ÖZET

ALARM PANELLERİNE SINIRSIZ SAYIDA KULLANICI ERİŞİMİNİN MERKEZDEN YÖNETİLMESİ SİSTEMİ VE YÖNTEMİ

Buluş, mevcut alarm panellerine(4) bağlanarak kişilerin önceden tek tek alarm panellerine(4) kaydolmasına gerek duymaksızın sınırsız sayıda kişinin merkezi bir sunucu uygulamasına(11) veya bulut hizmetine kaydedilmesi suretiyle ve tek kullanımlık şifre kullanarak alarm panelinin alarm durumunu açık/kapalı konuma getirebilmesiyle ilgilidir. Buluş konusu sistem, her türlü alarm paneliyle(4) kullanılabilir. Buluş, kişi, yer, zaman, süre ve fonksiyon esaslı üretilen tek kullanımlık şifrelerin çevrimdışı (offline) doğrulanması yöntemiyle çalışır.

İSTEMLER

1- Buluş, mevcut alarm panellerine bağlanarak kişilerin önceden tek tek alarm panellerine kaydolmasına gerek duymaksızın sınırsız sayıda kişinin merkezi bir sunucu uygulamasına veya bulut hizmetine kaydedilmesi suretiyle ve tek kullanımlık şifre kullanarak alarm panelinin alarm durumunu açık/kapalı konuma getirebilmesiyle ilgili olup; sistemin erişim kontrolü elektronik devresi(1), gömülü yazılım(2), tuş takımı(3), alarm paneli(4), merkezi erişim kontrolü yönetim uygulaması(5), masa üstü cihaz yönetim uygulaması(6), uzaktan izleme ve yönetim uygulaması(7), mobil uygulama(8), temassız kimlik kartı(9), kilitli kapı(10), merkezi erişim kontrolü yönetim uygulaması kullanıcısı(11), şifre kullanıcısı(12), tek kullanımlık şifre(13), alarm paneli uzaktan izleme ve yönetim uygulaması(14), alarm paneli uzaktan izleme merkezi(15), personel sicil numarası(16), kişi doğrulama kodu(PIN)(17), kısa mesaj(SMS)(18), telefonda sesli yanıtlama sistemi(19), sesli arama(20), web servis(21), e-posta(22) ve internet/yerel ağ(23) sisteminden meydana gelmiş olmasıdır.

2- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; buluşun her türlü alarm paneline(4) uygulanabilen bir sistem ve yönteme sahip olması ile karakterize edilmesidir.

3- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; buluşun alarm panelinde(4) kısıtlı sayıda kullanıcı tanımlanması zorunluluğunu ortadan kaldırması ve sonsuz sayıda kullanıcı ekleme/çıkarma işlemini merkezden merkezi erişim kontrolü yönetim uygulaması(5) ile yapılabilir hale getirmesine olanak sağlaması ile karakterize edilmesidir.

4- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; alarm panellerinin(4) alarm durumlarının sabit şifrelerle kapatılıp/açılması yerine, kişi, yer, zaman, süre ve fonksiyon esaslı tek kullanımlık şifre(13) yöntemi ile açılır ve kapatılır hale gelmesi ile karakterize edilmesidir.

5- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; Buluşun şifre doğrulamasını bir ağ bağlantısına(23) ihtiyaç duymadan çevrimdışı olarak yaptığı halde, bir ağ bağlantısı(23) üzerinden durumu hakkında detaylı bildirimde bulunabilmesi ve uzaktan izleme ve kontrol edilme imkânına sahip olması ile karakterize edilmesidir.

6- İstem 1'de belirtilen alarm panellerine sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; alarm Paneli Uzaktan İzleme ve Yönetim Uygulamasına(7) sınırsız sayıdaki şifre kullanıcısının kimlikleri, başarılı ve başarısız şifre giriş işlemleri ve erişim zamanlarına ait bilgilerini iletebilmesi ile karakterize edilmesidir.

7- İstem 1'de belirtilen alarm panellerine(7) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; tek kullanımlık şifre(13) girişiyle birlikte aynı anda hem alarm panelinin(4) alarmının kapatılması, hem de kilitli kapının(10) otomatik açılması özelliğine sahip olması ile karakterize edilmesidir.

8- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; Alarm Panelinin(4) alarmını kapatacak kişinin doğrulanması için (kişi doğruma kodu) PIN(17) bilgisinin yanı sıra Mifare/ RFID/ HID destekleyen temassız kimlik kartı(9) ve/veya personel sicil numarası(16) kullanılması ile karakterize edilmesidir.

9- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; erişim Kontrolü Elektronik Devresi ve onun Gömülü Yazılımında yapılabilecek her güvenli işlem için işleme (fonksiyona) özel bir tek kullanımlık şifre(13) üretilmesi ve bu şifrenin doğrulanması ile fonksiyonun yerine getirilmesi özelliği ile karakterize edilmesidir.

10- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; erişim kontrolü elektronik devresine(1) yapılacak devre dışı bırakma, hasar verme gibi saldırıları da alarm paneline(4) bir alarm durumu olarak iletmesi ile karakterize edilmesidir.

11- İstem 1'de belirtilen alarm panellerine(4) sınırsız sayıda kullanıcı erişiminin merkezden yönetilmesi sistemi ve yöntemi ile ilgili olup özelliği; sistemin erişim kontrolü elektronik devresi(1) ve bu devre içerisine yüklenmiş gömülü yazılıma(2) sahip olması ile karakterize edilmesidir.

TARİFNAME

ALARM PANELLERİNE SINIRSIZ SAYIDA KULLANICI ERİŞİMİNİN MERKEZDEN YÖNETİLMESİ SİSTEMİ VE YÖNTEMİ

Teknolojik Alan:

Buluş, mevcut alarm panellerine bağlanarak kişilerin önceden tek tek alarm panellerine kaydolmasına gerek duymaksızın sınırsız sayıda kişinin merkezi bir sunucu uygulamasına veya bulut hizmetine kaydedilmesi suretiyle ve tek kullanımlık şifre kullanarak alarm panelinin alarm durumunu açık/kapalı konuma getirebilmesiyle ilgilidir. Buluş konusu sistem, her türlü alarm paneliyle kullanılabilir. Buluş, kişi, yer, zaman, süre ve fonksiyon esaslı üretilen tek kullanımlık şifrelerin çevrimdışı (offline) doğrulanması yöntemiyle çalışır.

Tekniğin Bilinen Durumu:

- Zaman, kişi, yer esaslı ve tek kullanımlık şifreyle çalışan elektronik kasa kilitleri pazarda mevcuttur. Ancak aynı şifreleme teknolojisinin alarm panellerine uygulanmış bir örneği dünyada yoktur. Bu anlamda buluşumuz bir ilktir.
- Zaman, kişi, yer esaslı ve tek kullanımlık şifreyle çalışan elektronik kasa kilitlerinde çevrimdışı (Offline) ve çevrimiçi (Online) olmak üzere iki türde şifre doğrulama yapan ürünler vardır. Ancak bu kilitler pahalıdır ve sınırlı yönetim, izleme ve kayıt tutma yeteneğine sahiptir. Bu ürünler çoğunlukla ATM kasalarında kullanılmaktadır.
- Pazarda kullanılan tek kullanımlık şifre yöntemlerinde değişken çeşitliliği daha azdır. Kişi doğrulama için PIN, yer (cihaz) ve zaman aralığı değişkenleri ile çalışırlar. Buluşumuzdaki tek kullanımlık şifre değişkenleri kişi doğrulama için PIN'e ilave veya alternatif olarak sicil numarası, temassız kimlik kartı kullanabilir. Ayrıca şifreler kullanım amacına (fonksiyonuna) göre de ayrıştırılır.
- Pazardaki offline kasa kilitlerinin hiçbir şekilde uzaktan izlenmesi, uzaktan güncellenmesi ve işlem kayıtlarının uzaktan çekilmeleri mümkün değildir. Sıklıkla yetkili kişiler tarafından saha ziyareti gereklidir.
- Pazardaki online kasa kilitleri çalışabilmek için mutlaka sürekli olarak canlı bir ağ bağlantısına ve merkezi uygulamayla bağlantı halinde olmaya mecburdurlar. Girilen şifrenin onaylanması merkezden yapılır ve bu da merkez ile kilit arasında bir yerde

korsan bir saldırının yapılması riskini taşır. Buluşumuz, offline olarak şifre doğrulama yaparak daha güvenli bir altyapı sunarken, online bağlantı imkanı ile uzaktan izleme, güncelleme ve olay kayıtlarının merkeze çekilmesi avantajını sunar.

