Bulut Bilişim'de Kişisel Verilerin Güvenliği ve Mahremiyet Nasıl Sağlanabilir?

N. Tuğbagül ALTAN AKIN

Gebze Yüksek Teknoloji Enstitüsü, Bilgisayar Mühendisliği Bölümü, Kocaeli

tualtan@gyte.edu.tr

Özet: Şüphesiz bilginin elektronik ortamlarda işlenebilir, saklanabilir hale gelmesi insan hayatını kolaylaştırmıştır. Veri adı verilen elektronik ortamda işlenebilir ve saklanabilir bu bilgi türü, hayatlarımızda birçok kolaylık sağlarken bir takım sorunları da beraberinde getirmiştir. Özellikle son zamanlarda verinin kolay saklanabilir olması ile de ilgili olan artan özçekim miktarları, her anı fotoğraflama, kameraya alma ve saklama gibi isteklerin çoğalması kişisel bilgisayarların bellek miktarlarını yetersiz bırakmaktadır. Son zamanlarda, kişisel verilerin saklanması için gerekli olan bellek miktarı, çevrimiçi çalışan birçok uygulamanın da üzerinde çalışabildiği Bulut bilişim kullanılarak karşılanmaya çalışılmaktadır. Bulut bilişim, kişisel verilerin saklanılması için gerek duyulan bellek ihtiyacına olumlu cevap verse de kişisel verilerin korunması, gizlilik, mahremiyet ve bireysel haklar gibi konularda sorunlar barındırmaktadır.

Bu çalışmada, Bulut sisteminde saklanılması istenen kişisel verilerin, gizlilik, mahremiyet, bireysel haklar ve korunma prensipleri açısından ne gibi riskler taşıdığı ve bu riskler için ne gibi önlemler alınabileceği üzerinde durulmuştur.

Yapılan bu araştırma ile günümüzde kullanımı gittikçe yaygınlaşan ortak paylaşım alanlarında, kişisel verilerin, bahsedilen prensiplere uygun bir şekilde saklanması için geliştirilebilecek yaklaşımların neler olabileceği konusunda bir fikir verilmesi amaçlanmıştır.

Anahtar Sözcükler: Bulut Bilişim, Gizlilik, Bireysel Haklar, Mahremiyet, Kişisel Verilerin Korunması.

Abstract:

There is no doubt that human life becomes easy when data is processed and stored on digital machines. Therefore, some problems are caused by this issue. People need more memory to store their some private, personal documents because their desktop has not enough memory to store selfies, photos, records or other types documents which need a huge memory size. Thus, some people with memory problems begin to use Cloud Computing which is based on online servers. Using flexible, scalable Cloud Computing is an easy way to store, share data. Unfortunately, reliability, availability, security and privacy issues of Cloud Computing have important problems for users. In this paper, I focus on risks of reliability, availability, security and privacy problems on Cloud Computing. Then I explain some studies which work on these issues and aim to propose some ideas to solve these problems on Cloud Computing.

1. Giriş

Şüphesiz bilginin elektronik ortamlarda işlenebilir, saklanabilir hale gelmesi insan hayatını kolaylaştırmıştır. Veri adı verilen elektronik ortamda işlenebilir ve saklanabilir bu bilgi türü, hayatlarımızda birçok kolaylık sağlarken bir takım sorunları da beraberinde getirmiştir.

Özellikle son zamanlarda verinin kolay saklanabilir olması ile de ilgili olan artan özçekim miktarları, her anı fotoğraflama, kameraya alma ve saklama gibi isteklerin çoğalması kişisel bilgisayarların bellek miktarlarını yetersiz bırakmaktadır. Son zamanlarda, kişisel verilerin saklanması için gerekli olan bellek miktarı, çevrimiçi çalışan birçok uygulamanın da üzerinde çalışabildiği

Bulut bilişim kullanılarak karşılanmaya çalışılmaktadır.

