ÖZET

GÜVENLİ VE BAĞIMSIZ VERİ DEPOLAMA SİSTEMİ

Bu buluş, kritik verilere sahip olan kurumların veya güvenli bir şekilde çeşitli verilerini depolamak isteyen bireylerin, blok zincirleme (Blockchain) ve Merkle ağaçları kullanılarak depolanan verilerin merkezi olmayan ve dağıtılmış biçimde yüksek kullanılabilirlik ve düşük maliyetle sunulmasını sağlayan bir sistem (8) ile ilgilidir.

İSTEMLER

1. Depolanmak istenen verilerin güvenli bir şekilde dağıtılmasını, şifrelenmesini, parçalanmasını, birleştirilmesini ve depolanmasını sağlayan bir sistem olup, özelliği;

-verilerin bütün lojistik, hashing ve sistem denetimini yapan en az bir Yönetici Birim (3),

-Yönetici Birim (3) tarafından yönetilen, veriyi modern şifreleme algoritmalarıyla şifreleyen, şifreleme için gereken anahtar üretimini yapan en az bir Şifreleme Birimi (5),

-Şifreleme Birimi (5) için gereken bütün entropi gereksinimlerini, gürültü oluşturucu donanımlar veya sistemde bulunan donanımların sabit olmayan kod çalıştırma sürelerini baz alarak entropi havuzunu dolduran en az bir Entropi Birimi (7),

-veri depolama isteğini ileten ve sistemin (8) kullanıcı arayüzü olarak işlev görecek en az bir Uçbirim (2),

-depolanacak olan verinin peer-to-peer blockchain ağına (9) aktarılmadan önce tutulacağı en az bir Geçici Depolama Birimi (4),

-güvenli bir şekilde şifrelenen ve hashlerin Merkle DAG ağacı çıkarılan verinin adresleme bilgisinin tutulduğu en az bir Adres Tutma Birimi (6) ve

-Yönetici Birime (3) uçbirim tarafından ulaştırılan verinin, parçalanıp, şifrelenip, peer-to-peer ağa dağıtılarak verinin saklanması ile karakterize edilmesidir.

2. Kullanıcı verilerinin Geçici Depolama Birimi (4) kullanılmadan, direkt olarak şifreleme, hashleme ve dağıtma işlevleri ile karakterize edilen İstem 1'deki gibi bir sistem (8).

3. Herhangi bir verinin (1) dağıtık bir şekilde sunulması işlevini yerine getirecek, peer-to-peer ağ (9) üstünden depolama teşvik edilerek sunulması ile karakterize edilen İstem 1 veya İstem 2'deki gibi bir sistem (8).

4. Kullanıcıların, depolanan verileri, sığınak sistemden (8) bağımsız bir şekilde veriye özel adres kullanarak geri çağırabilmeleri ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

5. Herhangi bir verinin (1) hashlenerek Merkle DAG ağacına dönüştürülmesi ve bu ağacın peer-to-peer bir ağa dağıtılarak verinin depolanması ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

6. Herhangi bir verinin (1) şifrelemeye tabi tutulmadan, sadece hashlenerek ve adreslenerek özel bir ağa dağıtılarak verinin depolanması ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

7. Herhangi bir şifreleme, entropi, parçalama işlemi yapmadan veya bu görevleri yerine getiren birimleri kullanmadan, verinin (1) peer-to-peer ağı üstünden, Merkle DAG ağacından elde edilen adreslerin dağıtılması ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

8. Sistemin kurulmasında aktif görev alan işletmelerin sonradan dahil olan firmalardan alınan aylık veya yıllık abonelik üzerinden gelir elde edilmesini sağlayan Yönetici Birim (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

9. Gelir modellemesinde kullanıcıların dahil oldukları sistemde Platform as a Service hizmeti üzerinden gelir kazanmalarını sağlayan Yönetici Birim (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

10. Sisteme dahil olmayan işletmelerin ihtiyaçlarını karşılayacak hizmetlerin verilmesi üzerinden gelir elde etmesini sağlayan Yönetici Birim (3) ile karakterize edilen yukarıdaki istemlerden herhangi birindeki gibi bir sistem (8).

