instant message) ile devam etmiştir. Bu kapsamda 1995 yılında Vocaltec tarafından ilk IP telefon servisi verilmiştir. PC üzerinden arama ise 1998 yılında gerçekleştirilmiştir. Daha sonrasında ise bu mantık telefondan telefona şeklinde uygulanmıştır. Piyasada pazar payı büyük olan Cisco, Lucent, Nortel gibi firmaların Voice Over IP (VoIP) ağ anahtarlarının üretimine önem vermesi ile birlikte ilgili teknolojinin gelişimi hız kazanmıştır. 2000'li yılların başında VoIP trafiği, toplam ses trafiğinin %3'ünü geçmiş; 10 yıl içinde bu oran %44'lere ulaşmıştır.

Paket anahtarlamalı IP ağı üzerinden sesin iletilmesi mantığı VoIP'in tanımını vermektedir. Sesin iletilmesi için öncelikle analog işaretler sayısallaştırılıp sıkıştırılmaktadır. Ardından sıkıştırılmış sayısal veriler paketlere ayrılarak IP ağı üzerinden gönderimi sağlanır. Gönderilen sayısal işaret alıcı tarafında analog işarete dönüşümü sağlanır. Bu adımlar ile tek IP ağı ile veri iletimi tamamlanmış olmaktadır. VoIP az maliyetli olmasının yanında video konferans gibi yeni servislerin ve uygulamaların eklenebilme kolaylığı sayesinde kullanımı artmıştır.

Anomali, problem için tanımlanmış normal nitelikli davranışlara uygun olmayan davranışlardır. Siber saldırıların önlenebilmesi adına kuruluşların bir çoğu anomalileri tanımlamak için büyük veri teknolojilerini kullanmaktadır. Bunun yanında büyük veri teknolojisi güvenlik istihbaratlarında, tehdit algılamalarında, alarmları doğrulamakta kurumlar için uygulanmaktadır. Büyük verinin mantıksal olarak çözümlenmesinin yanında kurumlar için diğer bir risk verilerin güvenliğiğ ve gizliliğidir. Hadoop, Apache Spark gibi teknolojiler büyük veri için potansiyel tehditleri hesaplayabilme yeteneğine sahiptir. Bu gibi teknolojiler çok büyük boyutlu ve karmaşık yapıda olan verilerin depolanıp analiz edilmesini hızlı ve büyük ölçekli şekilde sağlamaktadırlar.

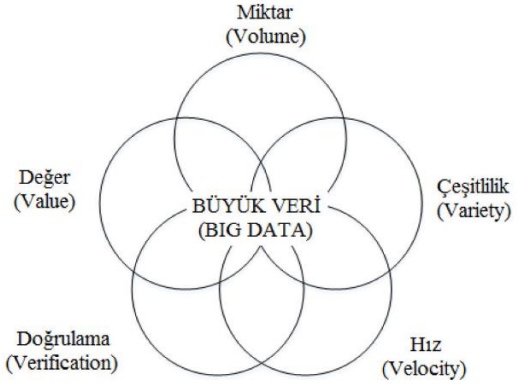
VoIP teknolojisi gerçek zamanlı veri ileten bir sistemdir. Sürekli olarak veri aktarımı gerçekleşmesi ortaya büyük bir veri oluşturmaktadır. Bunun yanında verinin sürekli akmasından ötürü gelen paketler güvenlik riskini arttırmaktadır. Bu çalışmada büyük veri yöntemlerinden biri olan Hadoop mimarisi üzerinden VoIP güvenliği amaçlanarak bir mimari önerilmiştir. Önerilen bu mimari sayesinde VoIP paketleri tespit edilip sınıflandırılarak; paketlerin önceliklendirilmesi sağlanacaktır.

