T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

ARAŞTIRMA ve İNCELEME

30.KONU : KRİPTOGRAFİ VE BİLGİ GÜVENLİĞİ

BİL 473 AĞ VE BİLGİ GÜVENLİĞİ
DÖNEM ÖDEVİ/PROJESİ RAPORU

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2021

1.AÇIKLAMA

Bu kısımda, çalışma ile ilgili, çalışmanın raporlanması ve sunulması ile ilgili gerekli bilgiler açıklanmıştır.

1.1. Çalışma Bilgileri :

- Bu ödev/proje, Prof. Dr. İbrahim SOĞUKPINAR tarafından, BİL 473 kodlu Ağ ve Bilgi Güvenliği dersi kapsamında, bölüm öğrencilerine, dönem ödevi/projesi olarak verilmiştir.
- Proje kapsamında öğrenciler, ders hocası tarafından listelenen konular içerisinden seçecekleri bir konu hakkında araştırma ve inceleme yapmalı, yaptıkları bu çalışmanın sonuçlarını istenen formatta raporlamalı ve yapılan çalışmayı özetleyen bir sunum yapmalıdır.
- Bu çalışma için belirlenen konu başlığı "Kriptografi ve Bilgi Güvenliği"dir. Bu konu araştırılıp incelenecektir, sonuçları raporlanacaktır, sunumu yapılacaktır.

1.2. Proje Raporu Bilgileri :

- Hazırlanan rapor, .doc/.docx dosya formatında, 4 Haziran 2021 gününe kadar, ders ilgili hocasına, e-posta ile gönderilecektir.

1.3. Proje Sunumu Bilgileri :

- Hazırlanan sunum, .ppt/pptx formatında olmalıdır, 1 Haziran 2021 günü, ders takviminin son haftasında, çevrimiçi ders ortamında, ders hocasına ve dersi alan diğer öğrencilere, sunulmalıdır.

2.ÖN HAZIRLIK

Bu kısımda, çalışmaya başlamadan önce yapılan ön hazırlık aşamalarından bahsedilecektir.

Konunun Seçilme Sebebi

Önceki bölümde de belirtildiği gibi, bu çalışma için seçilen konu başlığı "Kriptografi ve Bilgi Güvenliği"dir. Bu konunun seçilmesinin temel olarak iki sebebi vardır, ilki, ilk dönem "Kriptografi ve Bilgisayar Güvenliği" dersini almış, BA harf notu ile dersi tamamlamış, gerekli altyapıya kısmen de olsa sahip olduğumu düşünüyor olmamdır. Bu konuyu seçmemde temel oluşturan ikinci sebep ise, bu konuların ülkemizde özellikle son yıllarda ön planda olmasıdır.

Konunun Önemi ve Gerekliliği

Gelişen dijitalleşme çağına ülkemiz hızlıca uyum sağlamış, hatta e-devlet uygulamasına geçen ülkeler arasında ilk sıralarda yer almıştır, ancak bu durum beraberinde ülkemiz için veri güvenliği konusunu getirmiştir. Ayrıca pandemi süreci ile birçok özel/resmi kurumlar/kuruluşlar çevrimiçi çalışma düzenine geçmiştir, ancak açıkça görülmektedirki vatandaşlarımız, çalışma düzenine ayak uydursalar bile, veri güvenliği konusunda yeterli bilgiye sahip değildir. Dolayısıyla bu konuların üzerinde durulması gerekmektedir.

Konu Hakkında Bilinmesi Gereken Bazı Kavramlar

Konunun araştırılması ve incelenmesinden önce, konu ile ilgili bazı kavramların tanımlarının yapılması gerekmektedir.

Bilgi, Veri, Varlık, Ağ, Bilgisayar, Güvenlik

Bilgi : Bilgi, verinin belli bir anlam ifade edecek şekilde düzenlenmiş halidir. (Gürol CANBEK, Şeref SAĞIROĞLU, 2006)

Veri : Bilişim teknolojisi açısından veri, bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca, sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleri olarak tanımlanabilir. (Gürol CANBEK, Şeref SAĞIROĞLU, 2006)

Varlık : Varlık, felsefenin temel kavramlarından birisidir. Var olan ya da var olduğu söylenen şey, varlık kavramının içeriğini oluşturur. (Varlık, 2021)

Ağ : Bilgisayar ağı, küçük bir alan içerisindeki veya uzak mesafelerdeki bilgisayarların ve/veya iletişim cihazını iletişim hatları aracılığıyla birbirine bağlandığı, dolayısıyla bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaşıldığı, bir yerden başka bir yere veri aktarımının mümkün olduğu iletişim sistemidir. (Bilgisayar Ağı, 2021)

Bilgisayar : Bilgisayar, kendisine programlama yoluyla komuta edilmiş bir dizi aritmetik ya da mantık işlemini otomatik olarak yapabilen bir makinedir. (Bilgisayar, 2021) Kişisel bilgisayar, şahsi kullanımına yönelik özel olarak tasarlanmış, herhangi bir uzman veya operatörün yardımı olmadan kişilerin kendi başlarına kullanabileceği bilgisayar türüdür. (Kişisel Bilgisayar, 2021)

Güvenlik : Bilgi güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma, veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemidir. (Bilgi Güvenliği, 2021)

Bilgi Güvenliği, Veri Güvenliği, Ağ Güvenliği, Bilgisayar Güvenliği

Bu kavramlar sıklıkla birbirlerinin yerine kullanılmaktadır. Çoğu durumda, gerçekleştirilen güvenlik işlemleri tüm bu kavramlar için geçerli olsa da, bazı durumlarda ilgili kavrama özgü güvenlik işlemleri de mevcuttur.