- Pazardaki kilitler 9V pil ile çalışabilirler. Bu sebeple, sürekli olarak bir pil yenileme operasyonu ve pil maliyeti söz konusudur. Buluşumuz USB veya 5-24V arasındaki herhangi bir enerji kaynağı ile çalıştırılabilir. Pil tercihe bağlı olarak kullanılabilir.

Buluşu geliştirmekteki amacımız, kişi, yer, zaman, süre ve fonksiyon esaslı ve tek kullanımlık şifreyle çalışan erişim kontrol teknolojisinin kullanım alanını alarm panellerine uygulayarak alarm paneli sahiplerinin kullanıcı yönetimiyle ilgili ihtiyaçlarını karşılamak, alarm panellerinin bu konudaki eksiklerini gidermek, güvenlik seviyesini artırmak, ulusal ve uluslararası pazarlardaki ticari fırsatları değerlendirmektir.

Türkiye'de ve dünyada satılan mevcut alarm panellerinde kullanıcılar her bir alarm paneline ayrı ayrı tanımlanmak zorundadır. Alarm panellerinin kullanıcı tanımlama kapasiteleri sınırlı sayıdadır ve çoğu zaman yetersiz kalmaktadır. Operasyona dâhil olan yeni kullanıcıların tanımlanması zahmetli ve gecikmelere sebep olan bir işlemdir. Aynı şekilde bir kullanıcının silinmesi de zahmetli ve zaman alan bir işlemdir ve kullanıcı silme işlemindeki gecikmeler yetkisiz erişime olanak sağlayarak önemli güvenlik risklerine sebep olmaktadır. Yeterli sayıda kullanıcı tanımlama kapasitesi olmadığından, bazı durumlarda tek bir kullanıcı şifresi birden çok kişiyle paylaşılarak kullanılmaktadır. Bu durum önemli güvenlik risklerini doğurmakta ve mekâna gerçekten kimin girdiği tespit edilemediğinden geriye dönük sağlıklı bir suç takibi yapılamamaktadır. Ayrıca, alarm panellerinin pek çok kullanım biçiminde kullanıcı güvenli bölgeye fiziki bir anahtarla giriş yaptıktan sonra alarm panelini kapatmak zorundadır. Bu da zaman kaybına ve fiziki anahtarların yönetilmesiyle ilgili güvenlik ve lojistik zorluklara sebep olmaktadır.

Buluşumuz bir alarm paneline bağlandığında artık kullanıcı sayısı ile ilgili bir sınırlama kalmamaktadır. Ayrıca kullanıcı yönetimi, merkezi bir uygulama üzerinden yürütüldüğünden kullanıcı ekleme ve çıkarmayla ilgili gecikmeye bağlı güvenlik riskleri ve zaman kayıpları önlenmekte ve operasyonda kolaylık sağlanmaktadır. Buluş içerisinde kullanılan kişi, yer, zaman, süre ve fonksiyon esaslı tek kullanımlık şifre yöntemi ve bu şifrenin çevrimdışı (offline) doğrulanması alarm panellerindeki güvenliği en üst seviyeye çıkarmakta ve ortak şifre kullanımı, sabit şifre kullanımı gibi güvenlik risklerini ortadan kaldırmaktadır. Buluş, kapının dışına yerleştirilen bir tuş takımı ile beraber kullanıldığında üzerinde bulunan ayrı bir röle devresi sayesinde alarm panelinin alarmını kapatırken aynı zamanda kapıyı da açabilir. Böylece, kullanıcı fiziki bir anahtar bulundurmadan mekâna erişim sağlayabilir ve iki ayrı işlem

yapmadığı için zaman kazanmış olur. Fiziki anahtar kullanma zorunluluğu ortadan kalktığı zaman anahtar lojistiği ve anahtarların kopyalanması, çalınması gibi riskler de ortadan kalkmış olur.

- Buluş, kişi, yer, zaman, süre ve fonksiyon esaslı ve tek kullanımlık şifre algoritmasını kullanır. Şifreler merkezden üretilir ama sahada erişim kontrol cihazı üzerinde çevrimdışı olarak doğrulanır. Bu sayede hafızada kayıtlı kullanıcı ve onlara ait sabit şifreli yöntemlere veya çevrimiçi şifre doğrulama yöntemlerine kıyasla buluşumuzun yöntemi çok daha güvenlidir.
- Şifreler belirli bir kişi için üretilir ve kişi şifreyi girmeden önce kişisel doğrulama kodunu (PIN), ve/veya sicil numarasını ve/veya temassız kimlik kartını kullanarak kendini doğrulatır. Bu sayede erişim yapan kişinin doğrulanma güvenilirliği en üst seviyeye çıkmış olur.
- Şifreler belli bir erişim kontrol devresi için üretilir. Aynı şifre bir başka yerde, başka bir erişim kontrol devresi ile kullanılamaz.
- Şifreler belli bir zaman aralığında geçerli olmak üzere ve tek seferlik kullanım için üretilir. Erişim yetkisi verilen sürenin öncesinde veya sonrasında kullanılamaz. Erişim kontrol devresi, üzerinde zamanı tutabilecek kabiliyete sahiptir ve girilen tek kullanımlık şifrenin geçerli olduğu zaman aralığını doğrulayabilir.
- Şifreler belli bir fonksiyon için üretilir. Mesela cihazı cezalı konumdan çıkarmak için kullanılacak tek kullanımlık şifre ile kişi alarmı kapalı konuma getiremez. Fonksiyonlar programlanabilir niteliktedir ve ihtiyaca göre çoğaltılabilir.
- Şifreler erişim kontrol devresi üzerinde çevrimdışı olarak kontrol edilir. Şifrenin çevrimiçi onaylanması, yani şifreyi onu üreten merkeze ileterek merkezin onaylaması yönteminde olduğu gibi sunucu ve cihaz arasına izinsiz giriş yapılarak sistemin aldatılması riski bulunmaz.
- Sistem içerisinde kullanıcı ekleme/çıkarma işlemi merkezden yapılır, bu sayede yetkisiz kullanıcıların erişimini engellenir ve kullanıcıların sisteme eklenip çıkarılması kolaylaşır. Kullanıcılar için alarm panelinde veya erişim kontrol devresinde herhangi bir ön tanım yapmaya ihtiyaç yoktur.
- Sistem her müşteri bazında yerel bir sunucuda çalışan bağımsız bir merkezi erişim kontrolü yönetim uygulaması ile idare edilebileceği gibi, çoklu ve izole müşteri yönetimi özelliği sayesinde müşteriler bir bulut hizmeti olarak da sistemden yararlanabilirler.

- Buluş, 5-24V arası çalışma esnekliği sayesinde mümkün olan yerlerde USB veya alternatif enerji kaynaklarını kullanarak pil ile beslemeyi zorunlu olmaktan çıkarmaktadır. Pil yine de bir seçenek olarak kullanılabilecek bir enerji kaynağıdır.
- Buluş, üzerindeki Ethernet kapısı ile bir yerel ağa veya internete bağlanması durumunda, uzaktan izlenerek çalışıp çalışmadığı, hata veya cezalı durumuna girip girmediği takip edilebilir. Bu sayede merkezi operasyon kolaylaşır ve verimliliği artar.
- Buluş, üzerindeki Ethernet kapısı ile bir yerel ağa veya internete bağlanması durumunda, cihaz üzerinde tutulan olay kayıtları, doğru ve hatalı tüm şifre giriş kayıtları uzaktan gerçek zamanlı izlenebileceği gibi bellekte tutulan geçmiş şifre ve diğer olay kayıtları merkezi sisteme otomatik aktarılarak saklanabilir. Olası adli vakaların araştırılması kolaylaşır.
- Buluş, alarm panelinin yanı sıra erişim sağlanmak istenen mekânın giriş kapısına da bağlanabilir ve aynı anda alarm panelinin alarmını kapalı konuma getirirken kapının da otomatik olarak açılmasını sağlayabilir. Bunun için kapının motor destekli elektrikli bir kilide sahip olması gereklidir. Bu yöntem, mekanik anahtarlı kilitlere kıyasla önemli bir zaman ve maliyet avantajı sağlamaktadır. Erişim sağlayacak kişilerin fiziksel anahtarı bulundurma veya bir yere gidip temin etme zorunluluğu ortadan kalkmaktadır. Erişim sağlanması istenen mekâna en yakın mesafedeki yetkili kişi yönlendirilebilir ve çeşitli metotlarla iletilen tek kullanımlık şifresiyle hem kapıyı açması, hem de alarm panelinin alarmını kapalı konuma getirmesi sağlanabilir.
- Buluş, gömülü yazılımın masa üstü cihaz yönetim uygulamasıyla sahada veya çevrimiçi (online) bağlantının mevcut olduğu durumlarda uzaktan izleme ve kontrol uygulamasıyla uzaktan güncellenmesi mümkündür. Bu sayede gelecekteki güvenlik risklerine ve teknolojik gelişmelere karşı güncel kalması sağlanmaktadır.
- Buluşu, elle şifre tuşlama işlemine alternatif olarak bu buluş kapsamında geliştirilmiş olan mobil uygulamayla ve NFC iletişim teknolojisiyle kullanmak da mümkündür. Bu durumda merkezden birisinin şifre üretmesine gerek kalmaksızın yetkili personel mobil cihazını NFC destekleyen tuş takımına yaklaştırarak merkezi kilit yönetim uygulamasından kendisi için, ilgili cihaz için ve işlemin yapıldığı zaman için geçerli olacak bir şifre talebinde bulunur. Merkezi uygulama, belirli kıstasların karşılanması halinde şifreyi üretir. Geçerli şifre, elle girişe gerek kalmadan mobil uygulama üzerinden cihaza ulaştırılarak erişim sağlanır.
- Buluşun standardında tek kullanımlık şifreyle beraber kullanıcılara özel PIN (kişi doğrulama kodu) kullanılır. Tuş takımının kart okuma özelliği olması halinde, tercihe bağlı olarak Mifare, RFID veya HID destekleyen kimlik kartları da erişim kontrolünde

