ÖZET

BİR GÜVENİLİR İLETİŞİM METODU

Buluş konusu yöntem, iletişim sağlamakta kullanılan bileşenleri (bellek, klavye, mikrofon, kullanıcı arayüzü vb.) kontrol eden yazılım birimlerinin güvenilir işletim ortamı [102] çağırılması ile bu bileşenlerden gelen verilerin güvenilir işletim ortamı [102] şifrelenmesi sonucu oluşan şifreli verinin tercihen normal yollarla zengin ortam [103] uygulamasına gönderilmesi, zengin ortam [103] uygulamasının bu veriyi kendi protokolleri/yöntemleri ile karşı tarafa iletmesi ve karşı tarafta yine güvenilir işletim ortamı [102] açılarak kullanıcıya sunulması yoluyla güvenli bir iletişim sağlanması ile ilgilidir.

İSTEMLER

1- Buluş konusu yöntem bir iletişim uygulamasının [101] güvenilir işletim ortamı [102] yoluyla güvenli iletişim sağlaması için bir yöntem olup özelliği;

a. Zengin ortamda [103] çalışan iletişim uygulaması [101] içinden bir çağırılan girdi elemanları [108] yoluyla göndericiden [104] girdiyi güvenilir işletim ortamı [102] içinde alması,

b. Güvenilir işletim ortamı [102] içinde alınan girdinin yine güvenilir işletim ortamı [102] içinde şifrelemeden [107] geçirilmesi,

c. Güvenilir işletim ortamı [102] dışına şifreli olarak çıkarılması ve zengin ortam [103] içinde çalışan iletişim uygulamasına [101] şifreli olarak aktarılması ve iletişim uygulanması tarafından normal yollarla aktarılması,

d. Alıcıya [105] ulaşan mesajın şifreli olarak izlenebilmesi, izlenen şifreli mesajın diğerlerinden çeşitli yollarla ayırt edilebilecek biçimde gösterilmesi ve güvenilir işletim ortamı [102] içine alınarak şifrelemesinin [107] çözülmesi,

e. Şifrelemesi [107] çözülen mesajın güvenilir işletim ortamından [102] çağırılan güvenli kullanıcı arayüzü [110] ile kullanıcıya ulaştırılması ile karakterize edilmesidir.

2- İstem 1'de bahsedilen yöntem olup özelliği, zengin ortam [103] ile güvenilir işletim ortamı [102] arasında her iki yönlü geçişlerin bir yetkilendirme [106] yoluyla yapılması ve bu yetkilendirme işleminin güvenilir işletim ortamı [102] içerisinde yapılması ile karakterize edilmesidir.

3- İstem 2'de bahsedilen yöntem olup, güvenli kullanıcı arayüzünün [110] yazı da dahil olmak üzere görsel unsurlar içermesi durumunda ekranın tamamını veya bir bölümünü kapsayacak biçimde oluşturulması ile karakterize edilmesidir.

4- Buluş konusu ürün bir mobil veya sabit bilgi işlem cihazları için bir yazılım veya yazılımın yüklendiği veya işletildiği bir ortam olup özelliği;

a. Zengin ortamda [103] çalışan iletişim uygulaması [101] içinden bir çağırılan girdi elemanları [108] yoluyla göndericiden [104] girdiyi güvenilir işletim ortamı [102] içinde alması,

b. Güvenilir işletim ortamı [102] içinde alınan girdinin yine güvenilir işletim ortamı [102] içinde şifrelemeden [107] geçirilmesi,

c. Güvenilir işletim ortamı [102] dışına şifreli olarak çıkarılması ve zengin ortam [103] içinde çalışan iletişim uygulamasına [101] şifreli olarak aktarılması ve iletişim uygulanması tarafından normal yollarla aktarılması,

d. Alıcıya [105] ulaşan mesajın şifreli olarak izlenebilmesi, izlenen şifreli mesajın diğerlerinden çeşitli yollarla ayırt edilebilecek biçimde gösterilmesi ve güvenilir işletim ortamı [102] içine alınarak şifrelemesinin [107] çözülmesi,

e. Şifrelemesi [107] çözülen mesajın güvenilir işletim ortamı [102] çağırılan çıktı elemanının [109] tamamını veya bir bölümünü kaplayan güvenli kullanıcı arayüzü [110] ile kullanıcıya ulaştırılması ile karakterize edilmesidir.