Ölçeklenebilir, esnek bir yapıya sahip olan Bulut Bilişim yeni bir teknoloji olarak gözükse de 1960'lı yıllarda geliştirilmeye başlanmıştır [1]. Verilerin, kişisel bilgisayarlardaki bellekleri kullanmadan Bulut sistemi denilen çevrimiçi bir yapı içerisinde bulunan sunucularda saklanması, yine bu sistem içerisinde çeşitli uygulamaların çalıştırılması Bulut Bilişim teknolojilerinin kullanımını sürekli arttırmaktadır. Bulut bilişim sektöründe yapılan yatırımlar azımsanamayacak ölçülerdedir. Örneğin ABD federal hükümetinin Bulut hesaplama uygulamaları üzerinde yapacağı harcamaların 2020 yılına kadar on milyar doları geçeceği bildirilmektedir [2]. Birçok şirket sistemini Bulut Bilişim üzerine taşımak istemektedir ve bunun için gerekli altyapı sistemini sağlamaya çalışmaktadır. Teknolojik her gelişimde olduğu gibi Bulut hesaplama uygulamaları da hayatımızı kolaylaştırırken, çözülmesi gereken sorunları da beraberinde getirir. Bu sorunların çözülmesi teknolojiyi geliştirirken, teknolojinin gelişmesi sorunları çözdüğü gibi yeni sorunların da doğmasına yol açar. Gelişen teknoloji, uygulamada insan hayatını kolaylaştırırken, peki insan psikolojisinde ve insan hayatında sosyolojik açıdan ne gibi sorunlara yol açar ve bu sorunlar teknolojinin gelişmesi ile çözülebilir mi? Bu sorunun cevabını, teknik, psikolojik ve sosyolojik açıdan düşünmek önemlidir. Ancak bahsedilen bu farklı açıların iç içe geçtiği durumların varlığını da unutmamak gerekir.

Bulut Bilişim alt-yapısından kısaca bahsedecek olursak, dağınık bir sistem mimarisi üzerine kurulmuş, açık kaynak da olabilen yazılımlar ile geliştirilen bir sistemdir. Bulut Bilişim sisteminde, kullanıcılar ile kullanıcıların bilgilerinin hangi sunucuda tutulduğu ya da hangi sunucuda uygulamalarının çalıştırıldığı bilgisi paylaşılmaz. Bu durumda akla ilk gelebilecek sorulardan biri: "Bulut Bilişim'den faydalanmak isteyen kişi, kişisel verilerini bu sistem üzerinde tuttuğu zaman, bu bilgilerin mahremiyet, gizlilik prensiplerine uygun bir şekilde ve kişisel verilerinin güvenli bir şekilde korunduğundan nasıl emin olur? " sorusu olacaktır.

Sosyolojik açıdan, İnsan Hakları Evrensel Beyannamesi 1.ve 7. Maddeler (temel haklar) , Anayasa Madde 20 (Kişisel Bilgilerin Korunması), 5237 Sayılı Türk Ceza Kanunu Madde 135, Madde 136 ve Madde 137 gibi yasal düzenlemeler ile kişisel verilerin yasal olmayan şekilde paylaşılması ya da işlenmesi çeşitli yaptırımlara tabi tutulmuş olsa da, bu yaptırımların değiştirilmesi ya da yeni düzenlemeler yapılması ile birlikte teknik açıdan kişisel verilerin gizli kalması konusu, üzerinde düşünülen ve üzerinde çeşitli araştırmalar yapılan güncel bir konu olma özelliğini korumaktadır. Teknolojik gelişimler aynı zamanda bahsi geçen yaptırımlar üzerinde etkili olur ve yeni teknolojik gelişimler de yeni yasal düzenlemelere ihtiyaç doğurur. Ülkemizin ön sıralarda olmak üzere Bulut Bilişim'in parçası olan tüm ülkelerde, yeni teknolojik gelişimler için gerekli yeni yasal düzenlemelere acil olarak ihtiyaç vardır.

Limitsiz depolama, kolay paylaşım imkânına sahip olması ve bunun gibi kullanıcıyı etkileyen birçok cazibesi bulunan Bulut Bilişim üzerinde gizlilik, güvenlik ve güvenilirlik gibi oldukça elzem konular üzerinde düşünülmesi gerekir [3]. Bulut Bilişim üzerinde bahsi geçen konular üzerinde kullanıcılar bir takım sorunlar ile karşılaşmış ve karşılaşmaktadır. Bu nedenle araştırmacılar, Bulut Bilişim kullanıcılarına güven eksikliklerini giderme konusundaki çalışmalara daha çok yönlenir olmuştur [4]. Teknolojik gelişimler bu konularda kullanıcılara yeterince yardımcı olmaz ise Bulut sisteminde giderilmesi ümit edilen güvenilirlik ve gizlilik gibi konularda, toplumlarda endişe oluşur ve kullanıcılar bazı sistemleri kullanmaktan vazgeçebilirler.