Çalışmanın 2. bölümünde büyük veriden bahsedilecek; 3. Bölümde ise VoIP Teknolojisi ele alınarak önerilen sistem açısından saldırı türlerine yer verilecektir. 4. Bölümde geleneksel güvenlik çözüm önerileri ele alınarak detaylı inceleme sağlanacaktır. 5. bölümde Hadoop mimarisi üzerinden önerilen bir güvenlik yapısı detaylı bir şekilde açıklandıktan sonra son bölümde çalışmanın analizi gerçeklenecektir.

2. Büyük Veri

Büyük Veri (Big Data) terimi nispeten son yıllarda ortaya çıksada, detaylı veri analizi için büyük miktarlarda bilgi toplama ve depolama eylemi uzun yıllardır kullanılmaktadır. Büyük verinin kullanılabilmesi belirli bir ölçeklendirmeye ihtiyaç duymaktadır. Bu bilgiler ışığında, ölçeklendirilemeyen veri yönetimi zorlaştırmaktadır [1].

Yıllar içerisinde bilgisayar ağlarının daha da büyüyerek karmaşıklaşması ve iletişim teknolojilerinin gelişimi veri depolama sistemleri için bazı ihtiyaçlar ortaya çıkartmaktadır. Bu hızlı gelişim ile Sensör Ağları, Sosyal Medya Ağları, Dijital Kütüphaneler ve Arşivler, Multimedya Koleksiyonları ve Web Veri Hizmetleri gibi kullanılan çeşitli bilgisayar sistemleri üretikleri bilgiler ile ortaya büyük bir veri oluşturmaktadır [2]. Bu durum çok büyük verilerin üretildiği, bu verilerin saklanmasının, işlenmesinin ve yönetilmesinin çok önemli olduğu bir tasarıma ihtiyaç duymaktadır. Performans ve esneklik ihtiyacının giderek arttığı bu veri ortamında JAVA kütüphanesi temelli bir tasarım ortaya çıkmaktadır. Bu yeni mimarinin ismi Hadoop (HDFS, Hadoop Distribted File System) olarak adlandırılmaktadır. Hadoop esas olarak verilerin devasa boyutlara ulaşması nedeniyle, verileri saklamak için geliştirilmiştir. [1,3]. Büyük Veri yapısını yöneterek ağ yapısındaki işleri kolaylaştırmaktadır. Gelişen teknolojilerin ardından veri boyutları oldukça artmaktadır. Artan veri boyutu, verilerin analizini de daha zor hale getirmiştir. Bu durumdan ötürü büyük veriler ile çalışan sistemlerde verilerin hızlı işlenip analiz edilmesi önemli bir problemdir. Büyük verilerin tek makine üzerinde işlenerek analiz etme düşüncesi, analiz süresinin istenen seviyede olmayacağı dönüşünü sağlamaktadır. Süreyi iyileştirmek için yapılan kod düzeltimi veya makinenin donanımsal olarak kuvvetlenmesinin sağlanması adımları işe yaramakla birlikte tam randımanlı bir sonuç vermeyebilir.