TARİFNAME

GÜVENLİ VE BAĞIMSIZ VERİ DEPOLAMA SİSTEMİ

TEKNİK ALAN

Buluş, kritik verilere sahip olan kurumların veya güvenli bir şekilde çeşitli verilerini depolamak isteyen bireylerin, blok zincirleme (Blockchain) ve Merkle ağaçları kullanılarak depolanan verilerin merkezi olmayan ve dağıtılmış biçimde yüksek kullanılabilirlik ve düşük maliyetle sunulmasını sağlayan bir sistem ile ilgilidir.

TEKNİĞİN BİLİNEN DURUMU

Geleneksel veri depolama, arşivleme, soğuk-depolama ve bulut sistemlerinde veri, merkezi olarak bir yerde tutulmaktadır. Bunun yanında getirdiği, acil durum, doğal afet, felaket, ağ kayıpları ve otoriter kontrol gibi dezavantajlı durumların giderilmesi amacıyla teknikte bazı denetim ve dağıtım mekanizmaları halihazırda bulunmaktadır. Bu sistemlere örnek olarak çoklu dağıtıma sahip veri merkezleri verilebilir. US8676760B2 sayılı Birleşik Devletler patent dokümanında bahsi geçen buluş veri merkezleri arasında bir protokol oluşturup, tutulacak veriyi ana ve yardımcı sunuculara bölüştürme ve dağıtma yönteminden bahsetmektedir.

Tekniğin bilinen durumuna US5550976A sayılı Birleşik Devletler patent dokümanı örnek verilebilir. US5550976A sayılı Birleşik Devletler patent dokümanında bahsi geçen sistem, eşler arası aktarım teknolojisini kullanarak, verilerin merkezi olmayan bir biçimde depolanması, aktarılması ve analiz fonksiyonlarından bahsetmektedir. Ancak söz konusu doküman, verinin bütünlüğü ve güvenliğini sağlayan bir yapılandırmayı anlatmamaktadır.

BULUŞUN TANIMI

Mevcut buluş yukarıda bahsedilen dezavantajları ortadan kaldırmak ve ilgili teknik alana yeni avantajlar getirmek üzere geliştirilmiş bir sistemle ilgilidir.

Buluşun amacı, özellikle depolanan verinin güvenliği, taşınması ve depolama maliyetleri üstünedir. Buluş, depolanacak olan verinin, parçalar halinde hashlenerek, Merkle ağacı şeklinde kök ve alt dallar olmak üzere tercüme edilip, blok zincirleme yapılarak sadece kök hashin depolanmasıyla veriyi saklar. Buluş böylece, depolama masraflarını azaltır ve verinin dünya üzerinde herhangi bir yerde, sadece adres sağlanarak tekrar oluşturulup kullanılabilmesine olanak sağlar. Verinin güvenliğini sağlamak için, verinin sisteme aktarılmadan önce şifrelenmesi tercih edilir.

Buluşun bir başka amacı, büyük veya küçük ölçekli verilerin, merkezi olmayan biçimde dağıtılarak, güvenli bir şekilde saklanmasına olanak sağlamaktır. Sistemdeki verilerin tabi tutulduğu modern şifreleme yöntemleri, hem kurumların kritik ve hayati verilerinin (gizli veri, teknik veriler, muhasebe vb.), hem de kişilerin saklamak istediği her türlü verinin güvenli ve güvenilir bir biçimde depolanmasını sağlamaktadır. Sistemin verileri dağıtık bir biçimde tutması, olası bir sistem arızası, felaket veya güvenlik sorunu durumunda verilerin güvende kalmasını garantiye alır.

Buluşun bir diğer amacı, Verinin bütünlüğünün bozulmadan, sadece veri sahibi tarafından erişilebilir bir şekilde saklanmasıdır. Ayrıca verinin merkezi olmayıp, teşvik edilerek dağıtılmış olan dünya çapında peer-to-peer blockchain ağına depolanması, buluşun herhangi bir çevrimdışı durumunda bile verileri sunabilmesine olanak sağlar.