Bulut Bilişim'de güvenlik ve güvenilirlik konularını çok detaylı incelemek mümkündür. Örneğin Bulut sistemde paylaşılan bir verinin o veri olup olmadığının

kontrol edilmesi ile Bulut sisteme yüklenen verinin kimler ile paylaşıldığından emin olunması farklı yaklaşımlar gerektiren konulardır.

Bulut Bilişim, uygulama çalıştırma, veri iletme, veri alma, gibi birçok işlemin yapılmasına olanak sunar. Bu çalışmada, Bulut Bilişim özel verileri, depolama ya da sadece istenen kullanıcı veya kullanıcılar ile paylaşma amaçlı kullanıldığı zaman, bu özel verilerin güvenlik, mahremiyet ve verilerin korunması prensiplerine uygun bir şekilde saklanılması için alınabilecek önlemler bulunmakta ve bu konuda araştırmacılara bir fikir verilmesi amaçlanmıştır.

2. Bulut Bilişim ve Gizlilik Açısından Veri İletimi

Gelişmeler ile birlikte, Internet kullanıcıları yazılımları masaüstü bilgisayarlarında koşturmak yerine ağ bağlantılı sunucular, depolama birimleri ve cihazlardan oluşan Bulut'u kullanarak beklentilerini karşılayabilmektedirler. Bulut sistemi üzerinde veri alışverişi yapılırken veri gizliliği konusunda yeterince duyarlı olunamaması bir problem oluşturmaktadır [5]. [6] çalışmasında Bulut Bilişim'in mimari yapısına değinilmiş, güvenli iletim için Bulut entegretörlerinin, verilerin doğru yol üzerinde iletilmesinde çok önemli bir rol oynadıkları ifade edilmiştir. Bulut Bilişim'de veriler iletilirken değiştirilebilir, kullanıcının isteği dışında paylaşılabilir ya da kopyalanabilir. Tüm bu istenmeyen durumları önlemek için birçok yöntem geliştirilse de, mevcut sistemler için kesin bir çözüm bulunamamıştır.

Kullanıcılar, Bulut sisteminde kendi bilgisayarlarını sunucu yapabildikleri gibi kendi bilgisayarlarını paylaşıma açmadan da Bulut Bilişim'i kullanabilirler. Kendi bilgisayarlarını sunucu olarak göstermek isteyen kullanıcılar erişim sınırı getirip kendi bilgisayarlarının sadece bir miktar belleklerini ortam paylaşım alanı olarak da tanımlayabilirler. Tüm bu kolaylıklar aynı zamanda bir takım riskler taşımaktadır. Bu risklerin başında ortak paylaşıma açılan alanlara erişebilen kullanıcı profillerinin net olarak bilinmemesi gelir.

Çok sayıda sunucunun paylaşılmasına olanak sağlayan sanal makineler, depolama cihazlarının daha etkin kullanımını sağlarlar. Sanal makineler ile depolama alanı sağlanırken, sanal makinelerin saldırılar için çok daha fazla sayıda arayüze sahip olmaları önemli riskleri beraberinde getirir. Bu durum da ayrı olarak çözülmesi gereken bir güvenlik sorunu olarak düşünülebilir.

Kullanıcılar Bulut'ta gerçekleştirdikleri işlemlerin hangi sunucular üzerinde gerçekleştirildiğini tam olarak bilemeseler de servis sağlayıcılar, kullanıcıların Bulut sistemi üzerinde ne işlemler yaptıklarını ve bağlantılı sunucuları izleyebilmektedirler. Peki, kullanıcıların tam olarak hangi sunucuya bağlandıklarını bilmemelerine rağmen servis sağlayıcıların bu bilgileri bilmeleri gizlilik ve güvenlik gibi konularda yeterli gelmekte midir?

Bir bakıma kullanıcıların hangi verisinin nerede bulunduğunun kullanıcılar ile paylaşılmaması sistemin basitleştirilmesinin yanı sıra Bulut Bilişim'in kendi içerisinde, kullanıcı profillerine karşı gizlilik prensibini bir miktar karşıladığını gösterir. Servis sağlayıcıların verinin nerede olduğu konusunda izleri takip etmesi de, kişisel işlemler ya da kişisel verilere bir saldırı olduğu zaman, saldırının tespit edilmesinde elbette yardımcı olmaktadır ancak Bulut Bilişim'in sınırsız bir ölçeklenebilir yapıya sahip olması, ülkeler arası çok geniş bir alana hâkim olabilme özelliği veri takibinin tespitini zorlaştırmaktadır. Bu alanda da Bulut Bilişim'de yer alan ülkelerin belirli standartları sağlaması Hukuksal işlemlerin yürütülme sürecini hızlandıracaktır. Ayrıca Hukuksal işlemlerin sürekli değişen bu sistemlerde yaptırım gücünün korunması için yeni düzenlemelere ihtiyaç duyulmaktadır [7]. Diğer açıdan, bazı mahremiyet sınırları ya da iş ile ilgili haksız rekabet oluşturacak konularda bilgilerin paylaşılmasından sonra kim tarafından yapıldığının önemi, bu bilgilerin paylaşılması kadar önem