Şekil 1. Büyük Veri

Büyük verinin oluşumu açısından 5 temel özellik vurgulanmaktadır. Bunlar sırasıyla çeşitlilik, hız, veri büyüklüğü, doğrulama ve değer olarak belirtilmektedir (Şekil 1). Çeşitlilik (variety) temelde verilerin elde edildikten sonra bir başka veriye dönüştürülebilir olması esasına dayanmaktadır. Veriler çok çeşitli kaynaklardan toplanabilir. Bu çeşitli veriler bütünleşik şekilde kullanılabilir olabilmektedir. Bir diğer özellik olan hız (velocity) gün geçtikçe verilerin inanılmaz boyutlara ulaşması sonucu meydana gelmektedir[4,5]. Bu yapıda büyüyen veri aynı oranda işlem sayısı olarak ortaya çıkmaktadır. Aynı zamanda bilgisayar ağ yapısının bu hızı karşılayabilmesi gerekmektedir. Büyük veride hız kavramı temel aşamada değerlendirilmektedir. Veri büyüklüğü (Volume) veri tabanı sisteminin doğru planlanarak sistem kurulumu esnasında büyüyen veri ile nasıl başa çıkılacağı hesaplanarak elde edilebilmektedir. Doğrulama özelliği (Verification) bu yapının güvenlik tarafını temsil etmektedir. Veri güvenliği olmadığı sürece sistem kullanılamaz ve bütün yapı bozulabilir. İşte bu sürekli sisteme gelen büyük veri izinler ile doğru kişiler tarafından görülebilir olmalıdır[6]. Kurulan yapı itibariyle ortaya çıkan büyük verinin sunucu tarafında saklı kalarak gerekli ağ protokolleri ile yönetilmesi gerekmektedir. Son olarak Değer (Value) bu özellikler arasında öne çıkan kurallardan biridir[4,5,7]. Bilgi işlendikten sonra veri haline gelmektedir. Bu durumda bilginin doğru işlenerek ihtiyaç duyulan veriler elde edilmelidir. Büyük veri kullanılan kurum tarafından gerekli içeriğe sahip olmalıdır[8]. Şekil 1' de büyük veri parçalara ayrılmıştır. 5 temel özellik belirli bir çerçeve içerisinde ifade edilmiştir

3. VoIP Teknolojisi

IP protokolü kullanarak ses iletimi sağlayan teknoloji Voice Over IP (VoIP) olarak isimlendirilmektedir. VoIP mantığında ses telefon sistemleri ile değil internet üzerinden taşınmaktadır (Şekil 2). İletim esnasında bağlantının uçları VoIP telefonları, bilgisayarlar veya IP ağından oluşmaktadır. Bu birimler bloklardan meydana gelen bağlantı ucunu ifade etmektedir. Bloklar ise kodlayıcı, çözücü ve vocoderi içermektedir. Bu sayede ses analogtan sayısala; ardından sayısaldan analoğa dönüşüm işlemi ile kodlanmış sesin sıkıştırılma işlemi de sağlanmış olmaktadır.

Ağ arayüzü kartının sahip olduğu protokoller vasıtası ile elde edilen veri paketlere bölünür [9]. Bunun yanında sinyalleme ve çağrı işlemleri de ağ arayüzü kartı üzerinden gerçekleştirilmektedir.

Paketlerin bu trafikte iki taraflı olarak iletilmesi ve sonlanmasında ortam görevini IP ağı görmektedir. VoIP teknolojisinde konuşma esnasında bütün hat kesinlikle tek duruma tahsis edilmez. Eğer konuşma esnasında veri akımı yok ise boş kalan hat başka bir durum için yönlendirilir. Bu sayede sistemin verimliği arttırılmış olmakla birlikte büyük tasarruf sağlanmış olmaktadır.

VoIP teknolojilerinde tıpkı telefon sistemleri gibi iki protokol kullanılmaktadır. Bu protokoller sinyalleşme ve medya iletişim protokolleridir. SIP(Session Initation Protocol) ve H.323 protokolleri sinyalleşme için; RTP (Real Time Transport) protokolü medya iletişimi için kullanılmaktadır.

Şekil 2. VoIP Teknolojisi

3.1. VoIP Protokolleri

Literatürde birçok farklı VoIP protokolü bulunmaktadır. Bunun nedeni farklı nedenlerden ötürü farklı protokol kullanımına ihtiyaç olabilmesidir. Bütün ihtiyaçlar tek bir protokolde düşünülmesi olasılık dahilinde olmakla birlikte kurumlar kendi ihtiyaçlarına göre protokol seçimi yapmayı tercih etmektedirler. Farklı protokollerin ortak çalışması için geliştirilen arayüzlerin varlığı tek protokolde birleşme fikrini zayıflatmaktadır.

3.1.1. Sinyalleşme Protokolleri

IP üzerinden ses iletilmesinde sinyalleşme için kullanılan protokollerdir [10]. SIP (Session Initiation Protocol), H.323, SCCP (Skinny Call Control Protocol) ve MGCP (Media Gateway Control Protocol) en bilinen protokollerdendir.

