DATA PROTECTION

Ali AYDOGAN

Özet

Bu çalışmada, bilim ve teknoloji alanında gerçekleşen gelişmeler sonrası özel hayatın gizliliği kavramı altında kişiye özel veriler olarak tanımlayabileceğimiz kişisel verilerin korunması konusuna parmak basılmıştır. Bu çalışmalar sırasında verilerin korunması konusunda birçok makale üzerinde inceleme yapılmış ve bu makalelerin içerikleri esas alınarak veri koruması konusunda birçok metot önerildiği görülmüştür. Bu metotlar üzerinde gerekli araştırmalar yapılarak verinin nasıl korunması gerektiğini inceleyerek konu hakkında birçok fikir ve beyanda bulunduk.

1. Giriş

Verilerin korunması deyince akla ilk olarak "veri"lerin değil, bu verilerle ilgisi olan kişi ve kuruluşların korunması gelmelidir. Verilerin korunması kişi ve kuruluşları onların hakkındaki bilgilerin ele geçirilmesinden doğacak olan tehlike ve zararlardan koruma amacına yönelmiştir. Bilgisayarların ilk ortaya çıktığından beri sürekli gelişmesi ve teknolojinin ışık hızıyla ilerlemesinden dolayı çok fazla bilginin, daha kolay, daha hızlı ve daha ucuz olacak şekilde depolanması; ağların paylaşılmasını kolaylaştırdığı için kişilerin özel yaşamlarına dair birçok risk ve tehlikenin ortaya çıkmasına neden olmuştur.

Burada ilk olarak kişisel verinin ne olduğuyla söze başlayalım. Kişisel veri genel olarak belirli bir nitelikteki kişiye ait olan her türlü bilgi olabilir. Mesela en basit örneğiyle bir kişinin ismi onun bir kişisel verisidir. Kişisel veriler kişilere özeldir. Bazı kişiler için bu veriler mahremiyet tanımı içerisinde yer almaktadır. Mahremiyet kavramına gelecek olursak; herhangi bir kişinin diğer kişi ve kuruluşlarla paylaşamayacağı bilgilere genelde o kişinin mahremiyeti denir. Mahremiyet kavramının çiğnenmesi konusunda burada devreye veri koruma yöntemleri devreye girmektedir.

Yapmış olduğumuz araştırmalarda kişisel veriler üzerinde kişilerin bir hakkı bulunmasına ilk olarak Federal Almanya'da 1983 tarihli meşhur Nüfus Sayımı (Census) kararında yer verilmiştir. Ülkemizde 18 Ocak 2016 tarihli "Kişisel Verilerin Korunması Kanun Tasarısı"nda da kişilere bu konu hakkında önem verilmiştir.

2. Veri Koruma Metotları

İncelemiş olduğumuz makaleler sonucu birçok veri koruma yöntemleri tespit edilmiştir. Bulut teknolojisi, mobil teknolojiler gibi birçok alanda verilerin nasıl korunduğu konusunda birçok yöntem belirtilmiştir. Bu yöntemler verilerimizin korunurken ne gibi algoritmalar ve implementasyonlar yapıldığını bize göstererek bizim düşünce evrenimizde genişlemelere yol açacaktır.

2.1. Tabular Data Protection (Çizelgeli Veri Koruma)

Tabular data protection[1] isminden de anlaşılacağı üzere tablolar ve çizelgelerden oluşan bir yöntemdir. Tablonun her hücresi bireyler için toplu bilgileri göstermesine rağmen, bireysel verilerin açığa çıkma riski vardır.

		x_1	x_2	
⋮	...	...	...	...
51–55	...	38000€	40000€	...
56–60	...	39000€	42000€	...
⋮	...	...	...	...

(a)

		x_1	x_2	
⋮	...	...	...	...
51–55	...	20	1 or 2	...
56–60	...	30	35	...
⋮	...	...	...	...

(b)

a tablosunda ZIP code ve yaş aralığı için ortalama maaş bilgisi gösterilmektedir. b tablosu ise kişi sayısını göstermektedir.