taşımamaktadır. Güvenlik konusunun daha çok Bulut Bilişim sistemi ile ilgili olduğunu düşünürsek, gizlilik konusunun da kişi ile doğrudan ilişkili olduğu söylenebilir. Dolayısı ile gizlilik konusunu Bulut Bilişim üzerindeki sistemler üzerinden düşünmek yerine birebir kullanıcı üzerinden ele almak gerekir.

3. Önceki Çalışmalar

Bulut'ta güvenlik probleminin aşılması için birçok yöntem geliştirilmiştir. Bu yöntemler, ağ yapıları, veri tabanı, işletim sistemleri, sanallaştırma, kaynak ayırma, bellek yönetimi ve veri iletimi esnasında şifreleme gibi başlıklar altında yer alabilir [6].

[8] çalışmasında, araştırmacılar Bulut Bilişim'deki güvenlik ve gizlilik konuları üzerinde araştırma yapmış, belirli bir senaryo için istemci tabanlı gizlilik yönetim aracı önermiş ve bu yönetim aracını belirledikleri senaryo üzerinde test etmişlerdir. Önerilen aracın, sunucu ile iletişim kurduğu anda gizlilik prensibine uyulduğunun kontrolü yapılmak istenilmiştir. Ayrıca bu araç, kullanıcılara gizli bilgilerin Bulut'un dışında depolama imkânı sunmuştur. Bu çalışma gizlilik yönetimi, erişim kontrolü gibi önemli konularda başarılı olsa da geliştirilen araç genel yani her senaryo için kullanılır olmamıştır.

Büyük ya da küçük ölçekli birçok firma, bireysel kullanıcılar Bulut Bilişim'i kullanırken, veri kaybı, gizliliğin korunamaması gibi konularda endişe duymaktadırlar. Kullanıcıların güvenlik, gizlilik tehditleri ile karşı karşıya kalmalarını engellemek için geliştirilen birçok model olsa da bu önemli konularda yeterli derecede beklentileri karşılayan bir standart geliştirilememiştir [9].

[10]'da ise, araştırmacılar Bulut'ta güvenlik problemini çözmek için PasS adını verdikleri Bulut sistemi altyapısı ile ilişkilendirilmiş birçok güvenlik protokolü içeren bir yapıyı sunmuşlardır. Bulut sisteminde, bu yapının kriptografi üzerinde daha önceden yapılan çalışmalardan faydalanılarak oluşturulan, pratik bir çözüm olduğunu belirtmişlerdir. Ancak bu çalışmada anahtarlama ile ilgili geliştirilmesi gereken kısımların yanı sıra standartlaştırılamamış modellemeler de bulunmaktadır.

Güvenlik açıkları Bulut Bilişim'in gelişmesine engel olmaktadır. Dağınık hesaplama, paralel hesaplama, grid hesaplama ve birçok hesaplama altyapı sisteminden türemiş olan Bulut bilişimde, tek bir güvenlik metodu ile güvenlik problemlerini çözülmesi mümkün değildir. Birçok stratejiyi, eski veya yeni teknolojileri bir arada kullanarak Bulut sisteminin güvenlik problemine çözüm aranmalıdır [11]. Ancak birçok metodu ya da eski ve yeni teknolojilerin aynı sistem üzerinde bütünleşmesi kolay değildir. Böyle sistemlerde taşınabilir olma ve belirli standartlara uyma konularında sorunlar ile karşılaşılması olağandır. Durum böyle olunca, güçlü çözümler için pratikte uygulana bilirliği zayıf kalmaktadır. Geçerli çözümler bulabilmek için uzun vadeli çalışmalar, araştırmalar ve denemeler yapmak gerekir. Güvenlik ve mahremiyet gibi konularda uzun süreli beklemeler ise çok ciddi riskler taşımaktadır. Bu nedenle, ortak alan paylaşımı sağlayan sistemlerin güvenilir olması için uzun süre gerektiren çalışmalar devam ederken, kısa zamanda güvenilir sonuçlar verecek pratik çözümler bulmak gerekir. 2014 yılında yayınlanan [12] çalışmasında güvenliği sağlamak amaçlı SAPA adını verilen kimlik doğrulama üzerine bir protokol tanımlanmış, teorik olarak doğru tasarlandığı gösterilmiş ve Bulut sisteminde bulunan uygulamalar için kullanılabilir olduğu söylenmiştir. Bu çalışmada, şifreleme algoritmaları kullanarak, diğer yaklaşımlardan daha güçlü bir yaklaşım sergilemişlerdir. Ancak bu modellemenin de yine çevrimiçi bir modelleme olduğu aynı zamanda gerçek sistem üzerinde test edilememiş teorik olarak doğru olduğu gösterilen bir modelleme olduğu belirtilmelidir.