3.1.1. Veri Aktarma Protokolleri

Veri aktarım için kullanılan başlıca üç protokol RSVP (Kaynak Ayırma Protokolü), RTP (Gerçek Zaman Protokolü) ve RTCP (Gerçek Zaman Kontrol Protokolü) protokolleridir. RSVP kaynak ayırmak için; RTP gerçek zamanlı veri akışı için ve RTCP ise bu protokolün kontrolünü sağlamak amacı ile kullanılmaktadır.

3.2. VoIP Güvenlik Tehditleri

IP için varolan tüm güvenlik riskleri, VoIP için de tehdit unsuru olarak yer almaktadır. Bu tehdit unsurlarının yanında VoIP'e özel riskler de bulunmaktadır. VoIP için tehdit olarak gruplanabilecek riskler aşağıdaki gibidir [12]:

- ✓ Hizmeti engelleme (DoS- Denial of Service)
- ✓ Ortadaki adam saldırısı (Man-in-the-middle attack)
- ✓ Call Hijack
- ✓ Çağrı yönlendirme (Call redirect)
- ✓ Telekulak (Eavesdropping)
- ✓ Yanıltma (Spoofing)
- ✓ Tekrarlama saldırısı (replay)

4. Geleneksel Tedbirler

VoIP için nitelendirilebilecek güvenlik tedbirleri IP dünyası içerisinde VoIP'e özel olmayan diğer riskleri de barındırmaktadır. Bu sebepten ötürü IP ağı için alınması gereken güvenlik tedbirleri, VoIP güvenliği için de sağlanmalıdır.

Bir VoIP ağı için ses, çoklu ortam ve tüm veri paketleri aynı ağ içerisinde bulunmaktadır. Bu sebepten ötürü birbirlerinden etkilenmeleri olasıdır. Dolayısı ile veri iletiminin sağlandığı bir IP ağına yapılan saldırı, tüm ağda bulunan ses verilerine de zarar verecektir. Bu durum, ses ve veri trafiğinin birbirinden ayrılma tedbirini alınması gerekliğini ortaya koymaktadır. Tedbirin alınması için ses trafiğini ayrıştırarak ses ve veri trafiği ayrı LAN üzerinde sağlanması gerekmektedir. ACL (Access list) kullanımı ile ses ve veri VLAN (virtual LAN)ları arasındaki erişim limitlenmelidir.

VoIP ağında bulunan sunuculara istenmeyen kişilerin erişmesini engellemek amacıyla cihazlara telnet erişimi kısıtlanmalıdır.

VoIP ağının güvenliği için güvenlik duvarlarının (firewall) kullanımı önem arz etmektedir. VoIP oturumu oturumun kurulması sırasındaki sinyalleşme ve ses haberleşmesini taşıyan veri iletimi kısımlarından oluşmaktadır. Sinyalleşme kısmında, paketler kullanıcılar ile SIP proxy arasında gidip gelirken ses iletiminde paketler doğrudan uç terminaller (kullanıcılar) arasında iletilir. SIP kullanılan bir sinyalleşme kısmında genelde UDP/TCP 5060 portu kullanılmaktadır ve telekulak gibi saldırılara karşı savunmasızdır [13].

Ses verisinin iletildiği, uç noktalar arasında bulunan bağlantı için de aynı güvenlik açıkları söz konusudur. IP adreslerini gizlemek için IP adresi ve port değişimi sağlayan NAT (network address translation) kullanılabilir. NAT, IP paketlerini üçüncü katmanda değerlendirmektedir. Fakat VoIP protokollerinde IP adresi bilgisi beşinci katmanda gömülü olarak bulunmaktadır. Bu nedenle NAT uygulaması ile uyumsuzluk meydana gelmektedir. Çözüm olarak; VoIP uyumlu NAT cihazları ya da SBC (Session Border Controller) gibi ek bir cihaz kullanılarak uyumsuzluk ortadan kaldırılabilir.