BİR GÜVENİLİR İLETİŞİM METODU

TEKNİK ALAN

Buluş konusu ürün yazılımlar yoluyla haberleşmedeki güvenlik sorunu ile ilgilidir. Daha spesifik olarak buluş konusu ürün iki cihaz arasında bir uygulama yoluyla aktarılan verinin güvenilir işletim ortamı [102] içerisinde şifrelenerek aktarılması ile ilgilidir.

TEKNİĞİN BİLİNEN DURUMU

Günümüzde bir cihaz üzerinde kullanıcılar birden fazla uygulama kullanmaktadırlar. Bu uygulamalar cihazlar (masaüstü bilgisayarlar, taşınabilir bilgisayarlar, mobil cihazlar, cep telefonları, tabletler, akıllı cihazlar vb.) üzerinde çalışırken çeşitli girdi elemanlarını [108] (kamera, mikrofon, klavye, çeşitli sensörler, vb.) ve çıktı elemanlarını [109] (ekran, vb.) kullanırlar. Bu tip uygulamalar internet yoluyla erişilen çeşitli uygulama marketlerinden edinilebileceği gibi, doğrudan cihaz üzerine kurarak da yerleştirilebilirler. Dahası, cihaz üreticileri cihazlarını çok katmanlı işletim sistemleri ile piyasaya sürmektedirler; bunlara örnek olarak Linux™, Android™, IOS™ ve benzeri ticari ürünler verilebilir. Bu gibi çok katmanlı işletim sistemleri çeşitli yetenekler ile gelmekte ve uygulamaların kurulmasına olanak tanımaktadırlar.

Söz konusu cihazlar üzerindeki birçok uygulama hassas, özel ve(ya) değerli bilgiler içermektedir. Bu bilgilerin güvenli olarak saklanması, tutulması ve ihtiyaç halinde iletilmesi bir ihtiyaç olarak ortaya çıkmaktadır; bankacılık uygulamaları, iletişim uygulamaları, içerik uygulamaları ve benzeri uygulamalar bunlara örnek olarak verilebilir. Bu hassas ve gizli bilgileri içeren ve işleyen uygulamaların işletim sistemlerinde çalıştığının farkında olan işletim sistemi üreticileri donanım ve işletim sistemlerini içerisinde çeşitli güvenlik yöntemlerinin uygulanmasına izin verecek biçimde üretmektedirler.

Bunlardan biri, özellikle mobil cihazlarda çalışması için tasarlanmış olan güvenilir işletim ortamı [102] teknolojisidir. Buna göre cihazlardaki yazılım ve donanım, üzerinde çalışan uygulamaların tamamını veya bir bölümünü çalıştırmak üzere bir güvenilir işletim ortamı [102] oluşturulur. Bir güvenilir işletim ortamı [102], işletim sistemi ve donanımın üzerinde çalışan uygulamaların güvenli çalışması için oluşturulmuş bir alandır. Güvenilir işletim ortamı [102] uygulaması, sadece kendi içerisinde çalışmak için konfigüre edilmiş unsurları güvenli bir bölgede çalıştırarak istenmeyen erişimi önler. Güvenli işletim alanı içerisinde çalışmak için konfigüre edilmemiş uygulamalar veya bileşenler bu güvenlik önlemi dışında zengin ortamda [103] çalışmalarına devam ederler. Burada zengin ortam [103] ile anlatılmak istenen, cihazın güvenilir işletim ortamı [102] dışında kalan bölümlerinin tamamıdır. Kullanıcı bu zengin ortamda [103] çalışan uygulamaların çalışması açısından herhangi bir fark görmez. Güvenilir işletim ortamı [102] içerisinde çalışan uygulamaların güvenilir işletim ortamı [102] içerisinde, dışında çalışan uygulamaların zengin ortamda [103] çalışacağından kasıt esas olarak budur.