bir girdi olarak kullanılabilir (PIN ve/veya temassız kart ve OTC). PIN ve temassız kartın yanı sıra tercihe bağlı olarak kullanıcının sicil numarası da kullanıcı doğrulama sürecine dâhil edilebilir. Bu sayede kullanıcı doğrulamayla ilgili güvenlik daha da artırılmış olur (PIN ve/veya temassız kart ve/veya Sicil numarası ve OTC).

- Sistem içerisinde tek kullanımlık şifre talep etme yöntemleri çeşitlidir. Bu yöntemler şunlardır; a) Merkezi Erişim Kontrolü Yönetim Uygulamasında bir kullanıcı tarafından üretilir. b) Şifre kullanıcısı mobil uygulama ile sunucudan kendisi talep eder. c) Şifre kullanıcısı tuş takımı üzerinden istenen bilgileri tuşlayarak sunucudan talep eder. d) Şifre kullanıcısı SMS ile talepte bulunur. e) Şifre kullanıcısı e-posta ile talepte bulunur. f) Şifre kullanıcısı telefonla bir otomatik sesli yanıtlama sistemini (IVR) arayarak talepte bulunur. g) Başka bir sunucu yazılımı ile web servis bağlantısı sağlanarak diğer sunucu talepte bulunur.

  Şifre kullanıcısının talepte bulunduğu metotlarda kişi kendisini doğrulatmak için PIN ve/veya temassız kimlik kartı ve/veya sicil numarası kullanabilir.

- Sistem içerisinde üretilen tek kullanımlık şifrenin erişim talep eden kişiye ulaştırılma yöntemleri çeşitlidir. Bu yöntemler şunlardır; a) Merkezi erişim kontrolü yönetim uygulamasında şifreyi üreten kullanıcı şifre kullanıcısına tek kullanımlık şifreyi sesli veya yazılı olarak bildirir. b) Sunucu mobil uygulama ile iletilen talebe aynı kanal üzerinden şifreyi gönderir. c) Şifre kullanıcısına SMS ile bildirilir. d) Şifre kullanıcısına e-posta ile bildirilir. e) Şifre kullanıcısı telefonla bir otomatik sesli yanıtlama sistemi (IVR) tarafından aranarak sesli iletilir. f) Başka bir sunucu yazılımı ile web servis bağlantısı üzerinden gelen talep aynı kanal üzerinden yanıtlanır.
- Sistem, alarm paneli yönetim uygulaması ile bağlantı sağlayabilir, üretilen, kullanılan şifreler ve şifre kullanıcılarıyla ilgili verileri alarm paneli yönetim uygulamasına iletebilir. Sınırsız sayıda kullanıcı sisteme dâhil edilebildiği ve kimin nereye ne zaman erişim sağladığı takip edilebildiği için Alarm Paneli yönetim uygulamasına da daha detaylı ve sağlıklı bilgi aktarılabilir. Alarm paneli uzaktan izleme merkezlerinin işleri kolaylaşır ve verimlilikleri artar.
- Buluş kapsamındaki merkezi erişim kontrolü yönetim uygulaması yerel bir sunucuya kurularak yerel ağ içerisinde kullanılabileceği gibi, bir bulut hizmeti olarak da sunulmaktadır ve tercih edilmesi halinde ücretli bir hizmet olarak yararlanılabilir. Bulut hizmeti ilk yatırım maliyetlerini düşüren ve sunucu bakım ve yedekleme sorumluluğu kullanıcıya bırakmayan avantajlı bir seçenektir.
- Buluş her türlü alarm paneline bağlanabilir. Kullanımı yaygın ve esnektir.

- Buluş wiegand, seri (RS232, PS2), analog, dijital, matris tipi tüm tuş takımlarıyla uyumludur. Kullanımı yaygın ve esnektir.
- Buluş, erişim kontrolü elektronik devresine yapılacak devre dışı bırakma, hasar verme gibi saldırıları da alarm paneline bir alarm durumu olarak iletme özelliğine sahiptir. Böylece, devre dışı bırakılması halinde alarm izleme merkezi durumdan haberdar edilmiş olacaktır.

Şekillerin Açıklanması:

Buluş, ilişikteki şekillere atıfta bulunularak anlatılacaktır, böylece buluşun özellikleri daha açıkça anlaşılacak ve takdir edilecektir, fakat bunun amacı buluşu bu belli düzenlemeler ile sınırlamak değildir. Tam tersine, buluşun ilişikteki istemler tarafından tanımlandığı alanı içine dahil edilebilecek bütün alternatifleri, değişiklikleri ve denkliklerinin kapsanması amaçlanmıştır. Gösterilen ayrıntılar, sadece mevcut buluşun tercih edilen düzenlemelerinin anlatımı amacıyla gösterildiği ve hem yöntemlerin şekillendirilmesinin, hem de buluşun kuralları ve kavramsal özelliklerinin en kullanışlı ve kolay anlaşılır tanımını sağlamak amacıyla sunuldukları anlaşılmalıdır. Bu çizimlerde;

Şekil 1	Sistemin ön hazırlık kısmının şematik görüntüsüdür.
Şekil 2	Sistemin kurulum aşamasının şematik görüntüsüdür.
Şekil 3	Sistemin işleyişini gösteren şematik görüntüsüdür.

Bu buluşun anlaşılmasına yardımcı olacak şekiller ekli resimde belirtildiği gibi numaralandırılmış olup isimleri ile beraber aşağıda verilmiştir.

Referansların açıklanması:

1. Erişim Kontrolü Elektronik Devresi
2. Gömülü Yazılım (Firmware)
3. Tuş Takımı
4. Alarm Paneli
5. Merkezi Erişim Kontrolü Yönetim Uygulaması
6. Masa Üstü Cihaz Yönetim Uygulaması
7. Uzaktan İzleme ve Yönetim Uygulaması
8. Mobil Uygulama
9. Temassız Kimlik Kartı
10. Kilitli Kapı
11. Merkezi Erişim Kontrolü Yönetim Uygulaması Kullanıcısı
12. Şifre Kullanıcısı
13. Tek Kullanımlık Şifre
14. Alarm Paneli Uzaktan İzleme ve Yönetim Uygulaması
15. Alarm Paneli Uzaktan İzleme Merkezi
16. Personel Sicil Numarası
17. Kişi Doğrulama Kodu (PIN)
18. Kısa Mesaj (SMS)
19. Telefonda Sesli Yanıtlama Sistemi (IVR)
20. Sesli Arama
21. Web Servis
22. E-posta
23. İnternet/Yerel Ağ

Şekillerin Detaylı Açıklaması

- Erişim Kontrolü Elektronik Devresi (1): Buluş kapsamında özel olarak tasarlanmış ve üretilmiş bir elektronik devredir. Kullanılacağı cihaza göre farklı ölçü ve biçimlerde olabilir. Farklı kullanım yerlerine göre farklı modelleri mevcuttur. En kapsamlı modelinde 3 adet röle, Ethernet ve USB kapıları, programlama kapısı, wiegand, seri (RS232, PS2), analog, dijital, matris tipi tuş takımı (2) bağlantılarını desteklemek üzere

DB9 tipi seri bağlantı kapısı ve PS2 kapısı, 5-24V güç besleme girişi, NFC anteni yer almaktadır.