Karmaşık durumları çözmek için oluşturulmuş çok boyutlu, hiyerarşiyel ve link tabloları mevcuttur. Çok boyutlu tablolar 2'den daha fazla değişken olduğunda elde edilir. Bu tablolar

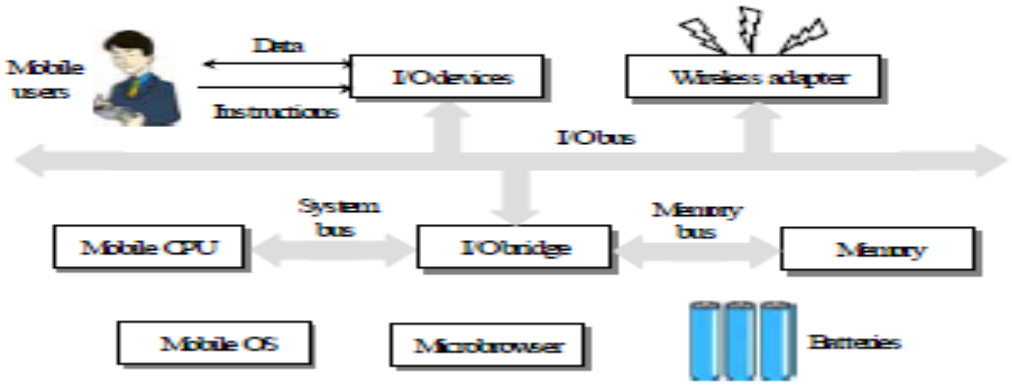
tek tek korunur. Hiyerarşiyel tablolar da ise verilen 2 değişken arasında hiyerarşik bir ilişkinin bulunduğu tablolardır. Posta kodu ve şehir arasındaki ilişki buna örnek olarak gösterilebilir. Hassas verilerin ortaya çıkmasını engellemek için değişkenler beraber korunmalıdır. Link tabloları ise önceki duruma bakılarak tablolar arasında bir genelleme yapılır. Birçok tablo aynı mikroverilerden yapılmaktadır. Burada bilgi paylaşımı mevcuttur. Ancak paylaşılan bilgiler hiyerarşik yani birbiriyle ilgili değildir.

2.2. Trap Array

Trap Array[2] isimli sistem sürekli veri koruma(CDP)'yi destekleyen bir yapıdır. Bu sistemin odak noktası CDP tarih verilerinin bitmesini azaltmaktır. Bu sistem depoda bulunan her bloğun versiyon tarihinin sıkıştırılmış yapısına ulaşır. Bu sistemin maliyeti herhangi bir versiyona ulaşmak için bloğun tüm geçmişini almak gerekir. Bu sistem yeni işletim sistemlerine erişebilirken, yapılan işlemlerde geri alma desteği sağlamaz.

2.3. Mobil Telefonlarda Metotlar

LAC sistem[4], mobil telefonlarda kullanıcı tarafından tanımlanan izin verilmiş bir tehlikeli kümenin çalışmasını engellemek için kullanılan bir sistemdir. Paranoid Android adı verilen Android telefonlarda kullanılan başka bir sistem de kötücül yazılımları tespit etmekle sorumludur.