Bir güvenilir işletim ortamı [102] güvenli elemanlar oluşturarak işlevini yerine getirir. Bu güvenli elemanlar işlemci, hafıza elemanları, gömülü elemanlar ve sair bileşenler olabilir. Bu güvenilir işletim ortamı [102] sanallaştırma teknolojileri ile oluşturabileceği gibi, Trustzone™ üzerinde çalışan TEE™ gibi protokoller veya standartlar çerçevesinde oluşturulmuş mimariler vasıtasıyla da oluşturabilir. Cihaz üzerinde bulunan donanım bileşenleri çağırmak için kullanılan sürücüler bu güvenilir işletim ortamı [102] içinde bulunabileceği gibi, sonradan da eklenebilir. Kullanıcıya görüntü sağlayan arayüzlerin tamamının veya bir bölümünün güvenilir işletim ortamı [102] çalıştırılması durumunda buna güvenilir kullanıcı arayüzü [110] denir. Bu durumda güvenilir kullanıcı arayüzüne [110] (örneğin ekran) cihaza yüklü başka bir uygulama tarafından erişilmesi olanaksız hale gelir. Burada esas olan cihazın kullandığı kaynakların her birinin tamamının veya bir bölümünün

kısıtlı zamanlar için zengin ortamda [103] yer alan tüm unsurlara erişime kapatılması ve sadece güvenilir işletim ortamında [102] çalışmasına izin verilen uygulamalar tarafından kullanılmasıdır. Burada güvenilir işletim ortamı [102] sağlayan mimariler, standartlar ve ürünler değişiklik gösterebilir. Esas olan güvenilir işletim ortamının [102] tüm uygulamaların erişimine kapalı olması, sadece özel olarak bu alanda çalıştırılan uygulamaların güvenilir işletim ortamından [102] alınan kaynaklara erişiminin sağlanmasıdır.

Tekniğin bilinen durumunda güvenilir işletim ortamı [102] ile haberleşme alanında birçok çözüm bulunmasına karşın, mevcut iletişim protokollerin ve uygulamaların kullanıldığı bir çözüme rastlanamamıştır.

BULUŞUN KISA AÇIKLAMASI

Buluş konusu yöntem, iletişim sağlamakta kullanılan bileşenleri (bellek, klavye, mikrofon, kullanıcı arayüzü vb.) kontrol eden yazılım birimlerinin güvenilir işletim ortamından [102] çağırılması ile bu bileşenlerden gelen verilerin güvenilir işletim ortamında [102] şifrelenmesi sonucu oluşan şifreli verinin tercihen normal yollarla zengin ortam [103] uygulamasına gönderilmesi, zengin ortam [103] uygulamasının bu veriyi kendi protokolleri/yöntemleri ile karşı tarafa iletmesi ve karşı tarafta yine güvenilir işletim ortamında [102] açılarak kullanıcıya sunulması yoluyla güvenli bir iletişim sağlanması ile ilgilidir.

BULUŞUN AYRINTILI AÇIKLAMASI

Buluş konusu ürün iletişim uygulamaları [101] üzerinde yapılan değişikliklerle çalışan bir güvenlik yöntemidir. Buna göre bir haberleşme uygulamasında eklenen bir seçenek ile yetkilendirmeden [106] geçen gönderici [104] iletişim uygulamasının [101] belli alanlarından (yazı penceresi, vb.) ve bu alanlara etki eden donanımlardan (mikrofon, klavye, ekran, vb.) en az birer tanesini güvenilir işletim ortamından [102] çağırır. Bu seçim yapılıp da uygulamanın

belli alanları ve bu alana girdi sağlayan girdi elamanları [108] güvenilir işletim ortamından [102] çağırıldıktan taşındıktan sonra, güvenilir işletim ortamına [102] dışarıdan erişim kısıtlanmış olur. Bu çağırma işleminden sonra kullanıcı iletişim uygulamasına [101] girdi sağladığı şekilde güvenilir işletim ortamında [102] girdiyi sağlar. Gönderici tarafından güvenilir işletim ortamında [102] sağlanan girdiler alınır ve yine güvenilir işletim ortamı [102] içerisinde şifrelemeye [107] tabi tutulur. Şifrelemenin [107] ardından varsa güvenilir işletim ortamı [102] içerisindeki kayıt silinerek yalnızca şifrelenmiş kayıt zengin ortam [103] veya çağıran uygulamaya taşınır. Bundan sonra, kayıt iletişim uygulamasının [101] bilinen yöntemleri ile taşınır ve aktarılır. Buluş konusu yöntem iletişim uygulamasının [101] aktarma sırasında yaptığı işlemlerde herhangi bir değişiklik öngörmemektedir.