- Gömülü Yazılım (Firmware) (2): Erişim kontrolü elektronik devresi (1) içerisinde çalışan yazılımdır. Zaman, kişi (12),yer ve fonksiyon esaslı tek kullanımlık şifreyi (13) üzerinde çevrimdışı çalışan algoritma ile çözümler. Şifreyi (13) onaylarsa elektronik devrenin (1) bir veya daha çok rölenin tetiklenmesini sağlar. Bunun dışında elektronik devrenin (1) davranışlarını belirleyen çeşitli fonksiyonlara ve çalışma değişkenlerine (parametrelerine) sahiptir ve bu değerlere göre elektronik devrenin (1) çalışmasını sağlar. Tuş takımı (3) veya NFC haberleşmeyle mobil uygulamadan (8) iletilen kişi doğrulama değerleri (PIN)(17), temassız kimlik kartı(9), sicil numarası(16) ve tek kullanımlık şifreyi (13) değerlendirerek üzerindeki röle devresini (devrelerini) tetikler veya reddeder. Üzerindeki bellekte başarılı ve başarısız şifre (13) girişlerini ve diğer olay kayıtlarını kaydeder. Tuş takımı (3) içinde NFC okuma/yazma kabiliyeti olan modellerde bu buluş kapsamında geliştirilmiş olan mobil uygulama (8) ile haberleşir. Şifre (13) alışverişi, kayıt güncelleme, yazılım (2) güncelleme, parametre güncelleme, zaman güncelleme gibi işlevleri Ethernet ve/veya NFC kablosuz iletişim aracılığıyla yerine getirir. Ethernet ile bir yerel ağa veya internete(23) bağlı olan modellerde, sisteme kayıtlı kişilerin (12) Merkezi erişim kontrolü yönetim uygulamasından (5) tek kullanımlık şifre (12) talep etmesini sağlar. Erişim kontrol devresinin (1) belleğinde biriken kullanılmış şifre (12) kayıtlarını uzaktan izleme ve kontrol uygulamasına (7) aktarır. Tüm olay kayıtlarını gerçek zamanlı olarak uzaktan izleme ve kontrol uygulamasına (7) aktarır. Uzaktan izleme ve kontrol uygulamasından (7) gelen komutları yerine getirir. Gömülü yazılım (2) ve parametrelerin uzaktan güncellenmesi görevlerini yerine getirir.
- Tuş Takımı (3): Şifre kullanıcısının (12) PIN kodunu (17) ve/veya personel sicil numarasını (16) tuşladığı ve/veya temassız kimlik kartını (9) okuttuğu (kart okuyuculu modellerde) ardından da kendisine temin edilmiş olan tek kullanımlık şifresini (13) tuşladığı tuş takımıdır. wiegand, seri (RS232, PS2), analog, dijital, matris tipi tüm tuş takımları buluşla birlikte kullanılabilir. Ayrıca, istenirse RFID, Mifare ve HID kart okuyucu ve NFC özellikli tuş takımları (3) da kullanılabilmektedir. İç mekân, dış mekân modelleri uygulamaya göre tercih edilebilir.
- Alarm Paneli (4): İzinsiz girişleri tespit ederek bir Alarm paneli uzaktan izleme merkezine (15) bildiren ve bulunduğu yerde siren ve ışıklı uyarı ile alarm üreten bir cihazdır. Normal koşullarda panele (4) önceden tanımlanmış bir kullanıcının mekâna girdikten sonra alarm paneline (4) şifresini girmek suretiyle panelin (4) alarmını kapalı

(disarm) konuma getirmesi gereklidir. Buluş her türlü alarm paneline (4) uyumlu olup, alarm paneline (4) bir kullanıcı tanımlamaksızın güvenli şekilde alarmın kapalı konuma gelmesini sağlamaktadır.

- Merkezi Erişim Kontrolü Yönetim Uygulaması (5): Uygulama web teknolojileri kullanılarak bu buluş kapsamında özel olarak geliştirilmiş bir sunucu uygulamasıdır. Erişim kontrolü elektronik devrelerinin (1), uygulama kullanıcılarının (11) ve şifre kullanıcılarının (12) ve onlara ait gerekli bilgilerin kaydedilmesi, silinmesi ve düzenlenmesi işlemlerini yerine getirir. Uygulama kullanıcıları (11) bu uygulama (5) üzerinden herhangi bir yetkili kişi (12) ve kayıtlı cihaz (1) için herhangi bir başlangıç zamanı ve geçerlilik süresi dâhilinde tek sefer kullanılabilecek şifreler (13) üretirler. Ayrıca, uygulamaya (5) şifre kullanıcısı (12) mobil uygulama (8), tuş takımı (3), SMS (18), telefonda sesli yanıtlama sistemi (19), aracılığıyla da tek kullanımlık şifre (13) talebinde bulunabilir. Uygulama kullanıcısı şifreyi (13) telefonla (20) şifre kullanıcısına (12) iletebileceği gibi, uygulama (5) bu şifreleri (13) kayıt altına aldığı halde tercihe göre alıcılara e-posta (22) ve/veya kısa mesaj (SMS) (18) ve/veya mobil uygulama (8) ve/veya IVR (19) ile gönderebilir. Ayrıca uygulama (5) web servis (21) üzerinden üçüncü taraf uygulamalarla haberleşebilir, şifre (13) talebi kabul edebilir ve iletebilir.
- Masa Üstü Cihaz Yönetim Uygulaması (6): Uygulama bu buluş kapsamında özel olarak geliştirilmiş bir PC uygulamasıdır. USB üzerinden cihazla bağlantı kurarak fonksiyon testi, zaman güncelleme, parametre güncelleme, gömülü yazılım (firmware) (2) güncelleme, benzersiz kimlik numarası ve ana anahtar kodunu değiştirme işlevlerini yürütür.
- Uzaktan İzleme ve Yönetim Uygulaması (7): Uygulama Web teknolojileri kullanılarak bu buluş kapsamında özel olarak geliştirilmiş bir sunucu uygulamasıdır. Uygulama yerel bir sunucuda barındırılarak yerel ağ içerisinde kullanılabileceği gibi internet(23) ortamında var olan bir bulut hizmeti üzerinden ücretli hizmet olarak da kullanılabilir. Sahadaki Ethernet bağlantısı sayesinde çevrimiçi çalışan erişim kontrolü elektronik devreleri (1) ile bağlantı kurarak cihazların (1) anlık durum bilgilerinin takip edilmesini sağlar, cihaz durum bilgilerini ve hata kayıtlarını geçmiş tarihli raporlar. Erişim kontrolü elektronik devrelerini (1) uzaktan sorgulayabilir, kapatıp açabilir, firmware (2) ve parametre güncellemesi yapabilir. Erişim kontrolü elektronik devrelerinin (1) benzersiz kimlik numarası ve ana anahtar kodlarını uzaktan değiştirebilir.
- Mobil Uygulama (8): Mobil cihazlarda çalışmak üzere bu buluşa özel olarak tasarlanmıştır. Donanımında NFC kablosuz iletişimi destekleyen tuş takımı (3) bulunduran modellerde NFC uyumlu bir mobil cihaz kullanarak ve tuşlama yapmadan

açmak için kullanılır. Uygulama (8) internet(23) üzerinden merkezi erişim kontrolü yönetim uygulaması (5) ile haberleşerek şifre kullanıcısı (12) ve tanımlı bir cihaz (1) için tek kullanımlık şifre (13) talep eder. Gelen şifreyi (13) ve şifre kullanıcısının (12) PIN numarasını (17) NFC bağlantısı üzerinden cihaza (1) göndererek cihazın (1) şifreyi (13) onaylamasını veya reddetmesini sağlar. Uygulama (8) ayrıca, zaman güncelleme, firmware (2) ve parametre güncelleme, kullanıcı PIN (17) değişikliği, cihazdan (1) kayıtlı veri aktarımı, benzersiz kimlik numarası ve ana anahtar kodlarının güncellenmesi işlemlerini yürütür.