Özellikle son zamanlarda üzerinde sıkça çalışılan, Bulut Bilişim'de güvenli iletimi sağlamak için önerilen homomorfik şifreleme

yaklaşımı, kullanıcının Bulut'a iletmek istediği veriyi şifreleme yaklaşımını içermektedir [13],[14]. Bu durum Bulut Bilişim'de güvenlik, gizlilik ve mahremiyet problemlerinin giderilmesi için kullanıcı verisinin şifrelenmesi üzerinden modelleme yapılması gerektiği fikrini desteklemektedir.

4. İleri Çalışmalar ve Öneriler

Veri paylaşımı ya da saklama için Bulut Bilişim kullanan birçok kullanıcı, kullandıkları uygulamaların kendilerine sağladıkları genel ya da özel paylaşım seçeneklerini tıkladıkları zaman bunun gizlilik açısından yeterli olabileceğini sanırken, bir süre Bulut Bilişim üzerinde sakladıkları ve daha sonra silinmesine karar verdikleri verileri, kendileri sistemden sildikten sonra bu verilerin sistemden gerçekten silindiklerinden emin dahi olamazlar.

Bu çalışmada, birçok işlemin yapılmasına olanak sunan Bulut Bilişim'i özel verileri depolama amaçlı kullandığımız zaman, gizlilik, mahremiyet ve verinin korunması açısından neler yapılabilir konusu üzerinde durulmuştur. Konu ile ilgili literatür çalışması yapılmış, bu konuda karşılaşılan sorunları gidermek için önerilen yöntemler incelenmiştir. Genel olarak bu yöntemlerin Bulut Bilişim sistemi içinde olan yani çevrimiçi yöntemler olduğu gözlemlenmiştir. Çok sayıda protokoller tanımlanmış Bulut'un güvenlik önlemleri artırılmaya çalışılmış, şifreleme algoritmaları tasarlanmıştır. Sistemin güvenliğini, sisteme bağlı çözümler arayarak sağlamak gerekli iken sisteme bağlı çözüm arayışları gizlilik için yeterli değildir.

Bu çalışma ile önerilen yöntem ise, çevrimiçi sistem ve çevrimdışı sistemin birlikte düşünülmesi sonucu ortaya çıkmıştır. Öyle ki, Bulut Bilişim'de gizlilik ve güvenilirlik açısından alınan yöntemler kullanıcıya sunulan sistemlerden oluşmaktadır. Diğer bir ifade ile ana aktör Bulut Hesaplama servisleridir. Oysaki sistemin güvenilirliğinden emin olmak isteyen taraf kullanıcıdır. Dolayısı ile bu çalışma ile önerilen yöntem, bir kullanıcının Bulut Bilişim'de bir veri saklama ya da paylaşmak istediğinde, ilgili veriyi Bulut Bilişim sistemini kullanmadan çevrimdışı çalışan bir şifreleme algoritmasından geçirdikten sonra verinin sistemi yüklenmesi olarak özetlenebilir. Bu şifreleme algoritmasından geçen şifrelenmiş veri Bulut Bilişim'de iletilebilecek biçemi kazandıktan sonra iletime hazır hala gelir. Kullanıcının masaüstünde bir kerelik üretilen şifre ile kullanılacak bu veri şifreleme algoritmasının, veri paylaşılması düşünülen kullanıcı veya kullanıcıların da çevrimdışı çalışan masaüstü bilgisayarlarında bulunması gerekir. Böylece Bulut Bilişim'in sağladığı güvenlik hizmetlerine ek olarak böyle bir çözüme gidilmesi en garanti yöntem olacaktır.