Çizimler

Yukarıda kısaca özetlenen ve aşağıda daha detaylı ele alınan mevcut buluşun uygulamaları, buluşun ekteki çizimlerde betimlenen örnek uygulamalarına başvurarak anlaşılabilir. Ancak ekteki çizimlerin yalnızca bu buluşun tipik uygulamalarını betimlediğini ve buluş, bu nedenle, diğer eşit derecece etkili uygulamalara izin verebileceği için, kapsamını sınırladığının varsayılmayacağını belirtmek gerekir.

Şekil 1, Buluşa ait bir yapılandırmanın şematik görünümü.
Şekil 2, Buluşun Blok Zincirleme yöntemi olarak kullanacağı örnek Merkle ağacı.

Anlaşılmayı kolaylaştırmak adına, şekillerde ortak olan özdeş elemanları belirtmek için, mümkün hallerde özdeş referans numaraları kullanılmıştır. Şekiller ölçekli çizilmemiştir ve açıklık için basitleştirilebilir. Bir uygulamanın elemanları ve özelliklerinin daha fazla açıklama lüzum olmaksızın diğer uygulamalara faydalı bir biçimde dâhil edilebileceği düşünülmektedir.

Çizimlerdeki Detayların Açıklanması

Şekillerde gösterilen referans numaralarının karşılıkları aşağıda verilmiştir.

1. Depolanmak İstenen Veri
2. Uçbirim
3. Yönetici Birim
4. Geçici Depolama Birimi
5. Şifreleme Birimi
6. Adres Tutma Birimi
7. İzole Entropi Birimi
8. Sığınak Sistem
9. Peer-to-peer ve Blockchain Ağı

BULUŞUN DETAYLI AÇIKLANMASI

Bu detaylı açıklamada buluş konusu sistem yapılanmasının tercih edilen alternatifleri, sadece konunun daha iyi anlaşılmasına yönelik olarak ve hiç bir sınırlayıcı etki oluşturmayacak şekilde açıklanmaktadır.

Buluşa konu sistemin çalışma yöntemi, depolanacak verinin (1), AES-128 ile şifrelendikten sonra xxHash algoritmasıyla hashlenerek sisteme gönderilmesiyle başlamaktadır. Buluş, verinin multihash ve veri uzunluğu bilgilerini kullanarak yönlü asiklik grafik (Merkle DAG) oluşturur. Bu ağaç, verinin saklandığı noktayı adres göstermenin yanı sıra, verinin değiştirilmeden saklandığını, bütünlüğünün korunduğunu doğrular. Veride yapılacak herhangi bir değişiklik, bütün ağacın değişmesine sebep olacağından, değişiklikler sonucu oluşan adres, başka bir dosyayı adresleyecektir. Sisteme yüklenen ve depolanmak istenen dosyalar (1),

hash işlemleri tamamlandıktan sonra, optimum 30 parçaya bölünür ve bütün parçalar, Peer-to-peer bir ağ (9) üstünde dağıtılır. Dağıtılan parçalar şifreli olduğu için, yüklenen sunucu üstünde güven faktörüne bakılmaz. Daha sonra dosya geri çağrılmak istendiğinde, parçalardan herhangi 10 tanesi, Reed-solomon algoritmasıyla birleştirilerek orijinal şifreli dosya elde edilebilir.

Buluşun, bütün yönlendirme, dağıtma ve birleştirme işlemleri Kubernetes platformu tarafından yönetilen, 6 çekirdek sunucu tarafından gerçekleştirilir. Bu sisteme “sığınak” (8) denmektedir. Sığınak sistem (8), geçici depolama birimi (4), adres tutma birimi (6), şifreleme birimi (5), pseudo-rastgele numara oluşturucu (PRNG) entropi birimi (7), yönetici birim (3) ve uçbirim (2) olarak katmanlara ayrılmıştır. Sığınak sisteme (8) güvenli bir kanal ile (HTTPS/TLS) gönderilen veri, uçbirime (2) ulaştıktan sonra, xxHash değerleri karşılaştırılır ve Yönetici Birim (3) tarafından Geçici Depolama Birimine (4) aktarılır. Eğer Geçici Depolama Birimine (4) aktarılan veri, ham veri ise, ya da şifrelenme prosedürlerinde değişiklik yapıldıysa, Şifreleme Birimi (5) tarafından şifrelenir.