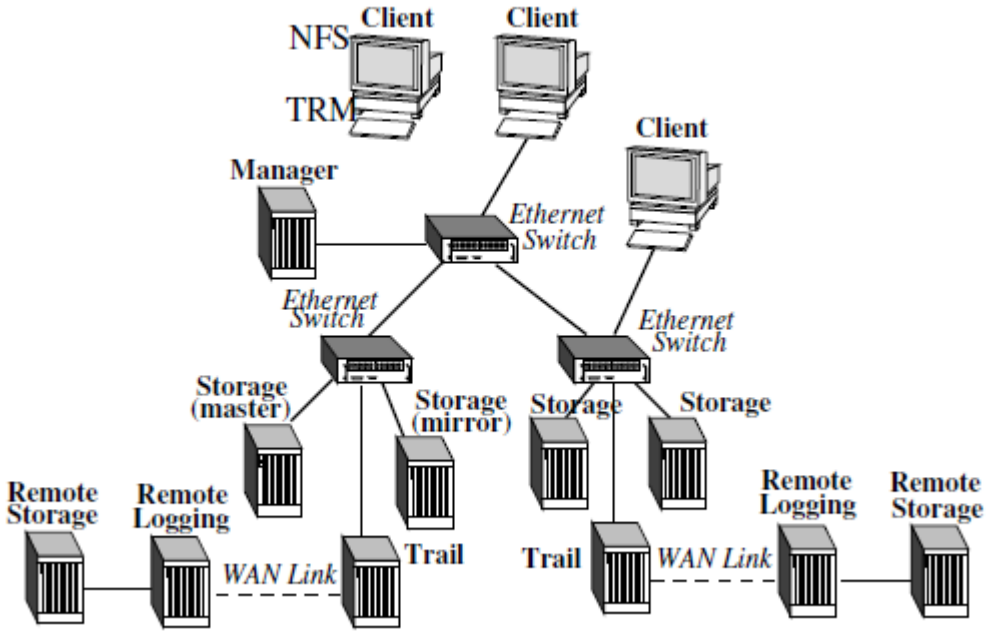


Mobil cihazlarda verileri korumak için 3 büyük teknoloji uygulanır.[7] Bunlardan ilki şifre belirlemektir. Ancak çoğu kullanıcı bunu ihmal etmektedir. Çünkü birçok insan şifreyi giriş veya şifreyi ezberleme konusunda sıkıntı çekmektedir. İkincisi ise retina, parmak veya yüz tanıma içeren biyometrik özelliklerin kullanılmasıdır. Ancak bu özellik bütün cihazlarda bulunmadığı için kullanımı çok yaygın değildir. Pratik olarak pek fazla uygulanmamaktadır. Üçüncü özellik ise kişinin cihazı kullanımına göre hafızada belirli bir depolama alanı oluşturulup başka kişilerin tanınmasını engellemektir.

2.4. Mariner Yapısı

Bu konuyla okumuş olduğum makalede[5] Mariner olarak bilinen ISCI tabanlı depolama sisteminin hesaplanması, implementasyonu ve tasarımı anlatılmıştır. Bu yapı performans yükünü oldukça azaltırken kapsamlı bir veri korumayı destekler.

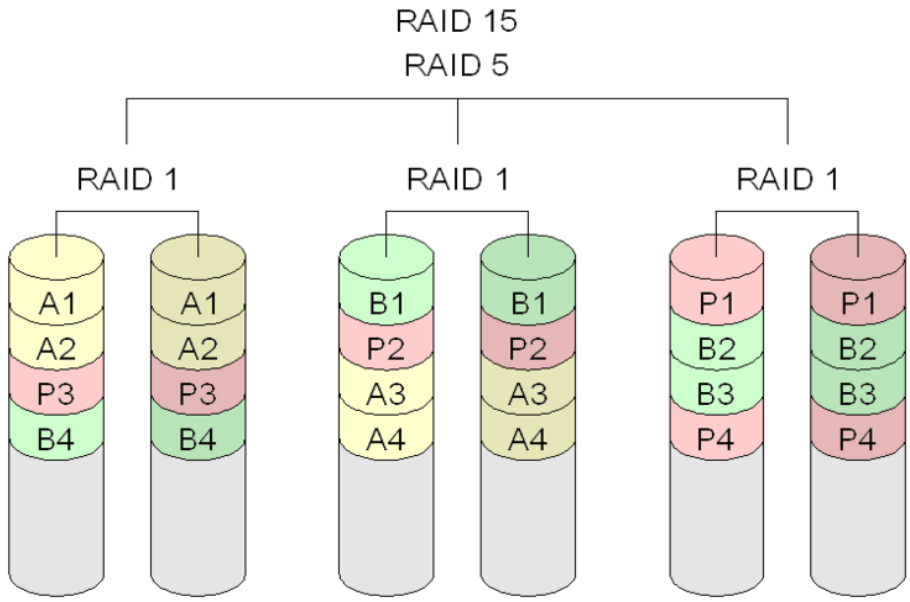
Bir mariner istemcisi 3 ISCI depolama sunucusuyla ilişkilidir. Bunlar master storage server, local mirror storage server, logging server olarak adlandırılmaktadır. Mariner istemcisi bir veri bloğuna yazmak istediğinde, yazma isteği bu 3 servera gönderilir. Veri bloğu senkronize olacak şekilde logging server'da işlenir ve daha sonra master server, local mirror server'da işlenir.