DoS saldırılarına karşı, VoIP ağındaki sunucular için yedekleme mutlaka sağlanmalıdır. Bunun yanında ses ve sinyalleşme paketleri şifrelenmelidir.

4.1. IPSec (IP Security)

IPSec(IP Security), çağrı kurulması ve kontrolu için kullanılan SIP mesajlarının ağ katmanında güvenliğinin sağlanmasında kullanılmaktadır[11]. IPSec, IETF tarafından geliştirilmiş, AH (Authentication Header) ve ESP (Encapsulating Security Payload) protokollerinin bütünleştirilmiş halidir. IPSec üzerinde iki güvenlik kipi bulunmaktadır. Ulaşım kipi üzerinde sadece veri şifrelenmektedir. Tünel kipi ise ulaşım kipine göre daha güvenlidir. Bu kipte ise hem veri hem de paket başlığı şifrelenmektedir.

IPSec kullanımı ile asıllama, mesaj bütünlüğü, tekrarlama saldırısına karşı koruma ve ulaşım kontrolü sağlanabilmektedir. Bununla birlikte ESP kullanımı sayesinde verinin şifrelenmesi ve kişisel gizlilik ek olarak sağlanabilmektedir. IPSec ile SIP mesajlaşmasının güvenliği sağlanması ise paket başlığına ekstra yük getirmektedir.

4.2. TLS (Transport Layer Security)

TLS, RFC 2246'da tanımlanan ve SIP mesajlarının ulaşım katmanında güvenliğinin sağlanması için kullanılan bir protokoldür. TLS, güvenli oturumların kurulmasında önemli bir rol oynamaktadır. SIP oturumunun kurulması için gerekli istemci/sunucu iletişimi, TLS veya SSL bağlantısı kurulması ile sağlanmaktadır.

TLS protokolünde iki katman bulunmaktadır:

- ✓ TLS record protocol-simetrik anahtarlı şifreleme kullanır.
- ✓ TLS handshake protocol-sunucu ve istemci arasında asıllama ve şifreleme algoritmasına, kullanılacak anahtara karar verilmesi.

SIP mesajı üzeründe bulunan https benzeri bir uzantı bulunmaktadır. Bu uzantı TLS kullanır ve SIPS URI uzantısı olarak isimlendirilmektedir. Eğer SIPS URI isteğindeki route uzerinde TLS bağlantısı varsa, istek kabul edilir, aksi halde reddedilir.

TLS, bağlantılı bir ulaşım katmanı protokolünün kullanımını gerektirdiğinden ötürü TCP ile kullanılırken; UDP ile kullanılamaz. TLS'in UDP-tabanlı SIP sinyalleşmesinde kullanılması mümkün değildir [12].

4.3. SRTP (Secure Real-Time Transport Protocol)

Bu bölüme kadar anlatılan güvenlik önlemleri, IP ağı için kullanılmaktadır. SRTP ise VoIP için geliştirilmiş, VoIP'de medya paketlerinin aktarılması için kullanılan bir protokoldür

RTP protokolü medya verilerinin gerçek zamanlı olarak veri iletimi için kullanılan bir protokoldür. SRTP protokolü ise RTP protokolünün güvenliğini arttırmak için kullanılmaktadır. Bu protokol sayesinde RTP protokolü paketlerinde gizlilik, asıllama, tekrarlama saldırılarına karşı güvenlik önlemleri arttılmış olmaktadır. SRTP, RTP protokollerine koruma özelliği eklemesinin yanında şifreleme gibi özellerini tek bir yapı içinde toplayıp yüksek throughput sağlayarak, RTP paketleri için ek yükleri de minimize etmektedir. RTP yığın uygulamasından ve seçilen anahtar yönetim algoritması ile SRTP protokolünün bağımlılığı bulunmamaktadır. SRTP protokollerinde anahtar yönetimi için MIKEY (Multimedia Internet Keying) tercih edilmesinin nedeni bu anahtar yönetim biçiminin SRTP protokolü ile çalışmak için geliştirilmiş olmasıdır. Fakat bu anahtar yönetim biçimini tercih etmek şart değildir.