Şifreleme, Deşifreleme, Anahtar

Şifreleme : Açık metni bir şifreleyici ve bir anahtar kullanarak şifreli metne dönüştürme sürecine denir. (SOĞUKPINAR, 2017)

Deşifreleme : Şifreli metni bir şifreleyici ve bir anahtar kullanarak açık metne dönüştürme sürecine denir. (SOĞUKPINAR, 2017)

Anahtar : Sadece gönderici ve alıcının bildiği şifreleyici tarafından kullanılan kritik bilgilere denir. (SOĞUKPINAR, 2017)

Simetrik Şifreleme, Asimetrik Şifreleme, Açık Anahtar, Gizli Anahtar

Gönderici ve alıcı aynı anahtarı kullanırsa buna **simetrik** (tek anahtarlı, **gizli anahtar**lı, veya geleneksel) **şifreleme**, eğer gönderici ve alıcının her biri farklı anahtar kullanırsa buna **asimetrik** (iki anahtarlı, veya **açık anahtar**lı) **şifreleme** denir. (SOĞUKPINAR, 2017)

Kriptolama, Kriptoloji, Kriptografi, Kriptanaliz

Kriptolama : Bilgisayar ağlarının ve haberleşme sistemlerinin güvenliğinin sağlanması için kullanılan en önemli işlem, verilerin şifrelenerek anlamsız hale getirilip hedefe gönderilmesi ve hedefte tersi işlem yapılarak tekrar eski hale getirilmesidir. (SOĞUKPINAR, 2017)

Kriptoloji : Kriptoloji, latince gizli anlamına gelen *kryptos* ve yine latince sözcük anlamına gelen *logos* kelimelerinin birleşiminden oluşan gizli ve güvenli haberleşme bilimidir. Kriptoloji temelde iki kısımda incelenir; bunların birincisi kritik bilgilerin yetkisiz kişi ve/veya kurumlardan korunması amacıyla geri dönüşümü mümkün olarak anlaşılmaz hale getirilmesi yani şifrelenmesi için kripto sistemlerinin tasarlanması demek olan **kriptografi** bilimidir. İkinci kısım ise kodlanmış veya şifrelenmiş olan gizli bilgilerin bulunmasına yönelik çalışmaların yapılması demek olan **kriptanaliz** bilimidir. (SOĞUKPINAR, 2017)

Konunun Araştırılma ve İnceleme Süreci

Çalışmamı yaparken, belirtildiği gibi, son 5-10 yıl içerisinde yayınlanan makalelere yöneldim. Ön hazırlığımı sağlarken, ülkemizde 2006 yılında yapılmaya başlanan, ardından uluslararası nitelik kazanan, tam da kendi konum ile ilgilenen "Bilgi Güvenliği ve Kriptoloji Konferansı"na denk geldim. Makaleler için dergi veya konferans şeklinde bir sınırlama olmadığı için bu konferansta bildirilen makaleleri kullanabileceğimi düşündüm. Ayrıca ders hocamız Sayın Prof. Dr. İbrahim SOĞUKPINAR'ın da konferansta Bilim Kurulu Üyesi olması, konferansta yayınlanan makalelere yönelmemdeki en büyük etkendir, buradan hocamıza saygı ve teşekkürlerimi iletiyorum.

Faydalanılan Kaynaklar

Makale araştırırken elbette Google Scholar, DergiPark, IEEE, BiblioTex, Publons, ORCID, ResearchGate gibi kaynaklardan da yararlandım. Ancak ülkemizde düzenlenmiş olması, ülkemiz ile ilgili güncel konuları da ele almış olması, ve bunun gibi sebeplerle daha çok bahsettiğim konferansta yayınlanan makalelere yöneldim. Konferansın ilgili resmi websitesi incelendiğinde, çok kullanışlı bir arayüz ile karşılaşılmaktadır. İlk olarak websitesi üzerinden önceki senelerde yapılan konferanslara, burada yapılan bildirilere ve sonuç bildirilerine ulaştım. Elimden geldiğince her sene yapılan konferansı, konferans konusunu, konferans bildirilerini ve sonuç bildirilerini okumaya çalıştım. Çoğu senenin kaynaklarına ulaşamadım, ulaştıklarımdan bazıları ise kullanılabilir değildi, mümkün olduğunca buldum ve inceledim.

Konuyla İlgili Makalelerin Seçim Süreci

Konferansta, her sene belirli konular seçilmektedir ve daha çok o konulara yönelmişlerdir. Bu konular tamamen bilgi güvenliğini ve kriptolojiyi ilgilendiren temel konulardır. Bilgi güvenliği doğası gereği çok geniş kapsamlı bir konudur. Örneğin ağ güvenliği, ipv6, siber güvenlik, telsiz ağlarda güvenlik, protokoller, kriptografik protokoller, kriptoloji, kriptografi, kriptanaliz, kullanılabilir güvenlik, stenografi, kuantum kriptografi, kişisel bilgi güvenliği, kurumsal bilgi güvenliği, bilgisayar güvenliği, güvenlik farkındalığı, veri mahremiyeti ve benzeri konular bunlardan sadece bazılarıdır.