Veriye veya kullanıcıya özel biçimde asimetrik şifreleme anahtarı veya GPG oluşturularak, anahtar depolanmadan kullanıcıya güvenli kanal aracılığı ile aktarılır. İsteğe bağlı olarak, buluş, kullanıcı tarafından sağlanan GPG Public anahtarını kullanarak şifreleme sağlayabilir. Şifreleme Biriminin (5) bağlı olduğu tek birim Entropi Birimidir (7). Entropi Birimi (7) anahtar oluşturma sırasında harcanacak olan donanımsal entropinin kabul edilebilir seviyelerde tutulmasını sağlamak ve bunu gözetmekle görevlidir. Entropinin azaldığı durumlarda, HAVEGED ve/veya donanımsal gürültü oluşturucular kullanılarak entropi havuzu doldurulur. Bu sayede tahmin edilebilir anahtarların oluşturulması önlenir.

Geçici Depolama Biriminde (4) tutulan veriler, Yönetici Birim (3) tarafından multihash alınarak, Merkle ağacına dönüştürülüp parçalanır ve DHT ile Peer-to-peer ağa (9) dağıtılır. Blok zincirleme tekniği olarak Merkle ağacı kullanılır. Veri parça parça hashlenerek, ağacın üst katmanlarına doğru yönelir. En üst noktaya gelindiğinde, verinin multihash adresi, Adres Tutma Biriminde (6) saklanır. Şekil 2

üstünde örnek Merkle Ağacı verilmiştir. Dağıtılan veri büyüklüğüne göre bir süre saklanmaya devam edilir ve daha sonra Geçici Depolama Biriminden (4) silinir. Katmanlar arasındaki iletişim, internet ağından bağımsız, iç ağ içinde TCP protokolü ile gerçekleştirilir. Sistemin (8) Şekil 1 üstünde belirtilen çift yönlü bağlantılar, veri alışverişini, durum raporlarını ve komut iletimi işlemlerini sağlar. Sığınak sistemden (8) veri geri çağrıldığında, Yönetici Birim (3), Adres Tutma Birimine (6) ulaşarak, ya da direkt adres sağlanıyorsa, Peer-to-peer ağına (9) bağlanarak veri parçalarını Geçici Depolama Birimine (4) aktarır. Reed-Solomon algoritmasıyla birleştirilen parçalar, güvenli bir kanal ile istemci noktaya sunulur. Geliştirilen sistemin çıktıları ve yönetimi, Uçbirim (2) tarafından sağlanan arayüz ile sağlanmaktadır.

Buluşun bir yapılandırılmasında veri şifreleme işlemleri, veri buluşa aktarılmadan önce yapılmaktadır.

Buluşun bir yapılandırmasında veri şifreleme işlemleri, veri buluşa güvenli bir kanal ile aktarıldıktan sonra yapılmaktadır.