Bunun yanında SRTP protokolü için asıllama, şifreleme gibi özelliklerin kullanımı zorunlu değildir. SRTP'nin RTP ile karşılaştırıldığında SRTP'nin sağladığı birçok kuvvetli avantaj bulunmaktadır:

- ✓ RTP ve RTCP için payload şifrelenmesi ile sağlanan güvenilirlik
- ✓ Tekrarlama saldırısına karşı koruma ile birlikte, RTP ve RTCP için mesaj bütünlüğünün sağlanması

- ✓ Oturum anahtarlarını periyodik olarak yenilenmesi yeteneği ile belli bir anahtar tarafından üretilmiş şifreli metin miktarını azaltmak
- ✓ Güvenli bir oturum anahtarı üretme algoritması (her iki uçta pseudo-random fonksiyon ile)
- ✓ Unicast ve Multicast RTP uygulamaları için güvenlik

5. Hadoop Üzerinden Önerilen Güvenlik Mimarisi

VoIP tabanlı iletişimin temelinde gerçek zamanlı (real-time) veriler bulunmaktadır. Bu sebeple iletişimin doğru bir şekilde gerçekleşmesi için güvenliğe ilişkin kararların hızlı verilmesi gerekmektedir.

Küçük veya orta ölçekli kurum ve işletmelerde dağıtık ağ yapısı yerine tek bir ağ yapısı ile rahatlıkla sağlanabilmektedir. Ancak büyük ölçekli kurumlar, işletmeler veya VoIP servis sağlayıcılarında ağ yapısı gereği anlık olarak ortaya çıkan veri VoIP paketleri açısından büyük veriyi oluştumaktadır. Buna bağlı olarak kısa sürede işlenmesi gereken büyük veri geleneksel çözüm yolları üzerinden güvenlik sağlanması zorlaşmaktadır. Tam bu noktada bu çalışmada büyük veri teknolojisi olarak Hadoop mimari kullanılarak önerilen yapı ile çözüm sunulmaktadır.

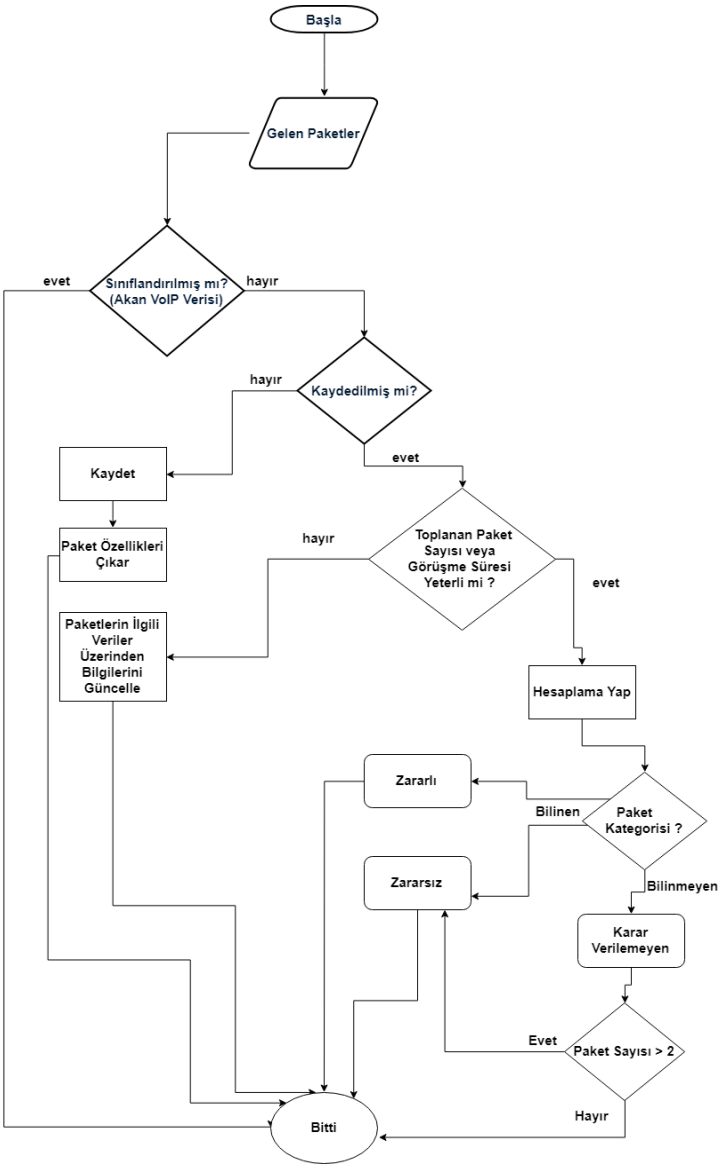
Şekil 3'te çeşitli dağıtık mimariler kullanılarak büyük verinin işlenmesi gösterilmiştir.