Mariner yapısı blok seviyesinde sürekli veri korumayı(CDP) destekler. Bu yapı her yazma isteği için yeni bir versiyon oluşturur. Zaman içinde herhangi bir nokta için roll-back'a izin verir. CDP, bozuk verileri düzeltmeyi sağlar. Marinerin logging server'ı belirli bir zaman periyodunda her disk yazım işleminden önce image almadan sorumludur. Bu yüzden böylece yaptıklarınızı geri alabilirsiniz. Diğer bir yapı olan Trap-Array'lar de böyle bir özellik mevcut değildi.

2.5. RAID

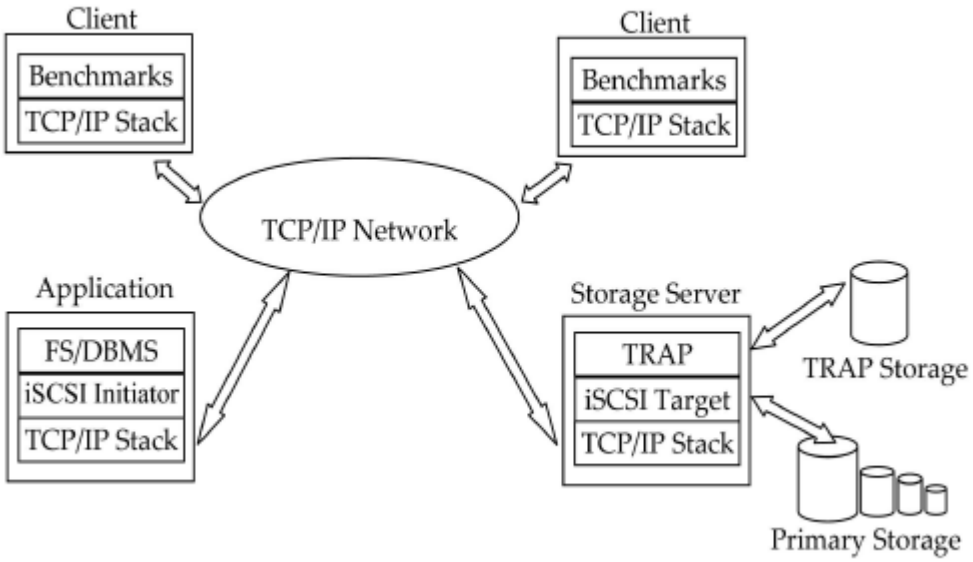
[9]Veri kaybını engellemek için yeni bir disk takıyorsunuz ve taktığınız bu disk ile ister performans elde edebilirsiniz, isterseniz de veri kaybını engellemek için güvenlik oluşturabilirsiniz. Raid 1+5 en önemli yapıdır. Çok önemli dosyaların saklanmasında kullanılır. 2 adet Raid 5 yapısının Raid 1 bünyesinde birleşmesidir ancak en az 6 adet disk gerektirmektedir. Şekil üzerinde gösterimi;



Raid sistemleri, donanımsal ve yazılımsal olmak üzere 2'ye ayrılmaktadır. Yazılımsal raid, ek bir donanıma ihtiyaç duymadan genelde Windows gibi işletim sistemlerinde kullanılmaktadır. Donanımsal raid ise, bir raid kartı gerekmektedir.

2.6. TRAP-4

Xiao[9], çalışmalarında TRAP-4 ismi verilen bir yapıyı implement etmiştir. Read-Modify-Write olarak bilinen parite hesaplama algoritması, güncellenmiş bütün veri blokları için orijinal veri değerlerini okumayı gerektiren bir yapıdır. Parite hesaplaması boyunca, TRAP gösterilen şeklin ilk 2 parçasını ekleyebilir. Veri bloklarının değişikliklerini tam olarak yansıtabilir.



[9]

Read-Modify-Write algoritmasının yanı sıra çoklu blok değişiklikleri için parite hesaplayan Reconstruct-Write isminde başka bir algoritma vardır. Reconstruct-Write algoritması bütün değişiklik yapılmamış veri değerlerini okur ve eski pariteyi yeniden kullanmak yerine bir veri şeridi içinde yeni veri bloklarından pariteyi inşa eder. Güncellenmiş bir veri şeridinde veri bloklarının çoğu ya da bütün şerit olduğu durumlarında bu algoritma oldukça etkilidir.