Güvenilir işletim ortamında [102] alınan, şifrelenen ve zengin ortam [103] aktarılan mesaj, iletişim uygulaması [101] tarafından aktarılması istenen alıcıya [105] aktarılır. Bu adımın ardından alıcıya [105] aktarılan mesaj şifreli olarak iletişim uygulaması [101]içinde görülür. Burada tercihen mesajı diğerlerinden ayıracak bir görsel ve(ya) işitsel unsur (örneğin kilit biçiminde bir görsel unsur, bir metin öğesi, spesifik bir ses tonu veya bunlardan birkaçı) kullanılır ve bu görsel unsura basıldığında bir yetkilendirme [106] ortamı açılır. Bu yetkilendirme [106] ortamında teknikte kullanılan birçok yolla yetkilendirme [106] yapılabilir; bir pencere içinde şifre girilmesi, bir donanım ile parmak izi okunması veya davranışsal analitik yöntemler ile yetkilendirme [106] bunlara örnek olarak verilebilir.

Tercihen güvenilir işletim ortamında [102] sağlanan bir yetkilendirmenin [106] ardından iletişim uygulaması [101] içinde gönderici [104] tarafından gönderilen mesajın şifreli hali güvenilir işletim ortamında [102] alınmış bir hafıza elemanına kopyalanır ve güvenilir işletim ortamı [102] içinde bilinen anahtar ile şifresi çözülerek ekranın tamamını veya bir kısmını kaplayan bir güvenilir kullanıcı arayüzü [110] içinde çıktı elemanı [110] üzerinde alıcıya [105] gösterilir, dinletilir veya oynatılır.

Alıcıda [105] buluş konusu ürünün çalışır durumda olmaması (örneğin yüklenmemiş olması) durumunda ise alıcı yalnızca gönderilen mesajı şifreli olarak ve herhangi bir anlam veremediği mesaj olarak görecektir. Buluş konusu ürünün yüklü olduğu ve çeşitli sebeplerle geçici veya kalıcı olarak çalıştırılmadığı durumlarda da gönderilen mesaj şifreli olarak görünür ve kullanıcı tarafından anlam verilemeyen bir karakterler dizisi olarak izlenebilir. Gönderilen mesajın yazılı mesaj değil, ses veya görüntü olması durumunda da şifreli bir biçimde görüntülenecek ve tercihen gönderilen türe ait fakat anlam ihtiva etmeyen bir mesaj olarak algılanacaktır.

Buluş konusu ürün bu haliyle iletişim uygulamaların [101] şifreleme ve aktarım protokollerine ek olarak gönderilen ve alınan mesajların bir güvenilir işletim ortamında [102] şifrelenmesi [107] ve şifrelerinin açılması ile ilgilidir. Bu işlemlerin gerçekleştiği hafıza ve işlemci alanları ile bu işlemlere aracılık eden girdi elemanları [108] ve çıktı elemanları [109] güvenilir işletim ortamı [102] içinden çağırılır ve işlenir ve iki yönlü görüntüler ekranın tamamını veya bir bölümünü kapsayan bir güvenli kullanıcı arayüzü [110] içinde gösterilir.

Böylelikle buluş konusu ürün dışından alınan veya gönderilen mesajlara erişim tamamen kısıtlanmış olur.

Teknikte uzman bir kişi kolaylıkla güvenilir işletim ortamından [102] çağırma işlemi yapabildiğinden bu işlemlerin detaylarına tarifname boyunca yer verilmemiştir. Benzer biçimde teknikte uzman bir kişi bir mesajın şifrelenmesi [107] ve bu şifrenin açılması işlemlerine hakim olduğundan ve bunlarla ilgili teknikte bilinen birçok yol ve yöntem olduğundan, bu işlemlerin detaylarına da tarifname boyunca değinilmemiştir.