Şekil 3. Gerçek Zamanlı VoIP Büyük Verisinin Dağıtık Mimari ile İşlenmesi

VoIP paketlerinin tespiti, önerilen mimaride önemli bir husustur. VoIP güvenlik tedbirlerinin servis sağlayıcılar gibi veri trafiğinin yoğun olduğu sistemlerde uygulanabilmesi sağlanmalıdır. Önerilen algoritmada Gelen VoIP Paketinin Tespit Akış Diyagramı gösterilmektedir. Öncelikle gelen paketin sınıflandırılma durumu kontrol edilmektedir. Eğer paket sınıflandırılmamışsa günlükler incelenir ve eğer günlük kaydı yoksa sisteme bilgi girişi yapılmaktadır. Kaydedilmemiş paketlerin sayısal kontrolü yapılmaktadır.

Bu aşamadan sonra yeterli paket yoksa, yeterli paket sayısı oluşana kadar ilgili veri akışına ilişkin paketler toplanmaya devam etmektedir. Yeterli paket sayısına ulaşılınca, sıradaki adım olan Paketin VoIP yada non-VoIP durumu belirlenir. Karar verilememesi durumunda paket non-VoIP olarak sınıflandırılır. VoIP olarak sınıflandırılan paketlerin sistemde öncelikli olarak işlem görmesi sağlanır. Böylece VoIP güvenlik tedbirleri uygulanmış olacaktır.

Şekil 4'te önerilen güvenlik mimarisinin akış diyagramı gösterilmektedir.



Şekil 4. Gelen VoIP Paketinin Tespit Akış Diyagramı.

6. Sonuç ve Tartışma

VoIP, sistem maliyeti açısından tasarruf sağlayan bir mantık taşıdığından ötürü popüleritesi yüksek olan ancak halen gelişmekte olan bir teknolojidir. Özellikle güvenlik konusu üzerindeki çalışmalar, VoIP teknolojisi içerisinde henüz başlangıç seviyesindedir. Literatüre bakıldığında VoIP konusunda güvenlik açıkları teorik olarak ortaya konmuş gözükmektedir. Bunun yanında ortaya konan güvenlik risklerinin pratiğe aktarılması zordur. Bu durumun nedeni güvenlik açıklarını kullanabilecek saldırganların VoIP teknolojisi üzerindeki uzmanlık düzeyinin düşük olmasının yanında VoIP test ortamının sınırlı olmasıdır. VoIP teknolojisinin kullanırlığı ve bu teknolojiye olan ilgi arttıkça risk daha fazlalaşacak; saldırganlar tarafından daha çekici hale gelecektir. Bunun sonucu olarak ilgili teknolojiye ait güvenlik risklerinin ve saldırı türlerinin de çoğalacağı öngörülmektedir. VoIP alanında yapılan çalışmaların birçoğu VoIP'ye özelleştirilmemiş; IP güvenliği üzerine kullanılmakta olan yöntemlerdir. Bu çalışmalar dışında VoIP üzerinde sinyalleşme ile birlikte medya paketlerinin güvenliğinin sağlanması adına çalışmalar da mevcuttur.