2.7. Depolama Snapshotları

Snapshotlar[8], veri ve sistemleri korumak için kullanılan yöntemlerden bir tanesidir. Snapshot, bilgisayar bilimlerinde sistemin belirli bir zamandaki durumunu ifade eder. Depolama snapshot'ı ise verilerimizin belirli bir andaki görüntü seviyesinde olan görünümüdür. Depolama snapshot'ı oluşturulduğunda varsayılan olarak alan kaplamaz. Yalnızca izleme amaçlı olarak ve işaretçilere dayanan değişiklikleri kaydetmek için kullanılan yakalanan verilerle ilgili bilgiler içeren meta verilerin bir kopyasıdır. Bu yapı anında oluşturulur, saniyeler içinde oluşturulur. Bundan dolayı RPO'ların dakikalar içinde gerçekleştirilmesini sağlayan bir yöntemdir. Snapshotlar bozulma ya da geri yükleme özelliklerini kontrol edecek herhangi bir araca sahip değildir.

3. Replication

[5]Kişisel hata ve doğal afet durumlarında, teknoloji alt yapısını kurtarmak ve devamlılığı sağlamak için kullanılan süreç ve yöntemleri temsil eder. Genel bir teknik olduğundan diğer metotlardan ayrı tuttum. Yapılan araştırmalara göre kritik verilerini kaybeden kurumların neredeyse tamamına yakını iki üç yıl içerisinde yok olmaktadır. İş süreçlerinin devam etmesi için bu teknik önemli bir yer teşkil eder. Birçok sektörde sistemlerin durması inanılmaz maliyetlere sebebiyet vermektedir. İş süreçleri için çok kritik olan verilerin korunması ve de sistemlerin maksimum ne kadar kapalı kalması gerektiği planlanarak önlemler alınmaktadır. Veri kopyalama çözümü platformlarımızın bir anlık veya kesintisiz olarak farklı bir platforma kopyalanmasını içeren, hatasız bir şekilde yapılması gereken ve de özellikle felaket ve kullanıcı hataları oluştuğunda kullanılması gereken bir tekniktir.

4. Bulut Teknolojisinde Veri Koruma

Veri kaybını önlemek için, bulut sistemlerinde[6] veri koruma ve esneklik olayları oldukça önemlidir. Bulut sistemlerinde bir veri kaybı oluşursa, bulut sistemine tekrar erişim sağlamak için bilgi işlem ortamına verilerin hızlı bir şekilde geri yüklenmesi gerekir. Bilgi işlem ortamı private, public ya da hybrid olduğunda bu genelleme doğrudur. Bulut teknolojisinde verileri korumak için makaleye göre birçok alternatif düşünülmüştür.

- **Integrity:** Saklanan veriler bozuk olmayacaktır.
- **Privacy:** Gizli veriler yetkilendirilmemiş bir kişi tarafından sızdırılmış olmayacaktır..
- **Access Transparency:** Kayıtlar her türlü veriye erişimi kim ya da ne olduğunu açıkça gösterecektir.
- **Ease of verification:** Müşterilere verilen uygulama kodu kolayca doğrulanacaktır.
- **Rich computation:** Bulut platformu kullanıcılara duyarlı kullanıcı verisinde, verimli ve zengin hesaplamalar sağlayacaktır.
- **Development and Maintanance:** Bu yapılar değişimlerin uzun bir listesini gösterir. (Sık yazılım güncellemeleri, sürekli kullanılan yapı değişimleri)

5. OneFS Veri Koruma

[8]Big Data için üretilen bir yapı olan EMC Isilon depolama biriminde Cluster'ın bütün nodeları üzerinde çalışan tek bir dosya sistemi mevcuttur ve her şeyi bu sistem yönetmektedir. RAID, volume'lar ve dosya sistemi bu yapı tarafından yönetilmektedir. Bu yöntemle az bir yönetim eforuyla birçok şeyle başa çıkılabiliyor.