Tarifname ekinde verilen çizimlerin açıklamaları şöyledir;

Çizim 1, Buluş konusu yöntemin göndericideki [107] uygulama esaslarının şematik gösterimidir. Buna göre mesajlaşmayı sağlayan uygulamanın bir bölümü zengin ortam [103] çalışmasına devam ederken, sadece kullanıcının girdi oluşturmasını sağlayan girdi elemanları

[108] güvenilir işletim ortamı [102] içine alınır. Bunun dışında mesajlaşma uygulaması normal işlevlerini yerine getirmeye devam eder. Bu esnada güvenilir işletim ortamında [102] bulunan unsurlar tarafından alınan mesaj, yine güvenilir işletim ortamı [102] içinde şifrelenir [107] ve şifreli olarak zengin ortama [103] taşınır. Zengin ortama [103] taşınan şifrelenmiş [107] mesaj, yine mesajlaşma uygulamasının rutin işlemleri ve protokolleri yoluyla (bunlardan biri yine şifreleme olabilir) alıcıya [105] aktarılır.

Çizim 2, Buluş konusu yöntemin alıcıdaki [105] uygulama esaslarının şematik gösterimidir. Buna göre şifreli olarak gelen mesaj şifreli haliyle iletişim uygulaması [101] içinde gösterilir ve güvenilir işletim ortamına [102] geçiş kullanıcıya için görsel olarak bir seçenek sunulur. Bu görsel seçeneğin seçilmesinin ardından bir yetkilendirme [106] işlemi uygulanır ve mesajın şifresi güvenilir işletim ortamı [102] içinde yer alan bilgiler ve işlemler ile açılır. Bunun ardından açılan mesaj ekranın tamamını veya bir bölümünü kapsayan bir güvenli kullanıcı arayüzü [110] içinde gösterilir.

Çizimlerde belirtilen referans numaralarının açıklamaları aşağıdaki gibidir.

101- İletişim uygulaması: Kullanıcı tarafından iletişim için kullanılan, yazılı, sesli, görüntülü mesajları veya dosyaları göndericiden [104] alıcıya aktaran uygulamadır. Cihazın işletim sistemi üzerinde çalışır ve kendine has aktarım, şifreleme, onay, ve benzeri protokolleri mevcuttur. Buluş konusu yöntem, bu protokollere dahil olmaksızın bir güvenli iletişim yöntemidir.

102- Güvenilir işletim ortamı: Cihazda oluşturulan ve dışarıdan erişime kapalı, cihaz üzerinde bulunan donanımlar için sürücüler bulunduran veya sürücü eklenebilen, bu sürücülerin çağırılması ile dışarıdan herhangi bir uygulama tarafından izlenemeyen ve müdahale edilemeyen unsurlar oluşturan bir işletim ortamıdır.

103- Zengin ortam: Cihazın güvenli işletim ortamı [102] dışında kalan ortamının tamamıdır. Güvenli işletim ortamı [102] olmayan cihazlarda bulunan ortama verilen addır.

104- Gönderici: Mesajı yazan ve alıcıya [105] ulaştırmak için iletişim uygulamasını [101] kullanan gerçek kişidir. Buluş konusu ürün bakımından girdi sağlayan kişidir.

105- Alıcı: Gönderici [104] tarafından iletişim uygulamasına [101] verilen mesajın hedefidir.