Başlangıçta her makalemi farklı bir alandan seçmeyi, sonuç kısmında hepsini tek bir konuya bağlayarak konumu özetlemeyi düşündüm. Ancak bu şekilde ilerlemeye çalıştığımda, ödevin/projenin amacından saptığımı farkettim. Ardından kendime bu kapsamda bir alt alan belirlemeye ve makaleleri de bu alana göre seçmeye karar verdim. Başlangıçta alt alan olarak, günümüzde de önem arz etmesi sebebiyle, "Kişisel/Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Yönetimi" konularını seçtim. Ancak bu kez de, tek bir konuya çok fazla yöneldiğimi farkettim.

Makalelerin Konuları

Sonuç olarak, alt alan konumu ("Kriptolojiinin Bilgi Güvenliği Konusundaki Yeri ve Önemi") "Bilgi Güvenliği Farkındalığı" şeklinde belirledim, ve bu konuları ilgilendiren makalelere yöneldim.

Özetle araştırdığım ve incelediğim, ve bu raporun da konusunu oluşturan makaleler,

- genel olarak bilgi güvenliği ve kriptolojiinin ne olduğunu,
- önem ve kapsamlarını,
- günümüzde bu konuların yerini,
- geçmişten günümüze bu konularda yapılmış çalışmaları,
- konuyla ilgili güncel çalışmaları,
- bilgi güvenliği konusunda alınabilecek önlemleri,
- kriptolojiinin bilgi güvenliği konusundaki önemini

konu alan makalelerdir.

Ön Hazırlıkta İncelenen Makaleler

Konuya ön hazırlık olarak incelediğim makaleler aşağıdaki gibidir :

1. M. Tekerek , "Bilgi Güvenliği Yönetimi", KSÜ Doğa Bilimleri Dergisi, c. 11, sayı. 1, ss. 132-137, Haz. 2008 (TEKEREK, Bilgi Güvenliği Yönetimi, 2008)
2. C. Öztürk, M. Tekerek, A.S. Yılmaz, "Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması", 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Eki. 2016 (Cumali ÖZTÜRK, Mehmet TEKEREK, Ahmet Serdar YILMAZ, 2016)
3. Y. Vural, M. Aydos, M. Tekerek, A.S. Yılmaz, "Akıllı Şebekeler Veri Mahremiyetine Yönelik Tehditler", Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Eki. 2016 (Yılmaz VURAL, Murat AYDOS, Mehmet TEKEREK, Ahmet Serdar YILMAZ, 2016)
4. G. Canbek ve Ş. Sağıroğlu , "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, c. 9, sayı. 3, ss. 165-174, Eyl. 2006 (Gürol CANBEK, Şeref SAĞIROĞLU, 2006)
5. M. Eminağaoğlu ve Y. Gökşen, "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, c. 11, sayı. 4, ss. 01-15, 2009 (Mete EMİNAĞAOĞLU, Yılmaz GÖKŞEN, 2009)
6. Henkoğlu, T , Yılmaz, B. (2013). Avrupa Birliği AB Bilgi Güvenliği Politikaları. Türk Kütüphaneciliği, 27 (3) , 451-471 . (Türkay HENKOĞLU, Bülent YILMAZ, 2013)
7. M. Güngör, "Ulusal Bilgi Güvenliği : Strateji ve Kurumsal Yapılanma" (Uzmanlık Tezi), T.C. Kalkınma Bakanlığı, Yayın No:2919, Bilgi Toplumu Dairesi Başkanlığı, Mar. 2015 (GÜNGÖR, 2015)
8. A. Bektaş, "Bilgi Güvenliği ve Kriptografi", SPK'da Geçen Ay Dergisi, Oca. 2006 (BEKTAŞ, 2016)
9. T. Henkoğlu , "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme", Arşiv Dünyası, no. 18-19, pp. 36-47, Ara. 2017 (HENKOĞLU, 2017)
10. Y. Vural ve Ş. Sağıroğlu, "Ülke Bilgi Güvenliği", 3.Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ara. 2008 (Yılmaz VURAL, Şeref SAĞIROĞLU, 2008)
11. U. Yavanoğlu , Ş. Sağıroğlu ve İ. Çolak , "Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler", Politeknik Dergisi, c. 15, sayı. 1, ss. 15-27, Mar. 2012 (Uraz YAVANOĞLU, Şeref SAĞIROĞLU, İlhami ÇOLAK, 2012)

Seçilen Makaleler

Seçip incelediğim belirli başlı bazı makaleler aşağıdaki gibidir :

Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2012-2019

1. "İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği" (TEKEREK, İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği, 2012)
2. "Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği" (Mustafa ALKAN, Mustafa ÜNVER, Hakan TEKEDERE, 2012)
3. "Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala" (Osman AKIN, Işıl ÇINAR, Muhammer KARAMAN, Fatih BİLEKYİĞİT, 2013)
4. "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri" (Seda YILMAZ, Şeref SAĞIROĞLU, 2013)
5. "Siber Güvenlik Konusunda Kurumsal Farkındalık Ve Entegre Çözüm Alt Yapısı" (DİNÇER, 2013)
6. "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri" (G ŞENGÜL, F.K. ATSAN, A. BOSTAN, 2014)
7. "Sosyal Ağlarda Güvenlik Farkındalığının Arttırılması" (YILDIRIM, 2015)
8. "Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme" (Salih Erdem EROL, Eyüp Burak CEYHAN, Şeref SAĞIROĞLU, 2015)
9. "Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması" (Cumali ÖZTÜRK, Mehmet TEKEREK, Ahmet Serdar YILMAZ, 2016)
10. "Akıllı Şebekeler: Veri Mahremiyetine Yönelik Tehditler" (Yılmaz VURAL, Murat AYDOS, Mehmet TEKEREK, Ahmet Serdar YILMAZ, 2016)
11. "Siber Güvenlikte Kamu ve Özel Sektör İşbirliği" (Gülcihan AYDANER, Ufuk ÇELİK, Senem NART, 2017)
12. "Kurumsal Bilgi Güvenliği Üzerinde Yeni Kayıtlı İnternet Sitelerinin Etkisinin Analiz Edilmesi" (Samet GANAL, Mehmet A. YALÇINKAYA, Ecir U. KÜÇÜKSİLLE, 2017)
13. "Medikal Verilerin Blok Zinciri Mimarisiyle Güvenliğinin Sağlanması" (KASIM, 2018)
14. "Büyük Genomik Verilerde Mahremiyet" (Enes CANBAZ, M. Emir ÇAKICI, Yılmaz VURAL, Yavuz CANBAY, 2018)
15. "Büyük Genomik Verisinin Mahremiyetinin Korunarak İşlenmesi" (Arian AJDARİ, Zeynep FENERCİ, Yılmaz VURAL, Yavuz CANBAY, 2018)
16. "Bilgi Güvenliği Bağlamında Yeni Teknolojik Devrim: Kuantum Teknolojiler" (YILMAZ, 2018)
17. "Kuantum Dijital İmza Teknolojilerini Kullanarak Kuantum Elektronik İmza Geliştirmek" (Cumali YAŞAR, İhsan YILMAZ, 2019)
18. "Hassas Verilerin Korunmasında Klasik ve Kuantum Kriptoloji Yöntemleri Üzerine Bir Araştırma" Ömer KASIM, Esmanur COŞKUN (Ömer KASIM, Esmanur COŞKUN, 2019)
19. "Kuantum Kriptanalizin Siber Güvenlikteki Yeri" Muharrem Tuncay GENÇOĞLU (GENÇOĞLU, 2019)

Seçilen Makalelerden En Popüler 4 Tanesi

Bunların içerisinden seçtiğim en popüler 4 makale aşağıdaki gibidir :

1. "Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme" (HENKOĞLU, 2017)
2. "Bilgi Güvenliği Bağlamında Yeni Teknolojik Devrim: Kuantum Teknolojiler" (YILMAZ, 2018)
3. "Medikal Verilerin Blok Zinciri Mimarisiyle Güvenliğinin Sağlanması" (KASIM, 2018)
4. "Büyük Genomik Verilerde Mahremiyet" (Enes CANBAZ, M. Emir ÇAKICI, Yılmaz VURAL, Yavuz CANBAY, 2018)

3.RAPOR

1.Giriş

Gelişen teknoloji çağı ve teknolojiye olan bağımlılık, her geçen gün artmaktadır. Artan bu gelişmeler, beraberinde sosyal, psikolojik vb. problemlerin yanısıra, bilgi ve haber güvenliği problemlerini de getirmiştir.

Her problemde olduğu gibi, bilgi güvenliği probleminin çözümünün de ilk adımı, bilgi güvenliği farkındalığıdır. Özel hayatımızda bir birey olarak, iş hayatımızda bir çalışan olarak ve ulusal anlamda bir vatandaş olarak, her alanda bilinçli bir kullanıcı olmalıyız. Korunması gereken varlıklarımızın ve kişisel verilerimiz üzerindeki haklarımızın bilincinde olmalıyız.

Teknolojik ortamlarda verilerimizin gizliliğini korumak için alınabilecek önlemleri 2 başlık altında toplayabiliriz :

1. **Kriptografi :** Bilginin/haberin gönderen tarafında özel bir program ile şifrelenmesi ve alıcının da aynı programı kullanarak şifreyi çözmesi
2. **Stenografi :** Gönderilecek bilginin/haberin bir ses ya da görüntü kaydının içine şifrelenerek yerleştirilmesi ve alıcı tarafında şifrenin çözülerek bilgiye/habere ulaşılması (BEKTAŞ, 2016)

Etrafımızda belirli tehditler ve bu tehditleri bize karşı kullanabilecek saldırganlar vardır. Bunların farkında olmalı, kendi güvenlik önlemlerimizi önce kendimiz almalıyız. Veriyi korumak için kullandığımız yöntemler, aşağıda belirtilenleri sağlamalıdır :

- **Gizliliği sağlamalı,** başkaları tarafından anlaşılmamalı,
- **Bütünlüğü sağlamalı,** karşı tarafa gönderilen verinin değiştirilip değiştirilmediği bilgisini bize vermeli,
- **Reddedilemez olmalı,** gönderici veriyi kendisinin gönderdiğini inkar edememeli,
- **Kimliği doğrulamalı,** gönderici veya alıcı, birbirleriyle haberleştiklerinden emin olmalı.