- Temassız Kimlik Kartı (9): Kuruluşların personellerine verdikleri ve turnike veya kapı geçişlerinde kullanılan temassız kimlik kartları Buluş içerisinde şifre kullanıcısını (12) doğrulamak ve/veya şifre kullanıcısının (12) tuş takımı (3) üzerinden şifre (13) talep etmesi için bir değişken olarak kullanılabilir. MiFare, RFID veya HID teknolojilerini destekleyen temassız kimlik kartları (9) yine aynı teknolojiyi destekleyen kart okuyuculu tuş takımlarının (3) bulunduğu modellerde şifre kullanıcısı (12) tarafından tuş takımına (3) okutulmak suretiyle tek kullanımlık şifre (13) içerisinde kişi doğrulama amacıyla kullanılır.
- Kilitli Kapı (10): Elektrik enerjisiyle tetiklenebilen bir motorlu kilide sahip kapıdır. Kapı, ihtiyaca göre iç mekân veya dış mekân kapısı olabilir. Tuş takımının (3) mekânın dışına yerleştirilmesi halinde, tercihe göre tek kullanımlık şifrenin (13) onaylanması sonrasında erişim kontrolü elektronik devresi alarm panelinin (4) alarmını kapalı hale getirirken aynı anda otomatik kapıyı da (10) açabilir.
- Merkezi Erişim Kontrolü Yönetim Uygulaması Kullanıcısı (11): Uygulamanın kullanıcıları, farklı rollerde olabilir. Her rolün farklı yetki ve erişim hakları vardır.
- Şifre Kullanıcısı (12): Sahada alarm panellerinin (4) alarmlarını kapalı konuma getirerek mekâna güvenli erişim sağlaması gereken kişilerdir. Merkezi erişim kontrolü yönetim uygulamasında (5) önceden tanımlanmış olan şifre kullanıcıları, kendilerine verilen veya kendilerinin değişik metotlara talep ettikleri tek kullanımlık şifreleri (13) kullanarak mekânlara güvenli erişim sağlarlar. Şifre kullanıcıları (12) erişim sağlamak için tercih edilen yönteme göre sahip oldukları PIN (17), temassız kimlik kartı (9), mobil uygulama (8) veya personel sicil numaralarından (16) bir veya birkaçını ve ardından tek kullanımlık şifreyi (13) ve varsa fonksiyon kodunu tuş takımına girerler.
- Tek Kullanımlık Şifre (13): Merkezi erişim kontrolü yönetim uygulaması (5) tarafından üretilen ve erişim kontrolü elektronik devresi (1) tarafından offline olarak değerlendirilen şifredir. Buluş kapsamında geliştirilmiş bir algoritma ile üretilir. Şifrenin oluşturulmasında gömülü yazılımın (2) benzersiz kimlik numarası, sistemde

tanımlı ana anahtar kodu, geçerlilik başlangıç zamanı, geçerlilik süresi ve fonksiyon kodu değişkenlerinin yanı sıra kişi doğrulamak amacıyla PIN (17), Temassız kimlik kartının (9) benzersiz kimlik numarası, personel sicil numarası (16) değişkenlerinden bir veya birkaçı kullanılır.

- Alarm Paneli Uzaktan İzleme ve Yönetim Uygulaması (14): Alarm panellerinin (4) uzaktan izlenmesini sağlayan üçüncü taraf uygulamalardır. Buluş, her türlü alarm paneli uzaktan izleme ve kontrol uygulamasına web servis (21) üzerinden bağlantı sağlayabilir, bilgi alıp bilgi verebilir. Merkezi erişim kontrolü yönetim uygulaması (5) mekâna kimin (12) hangi şifreyi (13) kullanarak ne zaman erişim sağladığıyla ilgili detaylı bilgileri aktarabilir ve şifre (13) oluşturma talebi alabilir.
- Alarm Paneli Uzaktan İzleme Merkezi (15): Alarm panellerini (4) alarm paneli uzaktan izleme ve kontrol uygulaması kullanarak uzaktan izleyen, merkeze ulaşan alarm bildirimlerini değerlendiren ve gerekli güvenlik prosedürlerini uygulayan iş birimidir.
- Personel Sicil Numarası (16): Kurumlar tarafından, çalışanlarının takibi ve yönetimi için kullanılmak üzere atanan benzersiz kayıt numarasıdır.
- Kişi Doğrulama Kodu (PIN) (17): Merkezi erişim kontrolü yönetim uygulaması tarafından (5) sisteme tanımlanan şifre kullanıcıları için atanan bir sayıdır. Kişi doğrulama kodu merkezi erişim kontrolü yönetim uygulaması (5) tarafından belirlenebileceği gibi, şifre kullanıcısı (12) tarafından da belirlenebilir ve/veya değiştirilebilir. Kod, şifre kullanıcısı (12) tarafından korunması gereken gizli bir bilgidir. Merkezi erişim kontrolü yönetim uygulaması tarafından (5) tek kullanımlık şifre (13) oluşturulurken bir değişken olarak kullanılırken, şifre kullanıcısı (12) şifreyi (13) tuş takımına girmeden önce kendi PIN kodunu (17) tuşlayarak gömülü yazılımın (2) aynı şifreyi (13) aynı algoritmayla hesaplayabilmesini sağlar.
- Kısa Mesaj (SMS) (18): Sistemde merkezi erişim yönetim uygulamasının (5) tek kullanımlık şifreleri (13) şifre kullanıcısına (12) göndermek ve/veya şifre kullanıcısının (12) şifre (13) talep etmesi için bir iletişim yöntemi olarak kullanılır. SMS'ler, üçüncü taraf bir SMS servis sağlayıcısının altyapısı bu sisteme entegre edilerek gönderilir.
- Telefonda Sesli Yanıtlama Sistemi (IVR) (19): Sistemde merkezi erişim yönetim uygulamasının (5) tek kullanımlık şifreleri (13) şifre kullanıcısına (12) iletmek ve/veya şifre kullanıcısının (12) şifre (13) talep etmesi için bir iletişim yöntemi olarak kullanılır. iletişim, üçüncü taraf bir IVR servis sağlayıcısının altyapısı bu sisteme entegre edilerek sağlanır.

- Sesli Arama (20): Sistemde merkezi erişim yönetim uygulamasının (5) tek kullanımlık şifreleri (13) şifre kullanıcısına (12) iletmek ve/veya şifre kullanıcısının (12) şifre (13) talep etmesi için bir iletişim yöntemi olarak kullanılır.
- Web Servis (21): Merkezi erişim yönetim uygulamasının (5) ve/veya Uzaktan izleme ve kontrol uygulamasının (7) sistem içinde birbirleriyle ve/veya sistem dışında üçüncü taraf uygulamalarla veri alış verişinde kullanılır. Önceden geliştirilmiş web servisleri (21) olduğu gibi, saha kurulumu sırasında ortaya çıkacak ihtiyaçlara göre veya müşteri taleplerine göre de yeni servisler (21) geliştirilir.
- E-posta (22): Sistemde merkezi erişim yönetim uygulamasının (5) tek kullanımlık şifreleri (13) şifre kullanıcısına (12) iletmek ve/veya şifre kullanıcısının (12) şifre (13) talep etmesi için bir iletişim yöntemi olarak kullanılır.
- İnternet/Yerel Ağ (23) : Yerel ağa bağlı bulunan internettir.

Buluşun Detaylı Açıklanması:

Buluş, mevcut alarm panellerine bağlanarak kişilerin önceden tek tek alarm panellerine kaydolmasına gerek duymaksızın sınırsız sayıda kişinin merkezi bir sunucu uygulamasına veya bulut hizmetine kaydedilmesi suretiyle ve tek kullanımlık şifre kullanarak alarm panelinin alarm durumunu açık/kapalı konuma getirebilmesiyle ilgilidir. Buluş konusu sistem, her türlü alarm paneliyle kullanılabilir. Buluş, kişi, yer, zaman, süre ve fonksiyon esaslı üretilen tek kullanımlık şifrelerin çevrimdışı (offline) doğrulanması yöntemiyle çalışır.

A. **Sistem Ön Hazırlık:** Erişim kontrolü elektronik devreleri (1) sahaya kurulmadan önce yapılması gereken ön hazırlıklar şu şekildedir;
   - Erişim kontrolü elektronik devrelerine (1) masa üstü cihaz yönetim uygulaması (6) kullanılarak USB üzerinden bağlantı sağlanır ve gömülü yazılım (2) ve çalışma değişkenleri yüklenir. Bu işlem sırasında devrelere benzersiz kimlik numarası ve ana anahtar kodu kaydedilir.
   - Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde tercihe bağlı olarak SMS (18), IVR (19) ve e-posta (22) servis sağlayıcılarına bağlantı için gerekli web servis (21) tanımlamaları yapılır.
   - Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde merkezi erişim kontrolü yönetim uygulaması kullanıcıları (11) ve erişim yetkileri tanımlanır. Kullanıcıların

mobil telefon numaraları ve e-posta adresleri kaydedilir. Uygulama (5) kullanıcılara (11) kullanıcı adı ve şifre bilgilerini SMS (18) ve e-posta (22) ile bildirir.

- Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde şifre kullanıcıları (12) ve çalışma gün ve saatleri tanımlanır. Şifre kullanıcılarının (12) telefon numaraları ve e-posta adreslerinin yanı sıra, tercihe bağlı olarak personel sicil numaraları (16) ve temassız kimlik kartı (9) bilgileri de kaydedilir. Uygulama (5) kullanıcılara (12) kullanıcı adı ve şifre bilgilerini SMS (18) ve e-posta (22) ile bildirir.

-Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde erişim kontrolü elektronik devreleri (1), bu devrelerin (1) birlikte kullanılacakları alarm panelleri (4) tanımlanır. Bu devreler (1) tanımlanırken uygulamaya (6) da her devrenin (1) benzersiz kimlik numarası ve ana anahtar kodu kaydedilir.

-Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde uzaktan izleme ve kontrol uygulaması (7) ile bilgi alışverişinde bulunabilmesi için gerekli web servisi (21) ayarları yapılır.

-Merkezi erişim kontrolü yönetim uygulaması (5) üzerinde alarm paneli uzaktan izleme ve kontrol uygulaması (14) ile bilgi alışverişinde bulunabilmesi için gerekli web servisi (21) ayarları yapılır.

B. Sistem Kurulum:

-Merkezi erişim kontrolü yönetim uygulaması (5) ve uzaktan izleme ve kontrol uygulamasının (7) SMS (18), IVR (19) ve e-posta (22) servislerini kullanabilmesi için gerekli internet veya yerel ağ(23) bağlantıları temin edilir.

-Merkezi erişim kontrolü yönetim uygulamasının (5) alarm paneli uzaktan izleme ve kontrol uygulamasıyla web servisleri üzerinden (21) veri alışverişi yapabilmesi için gerekli internet veya yerel ağ(23) bağlantıları temin edilir.

-Erişim kontrolü elektronik devreleri (1) alarmı açık / kapalı konuma getirmek üzere ilgili röle devresi üzerinden sahadaki alarm panellerine (4) bağlanır.

-Tercihe göre NFC ve/veya kart okuyucu özelliği olan veya olmayan dış mekân veya iç mekan uyumlu tuş takımları (3) mekan içine veya dışına monte edilir ve ilgili bağlantı noktası tipine uygun şekilde seri veya PS2 kapısı üzerinden erişim kontrolü elektronik devrelerine (1) bağlantısı sağlanır.

-Tuş takımının (3) mekân dışına bağlandığı halde, tercihe bağlı olarak erişim kontrol devresi (1) ilgili röle üzerinden kilitli kapının (10) kilit devresine bağlanır.

-Erişim kontrolü elektronik devresi (1), kendisine yapılacak sökme veya hasar verme saldırılarını bildirmek için ilgili röle devresi üzerinden alarm paneline (4) bağlanır.

-Erişim kontrolü elektronik devresine (1) sahadaki fiziki koşullara göre, USB kapısı üzerinden 5V veya başka bir enerji kaynağından 5V-30V arası bir enerji sağlanır.

C. Sistemin İşleyişi:

- Tek kullanımlık şifrenin (13) merkezi erişim kontrolü yönetim uygulamasında (5) bir kullanıcı (11) tarafından üretildiği durumda; Uygulama kullanıcısı (11), erişim sağlanması istenen mekanda yer alan erişim kontrolü elektronik devresi (1) için, erişim sağlayacak şifre kullanıcısı (12) için istenen gün ve saatte başlayacak ve istenen süre geçerli olacak bir tek kullanımlık şifre (13)üretir. Merkezi erişim kontrolü yönetim uygulaması (5) tek kullanımlık şifreyi üretmek için özel bir algoritma kullanır. Bu algoritmada erişim kontrolü elektronik devresini (1) belirlemek için uygulamada (5) kayıtlı olan benzersiz kimlik numarası ve ana anahtar kodu, şifre kullanıcısını (12) belirlemek için uygulamada (5) kayıtlı olan PIN (17) ve/veya personel sicil numarası (16) ve/veya temassız kimlik kartının (9) benzersiz kimlik numarası, epoch zaman değeri, geçerlilik süresi kodu ve fonksiyon kodu değişken olarak kullanılır. Uygulama kullanıcısı (11) bu şifreyi (13), şifre kullanıcısına (12) SMS (18) ve/veya IVR (19) ve/veya sesli arama (20) ve/veya e-posta (22) yöntemiyle iletir. Tek kullanımlık şifreyi (13) alan kullanıcı (12), şifrenin (13) geçerlilik süresi içerisinde mekânda bulunarak tuş takımına önce PIN (17) ve/veya personel sicil numarası (16) girer ve/veya temassız kartını (9) okutur. Daha sonra kendisine temin edilen tek kullanımlık şifreyi (13) tuşlar. Gömülü yazılım (2), merkezi erişim kontrolü yönetim uygulamasının şifreyi (13) üretmek için kullandığı özel algoritmayı ve değişkenleri kullanarak bir tek kullanımlık şifre (13) üretir. Üretilen şifre (13) ile kullanıcı (12) tarafından tuşlanan şifrenin (13) aynı olması halinde erişim kontrolü elektronik devresi alarm panelinin alarmını kapalı konuma getirir. Tuş takımının (3) mekânın dışında olduğu ve erişim kontrolü elektronik devresinin (1) kilitli kapıyla (10) bağlantılı olduğu durumlarda, erişim kontrolü elektronik devresi (1) alarmı kapalı konuma getirirken aynı zamanda kilitli kapının kilidini de röle devresi üzerinden tetikleyerek açılmasını sağlar.
- Tek kullanımlık şifrenin (13) şifre kullanıcısı tarafından tuş takımı üzerinden talep edildiği durumda; Şifre kullanıcısı (12) tuş takımına önceden belirlenmiş tercihlere göre kendisine verilmiş olan önce PIN (17) ve/veya personel sicil numarasını (16) girer ve/veya temassız kartını (9) okutur. Daha sonra tek kullanımlık şifre talebi için önceden belirlenmiş fonksiyon kodunu tuşlar. Gömülü yazılım (2) bu bilgilere belleğinde kayıtlı