OneFS, dosya sisteminin bir parçası olarak veri korumayı implement eder. Veri koruma bu yapıda RAID kontrollerinden ve donanımdan bağımsızdır. OneFS, Reed-Solomon Forward Error Correction ile veriyi korumaktadır. Ya da FEC adı verilen yüksek verim sağlayan güvenilir bir metodu kullanmaktadır.

6. İşletim Sistemlerine Göre Veri Koruma

[10] Yapılan çalışma farklı işletim sistemlerinde yapılmıştır. Bazı uygulamaların veri koruma için oluşan değerleri tablo üzerinde işaretlenmiştir.

Runtime environment, applications ***Threats***	***Measures***	***Android***	***Apple***	***Symbian***	***Windows***	***Blackberry***
+Monitoring (on phone) *+Third party service suppliers* *+Application repositories* *+File system privilege escalation* *+Permissions privilige escalation* *+Application security* *+Rooting*	*Anti virus check*	*X*		*X*	*X*	*X*
	Code signing	*X*	*X*	*X*	*X*	*X*
	Enhanced security features (such as trusted path execution)	*(X)*				

7. Sonuçlar

Genel olarak araştırdığımız makalelerde veriyi korumak için farklı teknikler kullanılmıştır. Ancak kullanılan tekniklerin bazılarında veriyi ifşa edecek durumlar hala mevcuttur. Bu şekildeki verileri korumak için daha farklı koruma yöntemleri geliştirilebilir. Eğer halen verilerinizin güvenliğini düşünüyor ve kullandığınız verilerin kaybolmasını istemiyorsanız kullandığınız parolalarda uzun ve güvenli seçimler gerçekleştirebilirsiniz, güvenlik duvarlarını aktif hale getirebilirsiniz, sisteminizi sürekli güncel halde tutabilirsiniz, e-mailler çok sakıncalıdır, gelen ve giden e-maillerinize dikkat ediniz, Trojan,Keylogger,Rootkit gibi zararlı yazılımlara karşı savunmalar oluşturabilirsiniz.

Kaynaklar

1- Jordi Castro* ,“Minimum-distance controlled perturbation methods for large-scale tabular data protection”,Department of Statistics and Operations Research, Universitat Politecnica de Catalonya, Pau Gargallo 5, 08028 Barcelona, Spain , Receivde 3 July 2003; accepted 9 August 2004 Available online 2 November 2004

2- Paula Ta-Shma, Guy Laden, Muli Ben-Yehuda, Michael Factor, “Virtual Machine Time Travel Using Continous Data Protection and Checkpointing” , IBM Haifa Research Lab

3- Deyan Chen, College of Information Science and Engineering Northeastern University Shenyang, China ,Hong Zhao,Academy Neusoft Corporation Shenyang,China , “Data Security and Privacy Protection Issues in Cloud Computing”

4- Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, Konstantin Beznosov, Electrical and Computer Engineering Department , The University of British Columbia Vancouver,Canada , “Understanding Users’ Requirements for Data Protection in Smartphones ”

5- Maohua Lu, Shibiao Lin, Tzi-cker Chiueh, Computer Science Department Stony Brook University{mlu,slin,chiueh}@cs.sunysb.edu “Efficient Logging and Replication Techniques for Comprehensive Data Protection”

6- Bhagya Laksimi,G. Sridevi “A Novel Computing Paradigm for Data Protection in Cloud Computing”

7- Wen-Chen Hu, Department of Computer Science University of North Dakota Grand Forks, North Dakota 58202-9015, Yanjun Zuo, Dept. Of Information Systems and Business Education University of North Dakota Grand Fork, North Dakota 58202-8363, “Mobile Data Protection Using Handheld Usage Context Matching”

8- EMC Products, www.emc.com, “EMC Isilon Scale-Out NAS: An Architecture for Resiliency,High Availability, and Data Protection

9- Weijun Xiao, Student Member, IEEE, Jin Ren, and Qing Yang, Senior Member, IEEE, “A case for Continuous Data Protection at Block Level in Disk Array Storages”

10- Cormac Callanan , Borka Jerman-Blazic and Hein Dries-Ziekenheiner* Postgraduate International School Jozef Stefan Jamova 39, Leiden, The Netherlands email:cc@aconite.com, borka@e5,ijs.si and hein@vigilo.nl, “Empirical Assesment of Data Protection And Circumvention Tools Availability in Mobile Networks”