Kısacası, kullanıcıların bilgi güvenliği farkındalığı oluşmalı, kullanıcılar korunması gereken varlıklarından haberdar olmalı, kişisel verilerimiz üzerindeki haklarımızın bilincinde olmalı, ve gerekli güvenlik önlemlerimizi almalıyız. Bu kapsamda kriptoloji bilimi her geçen gün gelişmekte, ve gelişen teknolojiye göre şekil almaktadır.

2.Teorik Açıklama ve Yapılan Diğer Çalışmalar

Bilgi güvenliği ve kriptoloji, birbiriyle ilişkili, birbirini tamamlayan, birbirini geliştiren iki temel konudur. Bu kapsamda akademik çalışmalar yapılmaktadır, kurumlarda veri gizliliği ve verileri koruma eğitimleri verilmektedir, ülkeler ise siber güvenlik alanında birçok ilerleme katetmiştir. Bilgi güvenliğinin farkında olunduğunda, korunması gereken birçok varlığın olduğu gözlenir. Bunun bir getirisi olarak, kriptoloji alanı hızla gelişmektedir.

Kriptoloji konusunun temelleri, çok eskilere dayanmaktadır. Daha önceleri verinin fiziksel anlamda korunması beklenirdi, böylece insanlar korumak istedikleri varlıklarını yer altına gömerek, kilitli sandıklara saklayarak, veya iletmek istedikleri mesajları türlü şekillerde muhafaza ederlerdi. Zamanla veriyi fiziksel olarak korumanın yerine, şifreleyerek korumak, böylece fiziksel olarak ulaşılsa bile anlaşılmaz hale getirmek amaçlanmıştır. Özellikle iletilmek istenen mesajların gizlenmesi üzerine yoğunlaşılmıştır.

Mesajları şifrelemek için, harflerin yerlerini değiştirme, harflerin yerine farklı harfler koyma, bunları birbirine karıştırma ve belirli sayılarda bu işlemleri tekrarlama gibi yöntemler uygulanmıştır. Doğası gereği kriptoloji bilimi, sağlam bir matematiksel altyapıya da dayanmaktadır. Gelişen teknoloji beraberinde çok güçlü matematiksel problemlere çözüm getirdiği gibi, kriptolojinin de gelişimini hızlandırmıştır. Bu alanda gelinen son nokta, kuantum teknolojisidir ve bu teknolojiyi kullanarak gerçekleştirilen kuantum kriptografisidir.

3.Popüler Çalışmaların Teorik Detayları ve Karşılaştırmaları

Çalışmamda, proje konum gereği, belirli bir yöntem veya metoddan söz etmek mümkün değildir, dolayısıyla raporumda buraya kadar, bilgi güvenliği ve kriptoloji konularını anlatmaya çalıştım. “Bilgi güvenliği ve kriptoloji kavramlarının tanımı nedir? Bu konuları ilgilendiren diğer temel terimler nelerdir? Bilgi güvenliği farkındalığı nedir? Korunması gereken varlıklar nelerdir? Kişisel verilerimiz üzerindeki haklarımız nelerdir, ve niçin korunmaya ihtiyaç duyarız? Korunması gereken varlıklarımızı, hangi yöntemlerle koruyabiliriz? Verilerimiz hangi tehditlerle karşı karşıyadır? Kriptolojinin tarihi nedir, temeli nereye dayanmaktadır, ve kriptolojideki son ilerlemeler nelerdir?” gibi soruların yanıtlarına genel anlamda değindim. Şimdi ise, proje konumu, konumla ilgili belirli konularda özelleştirip, önemli olduğunu düşündüğüm 4 makaleyi referans alarak, yapılan güncel çalışmalardan bahsedeceğim.

Makale 1

Tür	Dergi Makalesi
Yazar	Türkay HENKOĞLU
Başlık	Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme
Yayınlandığı Yer	Arşiv Dünyası Dergisi
Sayı	17-18
Sayfa	46-56
Yıl	2017

Özet

Bu makalede özetle, bilgi kavramının artık değiştiğinden, dolayısıyla bilgi güvenliği kavramının da anlamının değiştiğinden, kazandığı yeni anlama göre bilgi güvenliği kapsamının ve alınan önlemlerin ona göre tekrar düzenlenmesi gerektiğinden bahsedilmektedir. Kişisel verileri koruma kanununa, ekonomik açıdan ileride olan ülkelerin kanunlarının yön belirlediğine, bizim hem bilgi güvenliğinin güncel anlamına, hem kendi ülke şartlarımıza göre kanunlarımızı düzenlememiz gerektiğine değinilmiştir. Kişilerin bilgi güvenliği farkındalığının olmadığı, ve gerekli kişilerin gerekli sorumlulukları almadığı söylenmiştir. Bilgi güvenliği konusunda temel unsurlar nelerdir, sorunlar ve alınması gereken önlemler nelerdir, bu soruların yanıtları verilmiştir.

Yapılan Çalışmalar

Bu makalede yapılan çalışmalar, daha çok inceleme niteliğindedir. Bilgi güvenliği farkındalık dereceleri gözlemlenmiş, kişilerin aldığı ve almadığı sorumluluklar incelenmiştir. Mevcut anlayış göz önüne alınmış, yeterli olup olmadığı değerlendirilmiştir. Mevcut anlayışın günümüzde geçersiz olduğu, kişilerin farkındalığının yeterli düzeyde olmadığı, ilgili kişilerin gereken sorumluluğu almadığı ortaya koyulmuştur.