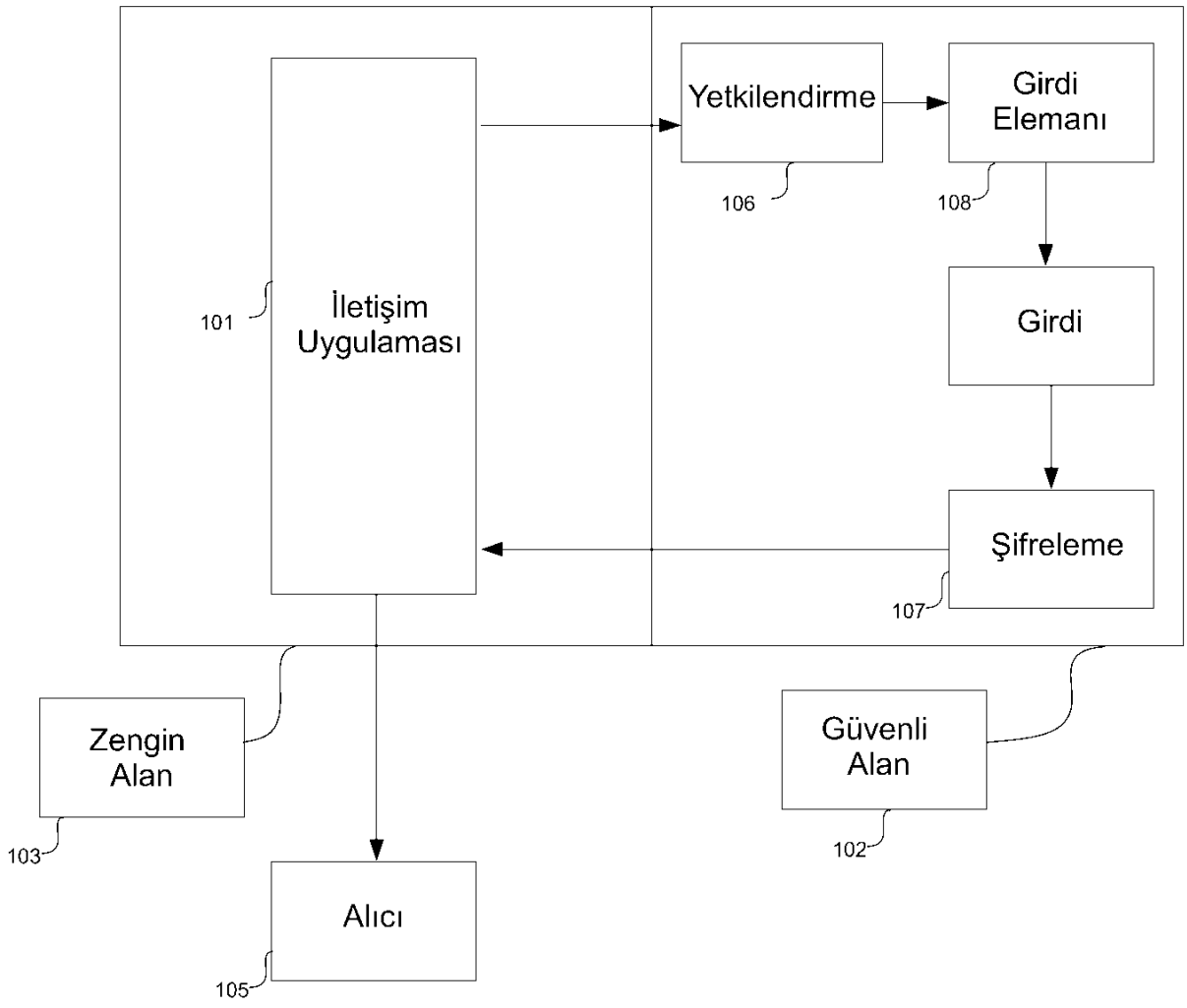
106- Yetkilendirme: Güvenilir işletim ortamına [102] giriş için uygulanan güvenlik önlemidir. Teknikte bilinen çeşitli yollarla kullanıcının güvenilir işletim ortamına [102] girmesi kısıtlanmıştır. Bu yollar muhtelif olabilir.

107- Şifreleme: Bir mesajın teknikte bilinen yollarla kripto edilmesi ve bu kriptonun açılması işlemidir. Teknikte bilinen birçok yolla yaygın olarak yapılabilir. Mesajın çözülmemiş halini anlamsız duruma getirir ve yalnızca bir anahtar ile açılabilmesini sağlar.