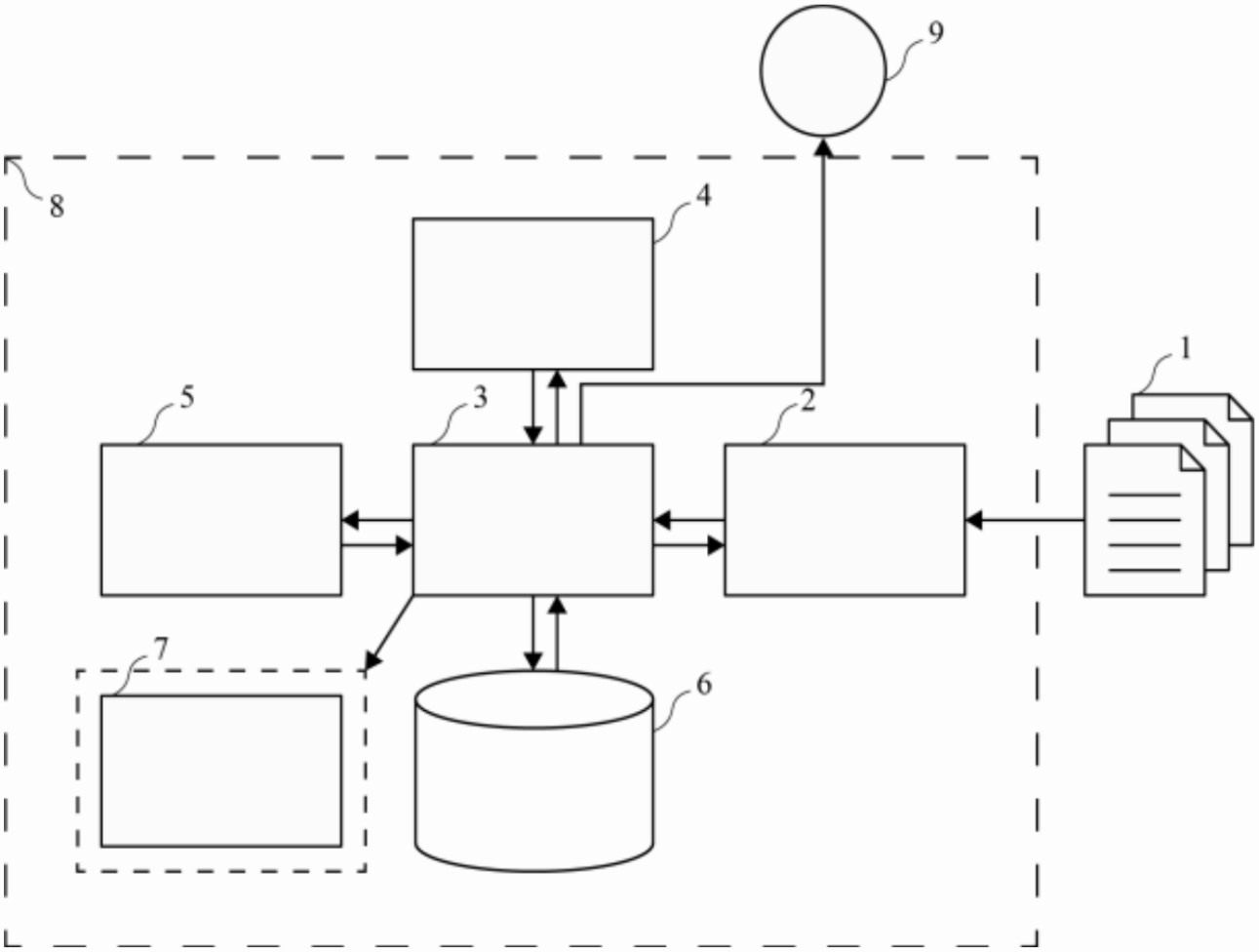
Tercih edilen uygulamada Uçbirime (2) erişim, dosya sahipliğini doğrulayan kullanıcı tarafından yapılmaktadır. Bu doğrulama işlemi, Adres Tutma Birimi (6) ile ilişkili bir kullanıcı denetim birimi ile yapılabilir.

Tercih edilen uygulamada Peer-to-peer ağda (9) yayılma hızını ve tutuculuk oranını arttırmak için, depolamayı ödüllendiren ve depolama kontratları sağlayan, dosya aktarım ve depolamasının doğrulanabildiği bir teşvik sistemi kullanılmalıdır.
Bu temel kavramlar etrafında, bir güvenli ve bağımsız veri depolama sisteminin (1) çok çeşitli uygulamalarının geliştirilmesi mümkün olup, buluş burada açıklanan örneklerle sınırlandırılamaz, esas olarak istemlerde belirtildiği gibidir.