Sonuç

Bu makalede sonuç olarak, kişisel verilerin korunması kapsamında, hukuksal süreçleri de göz önünde bulundurarak, alınması gereken önlemler listelenmiştir.

Makale 2

Tür	Konferans Bildirisi
Yazar	İhsan YILMAZ
Başlık	Bilgi Güvenliği Bağlamında Yeni Teknolojik Devrim: Kuantum Teknolojiler
Yayınlandığı Yer	Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı
Sayfa	32-39
Yıl	2018

Özet

Bu makalede özetle, dünyada gelişen kuantum teknolojileri ele alınmıştır, gelişmeleri kaçırmamak adına yapılması gerekenlerden bahsedilmiştir.

Yapılan Çalışmalar

Bu makalede yapılan çalışmalar, tamamen kuantum teknolojiler üzerinedir. Kuantum teknoloji devriminin dayandığı temeller, diğer teknolojilere karşı olan üstünlüğü ele alınmıştır. Kuantum teknolojisinin kullanıldığı alanlar ele alınmış, bu alanlarda geliştirilen araçlar ve cihazlar listelenmiştir. Kuantum bilgi ve iletişimde, geliştirilen bilgisayar ve çipler, programlama dilleri, işletim sistemleri ve derleyiciler, kriptografik algoritmalar, bilgi iletişim cihazları, algoritmalar, internet; kuantum detektörlerde, geliştirilen radarlar, görüntüleme cihazları, sensörler listelenmiştir. Ayrıca uzay araştırmalarında kuantum teknolojilerin yerinden söz edilmiştir.

Sonuç

Bu makalede sonuç olarak, kuantum teknolojinin üstünlüğü ortaya konmuş, ve çağı yakalamamız için ulusal anlamda yapmamız gerekenler listelenmiştir. Kuantum teknolojilerin gelişimi üzerine öneriler verilmiştir.

Makale 3

Tür	Konferans Bildirisi
Yazar	Ömer KASIM
Başlık	Medikal Verilerin Blok Zinciri Mimarisiyle Güvenliğinin Sağlanması
Yayınlandığı Yer	Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı
Sayfa	1-5
Yıl	2018

Özet

Bu makalede özetle, artan kişisel verilerden, bu verilerin içinde medikal verilerin de var olduğundan, medikal verilerin gizli kalması gerektiğinden, dolayısıyla bunların nasıl ve nerede saklanması gerektiğinden bahsedilmiştir. Ayrıca, bir çözüm olarak, medikal verilerin blok zinciri mimarisiyle saklanarak, güvenliğinin sağlanabileceğinden bahsedilmiştir.

Yapılan Çalışmalar

Bu makalede yapılan çalışmalar, medikal verilerin bulut depolama alanında güvenli bir şekilde saklanması ile ilgilidir. Sistemde veriler bulut depolama üzerinde saklanır. Saklanan veriler hastanın kişisel bilgileri, hastanın medikal bilgileri, verilerin kaydedildiği zaman damgası ve işlenen zincir sayısıdır. Bu verilere erişim, farklı kullanıcı rolleri ile sınırlanmıştır. Veriler belirli bir blok zinciri algoritmasına tabii tutulur ve bulutta bu şekilde saklanır. Şifreleme ile alınan güvenlik önlemine ek, kaydın eklendiği zaman damgası verisinin tutulması ve erişimin farklı kullanıcı rolleri ile sınırlandırılması sayesinde, güvenlik seviyesi arttırılmış olur. Ayrıca şifreleme algoritması, her yeni bloğun bir önceki blok bilgileri ile oluşturulması temeline dayandığı için, önceki verilere sahip olmadan yeni kayıt atılamaz, böylece güvenlik seviyesi yine arttırılmış olur. Tüm bunlara ek, herhangi bir kullanıcı, zincirdeki bloklardan daha fazlasını ekleyecek olursa, mimarinin yapısı gereği bu kullanıcının zincire sahip olma olasılığı vardır. Yeni blok ekleme işlemini belirli bir algoritmaya bağlayarak, bunun da önüne geçilmiş olur. Blok ekleme işlemi gerekli yapıya sahip olmadıkça gerçekleşmeyeceği için, dışarıdan bir kullanıcının zincire sahip olması engellenmiş olur. Geliştirilen bu sistem ile, bir hastanın medikal verilerinin bulut depolama alanında güvenli bir şekilde saklanması mümkün kılınmış olur.

Sonuç

Bu makalede sonuç olarak, kişilerin medikal verilerinin güvenli bir şekilde saklanması sağlanmıştır. Tahlil ve tedavi sonucunda girilen veriler, metin dosyasından bulut ortamına aktarılır. Hastanın verileri bulut ortamında blok zinciri mimarisi ile şifrelenerek saklanır, dolayısıyla direk erişim mümkün değildir. Herhangi bir kullanıcının verilere ulaşabilmesi için, yetkili olması gerekmektedir, yetkisi olan kişiler de yalnızca yetkili olduğu verilere ulaşabilir. Ayrıca hasta farklı bir hastahaneye gittiğinde, yine verileri bulut ortamından güvenli bir şekilde alınır, böylece medikal verilerin diğer hastahanelere veya farklı yerlere açık bir şekilde taşınmasının önüne geçilmiş olur.