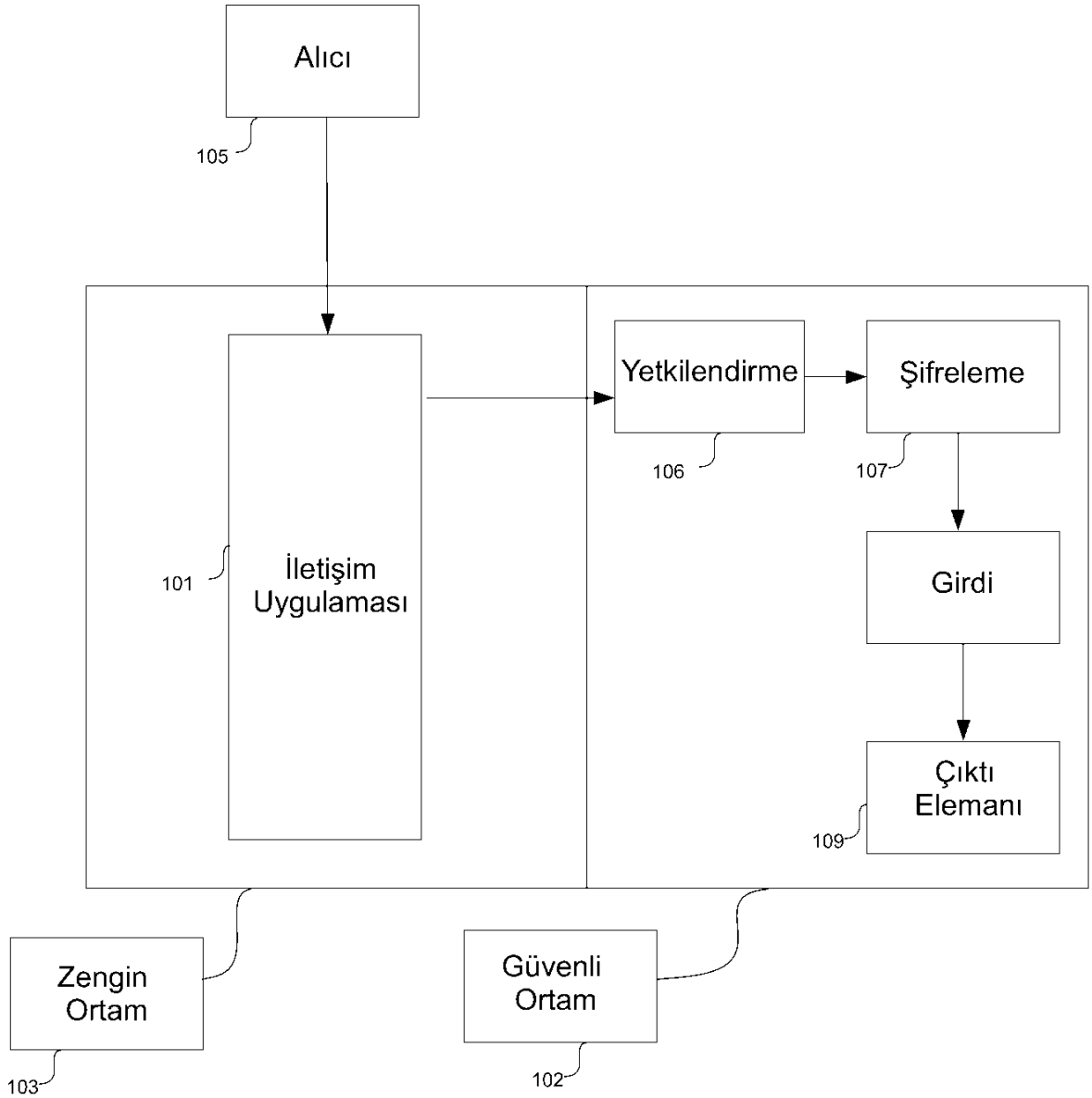
108- Girdi elemanı: İletişim uygulamasına [101] mesaj girilmesini sağlayan donanım ve bu donanımı çağıran sürücü veya sürücüleridir. Metin mesajları için klavye, ekran klavyesi için ekran ve dokunmatik yüzey, sesli yazı için hoparlör ve ilgili yazılım, görüntülü mesajlar için kamera ve benzeri gibi teknikte bilinen mesajı cihaza aktarmak için kullanılan unsurlardır.

109- Çıktı elemanı: İletişim uygulaması [101] tarafından bir mesajın kullanıcıya aktarılması için kullanılan donanımlar ve bu donanımların sürücüleridir. Ekran, hoparlör, kulaklık ve benzeri gibi teknikte bilinen donanımlardır.

110- Güvenli kullanıcı arayüzü: Çıktı elemanının tamamını veya bir bölümünün sürücülerinin güvenli işletim alanından [102] çağırılması ile elde edilen ve dışarıdan her tür erişime kapalı olan kullanıcı arayüzüdür. Bir örneği ekran olmakla beraber, her tür çıktı elemanı [109] üzerinde uygulanabilir.


İletişim Uygulaması
101
Yetkilendirme
106
Girdi Elemanı
108
Girdi
Şifreleme
107
Zengin Alan
103
Güvenli Alan
102
Alıcı
105

Çizim 1


Alıcı
105
İletişim Uygulaması
101
Yetkilendirme
106
Şifreleme
107
Girdi
Çıktı Elemanı
109
Zengin Ortam
103
Güvenli Ortam
102

Çizim 2