Büyük veri teknolojisi olan Hadoop mimarisinin dağıtık ağ yapısı üzerinden hızlı veri işleme ile güvenliği ön plana çıkartabilecek bir sisteme sahiptir. Hadoop mimarisinin doğru planlandığında ağ güvenliğine katkısı birden çoktur. Veriler üzerinde ağı izole etmesi, bulut teknolojisini kullanması, senkron ve kopyalama mimarisine sahip olması ve yedekli çalışması başlıca güvenlik destekleyici sebeplerdir.

Bu çalışmada önerilen güvenlik mimarisi sayesinde gelen paket sınıflandırılarak öncelikli işlem yapılması sağlanacak; non-VoIP olarak sınıflandırılması yapılan paketler ise işleme alınmayacaktır. Bu sayede VoIP'e özelleştirilmiş bir güvenlik tedbiri uygulanmış olacaktır.

Kaynakça

[1] Storey, V. C., & Song, I. Y. (2017). Big data technologies and management: What conceptual modeling can do. Data & Knowledge Engineering, 108, 50-67.
[2] Ge, M., Bangui, H., & Buhnova, B. (2018). Big Data for Internet of Things: A Survey. Future Generation Computer Systems.
[3] Castiglione, A., Colace, F., Moscato, V., & Palmieri, F. (2018). CHIS: A big data infrastructure to manage digital cultural items. Future Generation Computer Systems, 86, 1134-1145.
[4] Canito, J., Ramos, P., Moro, S., & Rita, P. (2018). Unfolding the relations between companies and technologies under the Big Data umbrella. Computers in Industry, 99, 1-8.
[5] Khan, S., Liu, X., Shakil, K. A., & Alam, M. (2017). A survey on scholarly data: From big data perspective. Information Processing & Management, 53(4), 923-944.
[6] Oussous, A., Benjelloun, F. Z., Lahcen, A. A., & Belfkih, S. (2017). Big Data technologies: A survey. Journal of King Saud University-Computer and Information Sciences.
[7] Shadroo, S., & Rahmani, A. M. (2018). Systematic survey of big data and data mining in internet of things. Computer Networks, 139, 19-47.
[8] Rani, S., Ahmed, S. H., Talwar, R., & Malhotra, J. (2017). Can Sensors Collect Big Data? An Energy-Efficient Big Data Gathering Algorithm for a WSN. IEEE Transactions on Industrial Informatics, 13(4), 1961-1968.
[9] Gökşen, Y., & Hakan, A. Ş. A. N. (2015). Veri Büyüklüklerinin Veritabanı Yönetim Sistemlerinde Meydana Getirdiği Değişim: NOSQL. Bilişim Teknolojileri Dergisi, 8(3), 125.
[10] Zheng, Y. (2015). Methodologies for Cross-Domain Data Fusion: An Overview. IEEE Trans. Big Data, 1(1), 16-34.
[11] Dexi, W., Jiang,Y., Song, H. Verification of implementations of cryptographic hash functions. IEEE Access, 2017, p:7816 - 7825.
[12] Yavaş, S., Orencik, B., "VoIP Güvenliği", İTÜ Bilgisayar Bilimleri Ders Notları
[13] Advantages and Disadvantages of Asymmetric and Symmetric Cryptosystems. [cited 2017 29 Dec]; Avaliable from: http://www.uobabylon.edu.iq/eprints/paper_1_2264_649.pdf