Makale 4

Tür	Konferans Bildirisi
Yazar	Arian AJDARİ, Zeynep FENERCİ, Yılmaz VURAL, Yavuz CANBAY
Başlık	Büyük Genomik Verilerde Mahremiyet
Yayınlandığı Yer	Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı
Sayfa	19-25
Yıl	2018

Özet

Bu makalede özetle, genom bilgisinin güvenliğinin öneminden bahsedilmiş, büyük genomik verilerin mahremiyetini ele alan çalışmalar incelenmiştir. Tıbbi verilerin mahremiyetinin teknoloji ilerledikçe daha az sağlandığı, verilerin güvenliği sağlanmadan teknolojinin ilerlemesinin kişiler açısından çok büyük sorunlara yol açacağı ortaya konmuştur.

Yapılan Çalışmalar

Bu makalede yapılan çalışmalar, büyük genomik verilerin ne olduğu, korunmasının ne kadar gerekli ve ciddi bir mesele olduğu yönündedir. Daha çok literatür taraması yapılmış ve örnekler vererek ilerlenmiştir. Dönemsel olarak keşiflerin değiştiği, dolayısıyla korunması gereken varlıkların evrildiği, ancak korunması gereken varlıkların korunmasının zorunlu olduğu gerçeğinin hep aynı kaldığından bahsedilmiştir. Büyük genom verilerinin, özellikle hassas parçaların anonim kalması gerektiği, ancak bunu sağlayarak genomlar üzerinde de araştırmalara devam edilmesi gerektiği, bunu sağlamadan da çalışmaların devam edemediği durumu ortaya koyulmuştur.

Sonuç

Bu makalede sonuç olarak, veri mahremiyeti sağlanmadıkça verilerin işlenmediği ve buna bağlı olarak tıbbi bilimlerin ilerlemesinin de yavaşladığı gösterilmiş, dolayısıyla bilgisayar bilimcilerinin ve tıbbi bilimlerde çalışanların birlikte ilerlemesi gerektiği söylenmiştir. Büyük genomik verilerin korunması gereken hassas bölgelerin korunmasının çok önemli olduğu ve bunun ciddi bir mesele olduğu dile getirilmiştir. Bu verilerin korunması için yapılması gerekenler listelenmiştir.

4. Sonuç ve Öneriler

Çalışma sonucunda varılan temel sonuç, bilgi güvenliği konusu hafife alınmayacak kadar önemlidir, ve ne yazıkki birçok kişi bundan habersizdir. Bu konuda çalışmalar yapılmalı ve öncelikle kişiler bilinçlendirilmelidir. Ayrıca verilerin korunması için çeşitli kriptografi yöntemlerine ihtiyaç vardır. Gelişen teknoloji ile kriptanaliz yöntemleri de kriptografi kadar hızlı gelişmekte, böylece şifreler daha hızlı çözülebilir hale gelmektedir. Bu da daha güçlü kriptografik yöntemleri gerektirir.

- Kişiler her şeyden önce, kendi güvenliğini sağlamalıdır.
- Artan sosyal medya kullanımı, veri gizliliğini yok saymaktadır, bu anlamda bilinçli bir sosyal medya kullanıcısı olmalı, paylaşımlarımızı kontrollü gerçekleştirmeliyiz.
- Kurumlar çalışanlarını bilinçlendirmeli, ve olası tehditlere karşı da verilerini koruma altına almalıdır. Gerekirse bazı önlemler şart koşulmalı, uygulanmadığı takdirde önlemler alınarak uygulanması sağlanmalıdır.
- Kişisel verilerimizi korumak konusunda haklarımızın bilincinde olmalı, herhangi bir verimizin güvenliğinin ihlali konusunda gerekli hukuki yaptırımları uygulayabilmeliyiz.
- Ulusal anlamda siber güvenlik önlemleri arttırılmalı, siber saldırılarla mücadele konusuna gereken önem verilmelidir.
- Kriptolojide, kriptografi ve kriptanaliz birbirini geliştirir, kırmızı şapka yerine beyaz şapkayı takmalı ve güvenlik saldırılarını kötü amaçlarla değil, olası güvenlik açıklarını tespit etmek amacıyla kullanmalıyız, akabinde kriptografik algoritmalar geliştirerek bu açıkları kapatmalıyız.

Kaynakça

Arian AJDARİ, Zeynep FENERCİ, Yılmaz VURAL, Yavuz CANBAY. (2018). Büyük Genomik Verisinin Mahremiyetinin Korunarak İşlenmesi. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 26-31). Ankara: Gazi Üniversitesi.

BEKTAŞ, A. (2016). Bilgi Güvenliği ve Kriptografi. *SPK'da Geçen Ay*.

Bilgi Güvenliği. (2021, 05 24). Vikipedi: https://tr.wikipedia.org/wiki/Bilgi_g%C3%BCvenli%C4%9Fi adresinden alındı

Bilgisayar. (2021, 05 24). Vikipedi: https://tr.wikipedia.org/wiki/Bilgisayar adresinden alındı

Bilgisayar Ağı. (2021, 05 21). Vikipedi: https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1 adresinden alındı

Cumali ÖZTÜRK, Mehmet TEKEREK, Ahmet Serdar YILMAZ. (2016). Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara: Gazi Üniversitesi.

Cumali YAŞAR, İhsan YILMAZ. (2019). Kuantum Dijital İmza Teknolojilerini Kullanarak Kuantum Elektronik İmza Geliştirmek. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 1-5). Ankara: Gazi Üniversitesi.