Ayrıca önerilerden diğeri ise, Bulut Bilişim'in parçası olan tüm ülkelerde, Hukuksal yaptırımların işlenebilir ve hızlı olması için Bulut Bilişim sistemine gerekli standartların getirilmesine acil olarak ihtiyaç olduğunu belirterek, belirli standartlara uygun Bulut Bilişim sistemlerinin kullanımına destek verilmesidir. Bunlara ek olarak, Hukuksal işlemlerin sürekli değişen sistemlerde yaptırım gücünü koruması için uzman kişilerden yardım alınarak çağa cevap verecek şekilde en güncel yasal düzenlemelerin yapılmasının önemi bir kez daha belirtilmelidir.

Bulut Bilişim'de, verinin mahremiyet, gizlilik prensiplerine uygun bir şekilde ve kişisel verilerin güvenli bir şekilde korunduğundan kesin olarak emin olunamayacağından ötürü çözüm olarak önerilen çevrimdışı veri şifreleme algoritması tasarlanması ileride yapılması planlanan çalışmalar arasında yer almaktadır. Bulut Bilişim'de saklanacak ya da paylaşılacak verilerin bu algoritmadan geçirildikten sonra sisteme yüklenmesi, Bulut Bilişim kullanımı esnasında risk taşıyan konularda kullanıcıların kendilerini daha güvende hissetmelerini sağlayacak, Bulut bilişime azalan güvenin tekrar artmasına yardımcı olacaktır.

Bu çalışma ile Bulut Bilişim sorunlarından olan mahremiyet, gizlilik ve kişisel verilerin

güvenli bir şekilde korunması konusuna farklı bir açıdan bakarak, bahsedilen sorunları gidermek için çözüm önerisinde bulunulmuştur. Böylece, bu konuda çalışan araştırmacılara farklı bir yaklaşım sunulması açısından, bu çalışmanın faydalı olacağı umulmaktadır.

Kaynaklar

[1] Lori, M. "Data security in the world of cloud computing." Co-published by the IEEE Computer And reliability Societies (2009): 61-64.

[2] "US Federal Cloud Computing Market Forecast 2010–2015," tabular analysis, publication: 05/2014.

[3] Nergiz, M. E., Atzori, M., C. Chris, **'**Hiding the presence of individuals from shared databases',SIGMOD '07 Proceedings of the 2007 ACM SIGMOD international conference on Management of data, Pages 665-676.

[4] Rakesh Agrawal and Ramakrishman Srikant, " Privacy- preserving data mining'', In Proc. Of ACM Management of Data (SIGMOD), 2000, PP. 439-450.

[5] Wang, J., Zhao, Y., Jiang, ' Providing Privacy Preserving in Cloud Computing', Test and Measurement, 2009. ICTM '09. International Conference on , Vol.2, 2009,pp 213-216.

[6] Sen, J. (2013). Security and Privacy Issues in Cloud Computing. In Mart´ınez, A. R., Marin-Lopez, R., and Pereniguez-Garcia, F., editors, Architectures and Protocols for Secure Information Technology Infrastructures,
pages 1–45. IGI Global.

[7] Yüksel, H., ' Bulut Bilişim El Kitabı(2012) '
http:// yükselis.wordpress.com ,(2014).

[8] Miranda & Siani, ―A Client-Based Privacy Manager for Cloud
Computing‖, COMSWARE'09, 2009, Dublin, Ireland.

[9] F.B. Shaikh and S. Haider, "Security Threats in Cloud
Computing", 6th International Conference on Internet Technology and Secured Transactions, IEEE, Dec 2011, pp. 214-219.

[10] Wassim Itani, Ayman Kayssi, Ali Chehab, "Privacy as a Service-
Privacy-Aware Data Storage and Processing in Cloud Computing
Architectures", IEEE Conference-2009.pp. 711-716.

[11] W. Liu, "Research on cloud computing security problem and strategy", in
Consumer Electronics, Communications and Networks (CECNet), 2012
2nd International Conference on, pp. 1216 – 1219, april 2012.

[12] Ning, H. , Xiong, Q. , Yang, L.T., "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", Parallel and Distributed Systems, IEEE Transactions on (Volume:PP , Issue: 99), pp.1., (2014).

[13] Zhao, F., Chao, L., Liu, C., F., "A cloud computing security solution based on fully homomorphic encryption", Advanced Communication Technology (ICACT), 2014 16th International Conference on, PP. 485-488, Feb. 2014.

[14] For more information about Homomorphic Encryption
http://phys.org/news/2013-06-cloud-algorithm-majorproblem- homomorphic.html