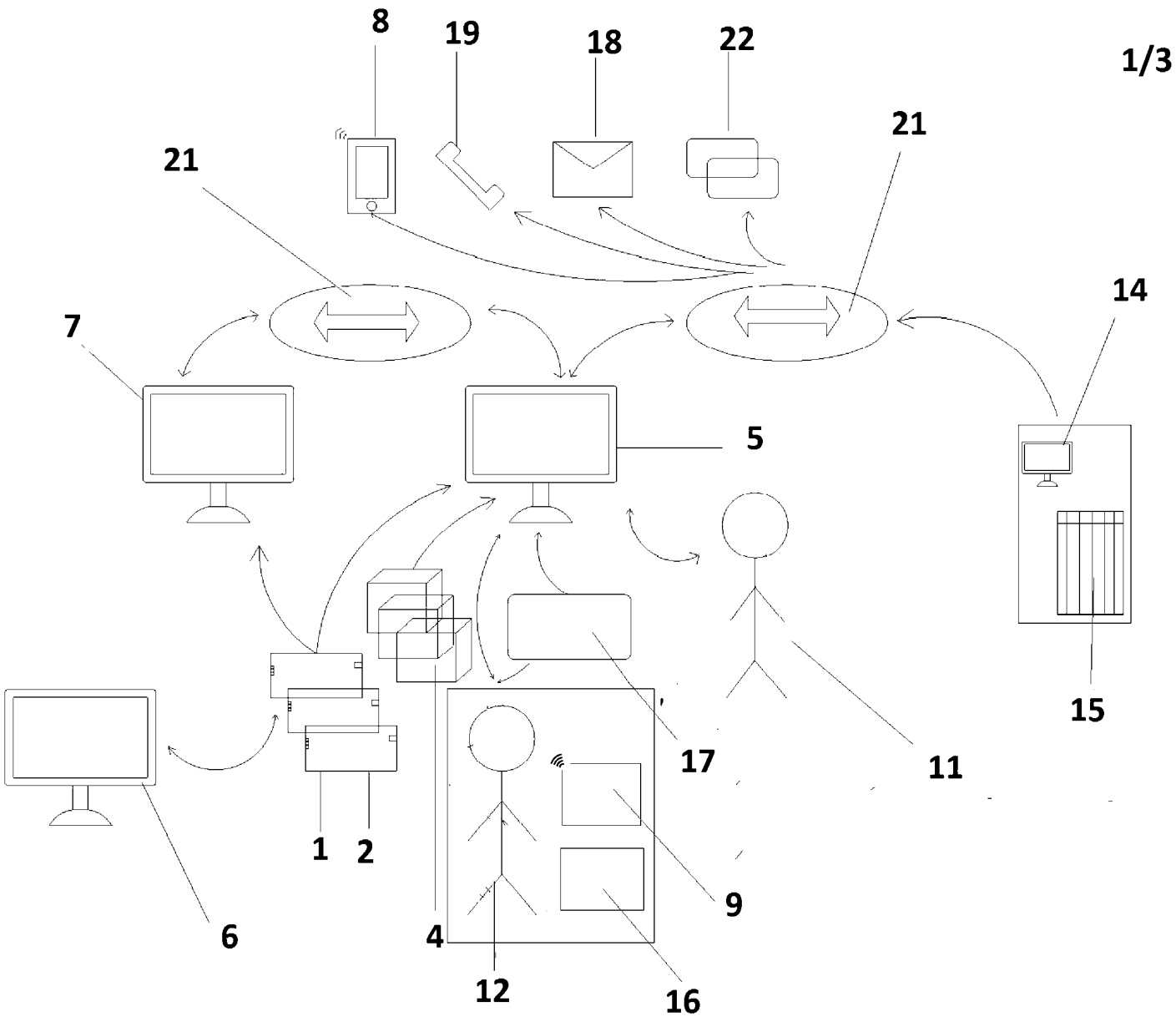
benzersiz kimlik numarasını da ekleyerek merkezi erişim kontrolü yönetim uygulamasına (5) iletir. Uygulama (5), erişim sağlanması istenen mekanda yer alan erişim kontrolü elektronik devresi (1) için, erişim sağlayacak şifre kullanıcısı (12) için talebin ulaştığı zaman için en kısa süreli zaman aralığında geçerli olacak bir tek kullanımlık şifre (13) üretir. Merkezi erişim kontrolü yönetim uygulaması (5) tek kullanımlık şifreyi üretmek için özel bir algoritma kullanır. Bu algoritmada erişim kontrolü elektronik devresini (1) belirlemek için uygulamada (5) kayıtlı olan benzersiz kimlik numarası ve ana anahtar kodu, şifre kullanıcısını (12) belirlemek için uygulamada (5) kayıtlı olan PIN (17) ve/veya personel sicil numarası (16) ve/veya temassız kimlik kartının (9) benzersiz kimlik numarası, epoch zaman değeri, geçerlilik süresi kodu ve fonksiyon kodu değişken olarak kullanılır. Merkezi erişim kontrolü yönetim uygulaması (5) şifreyi şifre kullanıcısına (12) SMS (18) ve/veya IVR (19) ve/veya sesli arama (20) ve/veya e-posta (22) yöntemiyle iletir. Tek kullanımlık şifreyi (13) alan kullanıcı (12), şifrenin (13) geçerlilik süresi içerisinde tuş takımına önce PIN (17) ve/veya personel sicil numarasını (16) girer ve/veya temassız kartını (9) okutur. Daha sonra kendisine temin edilen tek kullanımlık şifreyi (13) tuşlar. Gömülü yazılım (2), merkezi erişim kontrolü yönetim uygulamasının şifreyi (13) üretmek için kullandığı özel algoritmayı ve değişkenleri kullanarak bir tek kullanımlık şifre (13) üretir. Üretilen şifre (13) ile kullanıcı (12) tarafından tuşlanan şifrenin (13) aynı olması halinde erişim kontrolü elektronik devresi alarm panelinin alarmını kapalı konuma getirir. Tuş takımının (3) mekânın dışında olduğu ve erişim kontrolü elektronik devresinin (1) kilitli kapıyla (10) bağlantılı olduğu durumlarda, erişim kontrolü elektronik devresi (1) alarmı kapalı konuma getirirken aynı zamanda kilitli kapının kilidini de röle devresi üzerinden tetikleyerek açılmasını sağlar.

- Tek kullanımlık şifrenin (13) şifre kullanıcısı tarafından mobil uygulama üzerinden talep edildiği durumda; Tuş takımının (3) NFC okuyucusunun olduğu ve mobil uygulamanın (8) da NFC desteği olan bir mobil cihaz üzerinde çalıştırıldığı durumda, şifre kullanıcısı (12) mobil uygulamasını (8) çalıştırır ve cihazını tuş takımına yaklaştırır. Mobil uygulama (8) tuş takımı (3) ile iletişim kurar ve erişim kontrolü elektronik devresinin benzersiz kimlik numarasını okur. Şifre kullanıcısı (12) daha sonra mobil uygulamasına telefon numarasını ve/veya PIN (17) ve/veya personel sicil numarasını (16) girer ve tek kullanımlık şifre (13) talebini merkezi erişim kontrolü yönetim uygulamasına (5) iletir. Tuş takımının ve/veya mobil cihazın NFC okuyucu özelliğinin olmadığı hallerde şifre kullanıcısı (12) öncelikle mobil uygulama (8) üzerinden erişim sağlamak istediği mekanı seçer ve diğer kişi doğrulama bilgilerini de

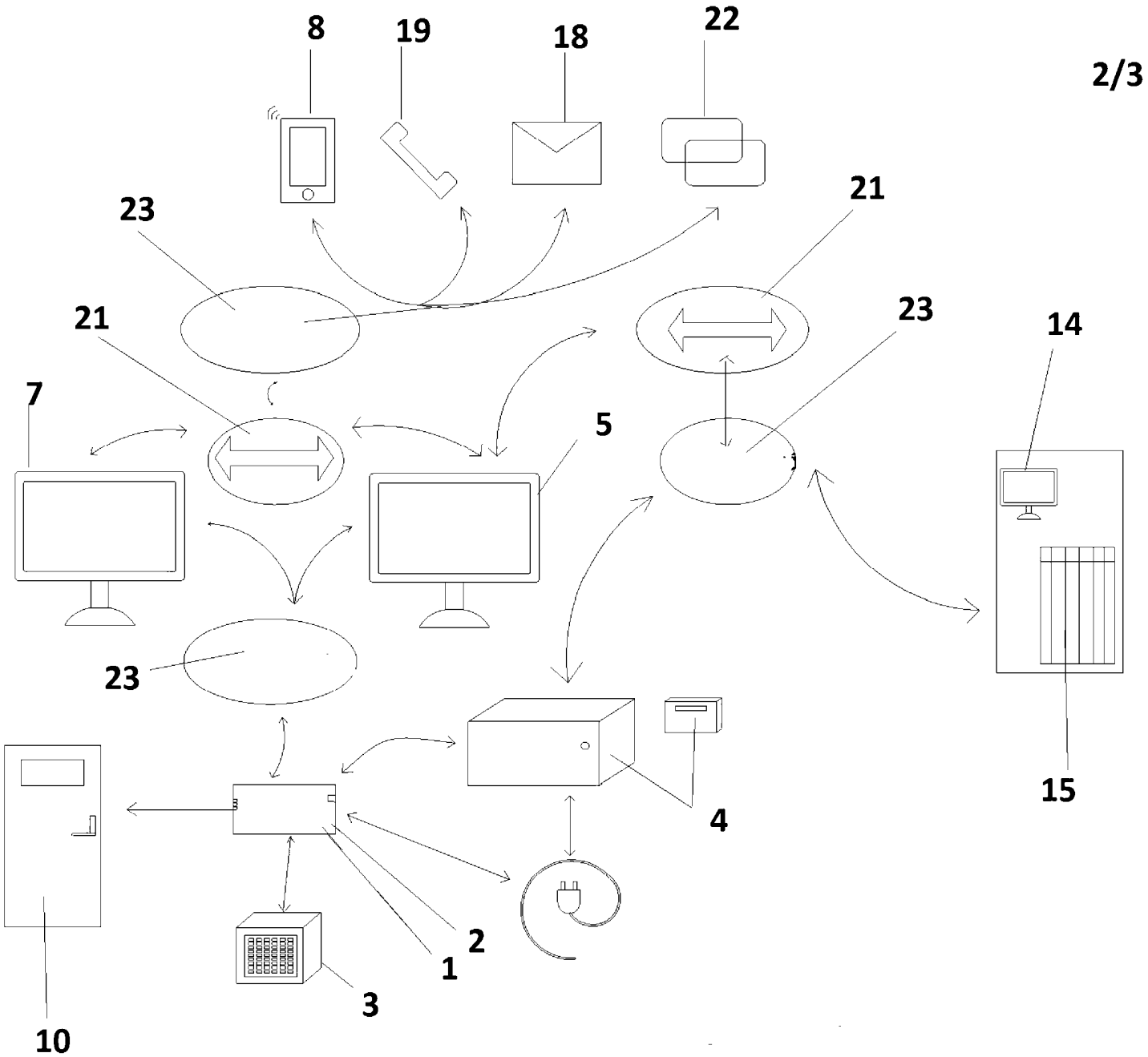
girerek tek kullanımlık şifre (13) talebini merkezi erişim kontrolü yönetim uygulamasına (5) iletir. Uygulama (5), erişim sağlanması istenen mekanda yer alan erişim kontrolü elektronik devresi (1) için, erişim sağlayacak şifre kullanıcısı (12) için talebin ulaştığı zaman için en kısa süreli zaman aralığında geçerli olacak bir tek kullanımlık şifre (13) üretir. Merkezi erişim kontrolü yönetim uygulaması (5) tek kullanımlık şifreyi üretmek için özel bir algoritma kullanır. Bu algoritmada erişim kontrolü elektronik devresini (1) belirlemek için uygulamada (5) kayıtlı olan benzersiz kimlik numarası ve ana anahtar kodu, şifre kullanıcısını (12) belirlemek için uygulamada (5) kayıtlı olan PIN (17) ve/veya personel sicil numarası (16) ve/veya temassız kimlik kartının (9) benzersiz kimlik numarası, epoch zaman değeri, geçerlilik süresi kodu ve fonksiyon kodu değişken olarak kullanılır. Merkezi erişim kontrolü yönetim uygulaması (5) şifreyi şifre kullanıcısının (12) mobil uygulamasına (8) iletir. NFC üzerinden iletişim kurulduğu hallerde şifre kullanıcısı (12) mobil cihazını tuş takımına tekrar yaklaştırarak şifrenin (13) tuş takımı (3) üzerinden erişim kontrolü elektronik devresine iletilmesini sağlar. NFC bağlantının olmadığı hallerde, tek kullanımlık şifreyi (13) mobil uygulama ekranında görüntüleyen kullanıcı (12), şifrenin (13) geçerlilik süresi içerisinde tuş takımına önce PIN (17) ve/veya personel sicil numarasını (16) girer ve/veya temassız kartını (9) okutur. Daha sonra kendisine temin edilen tek kullanımlık şifreyi (13) tuşlar. Gömülü yazılım (2), merkezi erişim kontrolü yönetim uygulamasının şifreyi (13) üretmek için kullandığı özel algoritmayı ve değişkenleri kullanarak bir tek kullanımlık şifre (13) üretir. Üretilen şifre (13) ile kullanıcı (12) tarafından tuşlanan şifrenin (13) aynı olması halinde erişim kontrolü elektronik devresi alarm panelinin alarmını kapalı konuma getirir. Tuş takımının (3) mekânın dışında olduğu ve erişim kontrolü elektronik devresinin (1) kilitli kapıyla (10) bağlantılı olduğu durumlarda, erişim kontrolü elektronik devresi (1) alarmı kapalı konuma getirirken aynı zamanda kilitli kapının kilidini de röle devresi üzerinden tetikleyerek açılmasını sağlar.