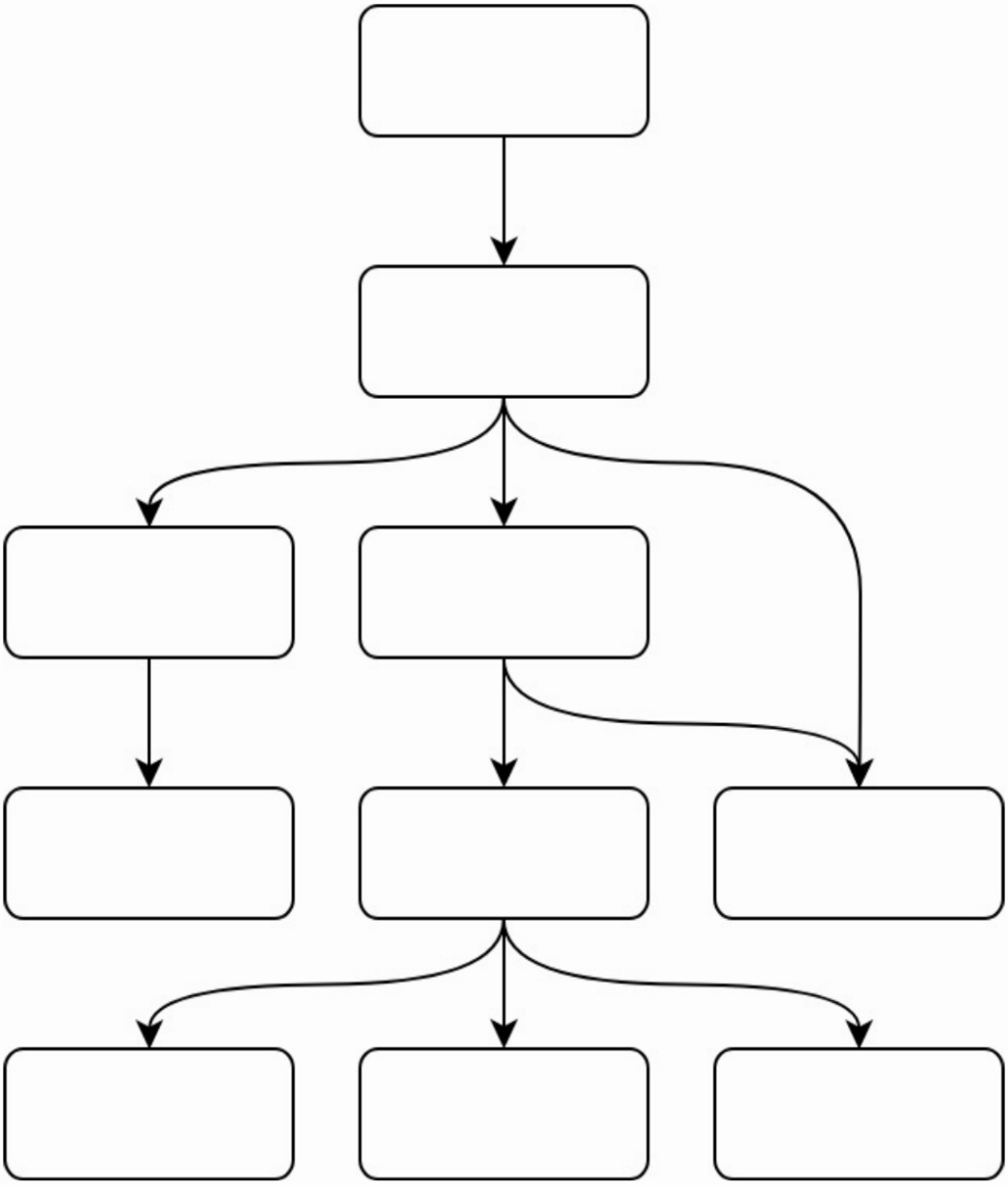
Buluş konusu sistem (8), büyük veya küçük ölçekli verilerin, merkezi olmayan biçimde dağıtılarak, güvenli bir şekilde saklanmasına olanak sağlar. Sistemdeki (8) verilerin tabi tutulduğu modern şifreleme yöntemleri, hem kurumların kritik ve hayati verilerinin (gizli veri, teknik veriler, muhasebe vb.), hem de kişilerin saklamak

istediği her türlü verinin güvenli ve güvenilir bir biçimde depolanmasını sağlamaktadır. Sistemin (8) verileri dağıtık bir biçimde tutması, olası bir sistem arızası, felaket veya güvenlik sorunu durumunda verilerin güvende kalmasını garantiye alır.

Buluşta alternatif olarak kullanılan çekirdek sunucuları kullanmadan, aynı işlevi yerine getiren, kullanıcı tarafında çalışan bir sistem yapılabilir. Ayrıca buluşta kullanılan şifreleme ve hashleme yöntemleri, daha hızlı alternatifleriyle değiştirilip, büyük ölçekli verilerin ağa dahil edilme süresi de hızlandırılabilir.



Şekil 1



Şekil 2