DİNÇER, İ. (2013). Siber Güvenlik Konusunda Kurumsal Farkındalık Ve Entegre Çözüm Alt Yapısı. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 242-245). Ankara: Gazi Üniversitesi.

Enes CANBAZ, M. Emir ÇAKICI, Yılmaz VURAL, Yavuz CANBAY. (2018). Büyük Genomik Verilerde Mahremiyet. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 19-25). Ankara: Gazi Üniversitesi.

G ŞENGÜL, F.K. ATSAN, A. BOSTAN. (2014). Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 95-101). Ankara: Gazi Üniversitesi.

GENÇOĞLU, M. T. (2019). Kuantum Kriptanalizin Siber Güvenlikteki Yeri. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 83-87). Ankara: Gazi Üniversitesi.

Gülcihan AYDANER, Ufuk ÇELİK, Senem NART. (2017). Siber Güvenlikte Kamu ve Özel Sektör İşbirliği. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 57-67). Ankara: Gazi Üniversitesi.

GÜNGÖR, M. (2015, Mart). Ulusal Bilgi Güvenliği : Strateji ve Kurumsal Yapılanma. T.C. Kalkınma Bakanlığı.

Gürol CANBEK, Şeref SAĞIROĞLU. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 165-174.

HENKOĞLU, T. (2017). Kişisel Verileriniz Ne Kadar Güvende? Bilgi Güvenliği Kapsamında Bir Değerlendirme. *Arşiv Dünyası*, 18-19.

KASIM, Ö. (2018). Medikal Verilerin Blok Zinciri Mimarisiyle Güvenliğinin Sağlanması. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 1-5). Ankara: Gazi Üniversitesi.

Kişisel Bilgisayar. (2021, 05 24). Vikipedi: https://tr.wikipedia.org/wiki/Ki%C5%9Fisel_bilgisayar adresinden alındı

Mete EMİNAĞAOĞLU, Yılmaz GÖKŞEN. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 01-15.

Mustafa ALKAN, Mustafa ÜNVER, Hakan TEKEDERE. (2012). Kayıtlı Elektronik Posta Sistemi ve E-Posta Güvenliği. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 251-255). Ankara: Gazi Üniversitesi.

Osman AKIN, Işıl ÇINAR, Muhammer KARAMAN, Fatih BİLEKYİĞİT. (2013). Siber Durum Farkındalığını Artırmada Etkili Bir Yöntem: Bayrağı Yakala. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 21-27). Ankara: Gazi Üniversitesi.

Ömer KASIM, Esmanur COŞKUN. (2019). Hassas Verilerin Korunmasında Klasik ve Kuantum Kriptoloji Yöntemleri Üzerine Bir Araştırma. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 74-79). Ankara: Gazi Üniversitesi.

Salih Erdem EROL, Eyüp Burak CEYHAN, Şeref SAĞIROĞLU. (2015). Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 1-9). Ankara: Gazi Üniversitesi.

Samet GANAL, Mehmet A. YALÇINKAYA, Ecir U. KÜÇÜKSİLLE. (2017). Kurumsal Bilgi Güvenliği Üzerinde Yeni Kayıtlı İnternet Sitelerinin Etkisinin Analiz Edilmesi. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 116-120). Ankara: Gazi Üniversitesi.

Seda YILMAZ, Şeref SAĞIROĞLU. (2013). Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 158-166). Ankara: Gazi Üniversitesi.

SOĞUKPINAR, İ. (2017, 02 19). Veri ve Ağ Güvenliği Ders Notları. *Bilgisayar Mühendisliği Bölümü*. Kocaeli, Gebze, Türkiye: Gebze Yüksek Teknoloji Enstitüsü.

TEKEREK, M. (2008). Bilgi Güvenliği Yönetimi. *KSÜ Doğa Bilimleri Dergisi*, 132-137.

TEKEREK, M. (2012). İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği.

TEKEREK, M. (2012). İlköğretim ve Lise Öğrencilerinin Bilgi ve Bilgisayar Güvenliği Farkındalığı: Kahramanmaraş Örneği. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 87-92). Ankara: Gazi Üniversitesi.

Türkay HENKOĞLU, Bülent YILMAZ. (2013). Avrupa Birliği AB Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği*, 451-471.

Uraz YAVANOĞLU, Şeref SAĞIROĞLU, İlhami ÇOLAK. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi*, 15-27.

Varlık. (2021, 05 24). Vikipedi: https://tr.wikipedia.org/wiki/Varl%C4%B1k adresinden alındı

YILDIRIM, E. Y. (2015). Sosyal Ağlarda Güvenlik Farkındalığının Arttırılması. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara: Gazi Üniversitesi.

Yılmaz VURAL, Murat AYDOS, Mehmet TEKEREK, Ahmet Serdar YILMAZ. (2016). Akıllı Şebekeler Veri Mahremiyetine Yönelik Tehditler. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara: Gazi Üniversitesi.

Yılmaz VURAL, Şeref SAĞIROĞLU. (2008). Ülke Bilgi Güvenliği. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 3-20). Ankara: Gazi Üniversitesi.

YILMAZ, İ. (2018). Bilgi Güvenliği Bağlamında Yeni Teknolojik Devrim: Kuantum Teknolojiler. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı* (s. 32-39). Ankara: Gazi Üniversitesi.

RAPOR SONU

SON DEĞİŞİKLİK : 01.06.2021 05:30

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2021