- <u>Uzaktan izleme ve kontrol uygulaması (7) ile erişim kontrol elektronik devrelerinin (1) uzaktan izlenmesi ve kontrol edilmesi:</u> Erişim kontrolü elektronik devresi (1) bir internet veya yerel ağa(23) bağlı olarak çalıştığı halde kendi durumuyla ilgili bilgileri uzaktan izleme ve kontrol uygulamasına (7) özel bir iletişim protokolü üzerinden gönderir. Durum bilgileri, Elektronik devrenin aktif olarak çalışıp çalışmadığı, herhangi bir hata durumunun olup olmadığı, varsa hatanın ne olduğu, cezalı konumda olup olmadığı, rölelerin durumu gibi verileri içerir. Ayrıca, uzaktan izleme ve kontrol uygulaması (7) erişim kontrolü elektronik devresini (1) uzaktan kontrol edebilir. Bu

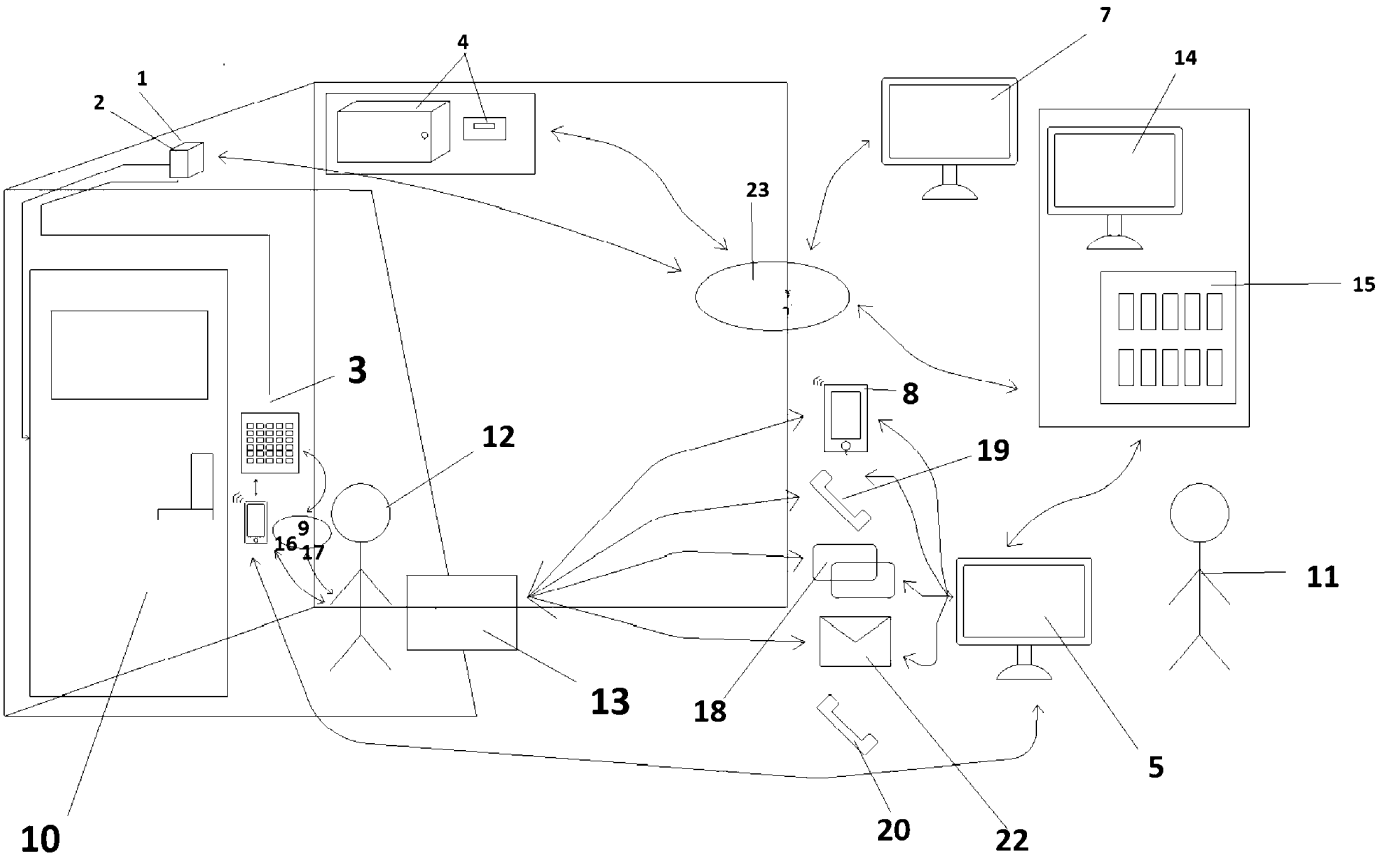
kapsamda uygulama (7) elektronik devrenin (1) üzerinde yüklü olan gömülü yazılımdan (2) seri numarası, ürün kodu, gömülü yazılım (2) sürüm numarası, çalışma değişken değerleri, geçmiş işlem kayıtları gibi bilgileri alabilir, elektronik devrenin (1) kapanıp açılmasını sağlayabilir, gömülü yazılım (2) ve çalışma değişken değerlerini yeni sürümlerle güncelleyebilir ve zaman kontrolü ve güncellemesi yapabilir. Uzaktan izleme ve kontrol uygulaması (7), sahadaki erişim kontrolü elektronik devrelerinden (1) topladığı gerçek zamanlı verileri grafik ve tablolardan oluşan bir gösterge ekranında özetlerken aynı zamanda kendi veri tabanında saklayarak geçmişe yönelik raporlama ve analiz işlemlerini yürütür. Uzaktan izleme ve kontrol uygulaması (7), otomatik uyarı mekanizması sayesinde erişim kontrolü elektronik devrelerinden (1) gelen hata ve durum bilgileri uyarınca önceden tanımlanmış kurallar çerçevesinde otomatik uyarı bildirimlerinde bulunur. Uzaktan izleme ve kontrol uygulaması (7), web servisleri (21) aracılığı ile merkezi erişim kontrolü yönetim uygulaması ile de anlık veri alışverişinde bulunur.



ŞEKİL 1



ŞEKİL 2



ŞEKİL 3