(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 821 262 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:
22.08.2007 Patentblatt 2007/34

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Anmeldenummer: **07002999.6**

(22) Anmeldetag: **13.02.2007**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL BA HR MK YU

(30) Priorität: **13.02.2006 AT 2182006**

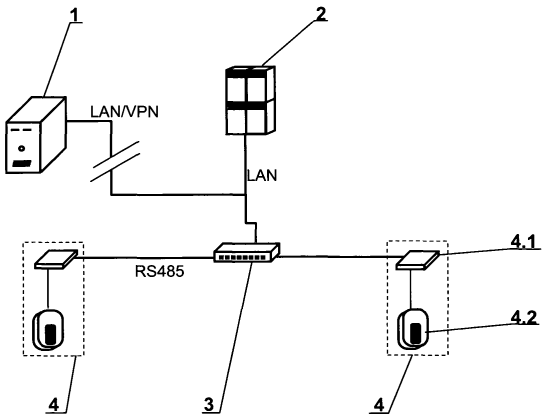
(71) Anmelder: **Gallner, Leopold**
4491 Niederneukirchen (AT)

(72) Erfinder:
- **Gallner, Leopold, Dr.**
  4491 Niederneukirchen (AT)
- **Moser, Thomas, Ing.**
  4052 Ansfelden (AT)
- **Keldorfer, Signot**
  4600 Wels (AT)

(54) **System zur Kontrolle von Berechtigungen von Personen, zu autorisierende Tätigkeiten durchzuführen**

(57) Die Erfindung betrifft eine Anlage zur Kontrolle der Vergabe von Möglichkeiten an Personen, zu autorisierende Tätigkeiten in verteilt angeordneten Gebäuden durchzuführen. Ein typischer Anwendungsfall ist die Vergabe von Zutrittsberechtigungen von Personen zu Gebäuden oder Räumen, und die Aufzeichnung der Zutrittsdaten. Ein Zentralserver (1) ist über Datenübertragungsverbindungen mit den Terminals (4) an den einzelnen Kontrollstellen verbunden. Am Zentralserver (1) sind die relevanten Daten aller Terminals und Personen gespeichert. An den einzelnen Terminals (4) sind die relevanten Daten genau jener Personen nochmals gespeichert, welche an diesen Terminals Berechtigung haben, eine zu autorisierende Tätigkeit durchzuführen. Die Entscheidung ob im Anlassfall einer Person an einem Terminal (4) eine zu autorisierende Tätigkeit ermöglicht wird, wird im Terminal (4) anhand der in ihm gespeicherten Information durchgeführt, ohne dass es dazu einer aufrechten Datenübertragungsverbindung zum Zentralserver (1) bedarf. Das Terminal (4) registriert die Information wann welche Person welche Berechtigung ausgeübt hat, und sendet diese Information an den Zentralserver (1). Wenn die Datenübertragungsverbindung zum Zentralserver (1) unterbrochen ist wird diese Information im Terminal so lange zwischengespeichert, bis die Verbindung wieder aufrecht ist, dann wird die Information übertragen.

Fig. 1



EP 1 821 262 A2

Beschreibung

[0001] Die Erfindung betrifft ein System zur Kontrolle von Berechtigungen von Personen, zu autorisierende Tätigkeiten durchzuführen. Das System ist insbesondere zur Verwaltung einer großen Anzahl von Berechtigungen an örtlich beliebig voneinander entfernt angeordneten Gebäuden vorteilhaft anwendbar. Ein typischer Anwendungsfall ist die Verwaltung von Zutrittsberechtigungen. In einer vorteilhaften Ausführungsform werden biometrische Daten der im System registrierten Personen als Erkennungsmerkmale angewendet.

[0002] Entsprechend der EP 523 908 B1 wird die Unterschrift einer Person als Schlüsselinformation für die Zugangskontrolle verwendet. Kennzeichnende Informationen zur Art des Unterschreibens einer prinzipiell zutrittsberechtigten Person werden einmalig an Hand von Unterschriften erstellt und gespeichert. Will diese Person dann konkret einen Zutritt erlangen, muss sie wieder eine Unterschrift leisten, daraus werden Daten generiert, welche mit den gespeicherten Daten verglichen werden. Bei ausreichender Übereinstimmung wird Zutritt gewährt. Entsprechend diesem System ist es nicht mehr erforderlich, einen als Schlüssel wirkenden Gegenstand mitzuführen oder ein Passwort anzuwenden. Über die Verwaltung von Zutrittsberechtigungen in entfernt voneinander angeordneten Gebäuden mit insgesamt vielen Zutrittsöffnungen wird nichts ausgesagt.

[0003] Die DE 296 02 655 U1 beschreibt ein System zur Vergabe von Zutrittsrechten an dezentralen Einrichtungen. Die Kontrollgeräte an den jeweiligen Türen sind nicht mit der Zentraleinheit verbunden. Sie erhalten Zutrittsregeln in Form von Daten, welche auf einem mobilen Datenträger manuell herangebracht werden, und nachdem die Leseeinheit aufgesperrt wurde, eingelesen werden. Die Eintritt begehrenden Personen müssen über eine Eingabeeinheit, z.B. einen Zifferntastatur gültige Schlüsselinformationen eingeben. Das Kontrollgerät kann auch Daten aufnehmen, beispielsweise wer wann gekommen und gegangen ist. Im Bedarfsfall müssen diese Daten mittels mobilem Datenträger manuell zur Zentraleinheit gebracht werden. Vorteilhaft an diesem System ist, dass es keines aufrechten Datennetzes zwischen Zentraleinheit und verteilt angeordneten Kontrollgeräten bedarf. Nachteilig ist, dass der Datenaustausch zwischen Zentraleinheit und verteilt angeordneten Kontrollgeräten durch physischen Transport eines Datenträgers, und damit sehr langsam und umständlich, erfolgt. Diese Methode ist daher nur dann sinnvoll anwendbar, wenn alle Anlagenteile geografisch nahe aneinander liegen.

[0004] Die AT 410 489 B beschreibt ein System zur Anmeldung an einer verteilten Datenverarbeitungsanlage unter Zuhilfenahme eines biometrischen Merkmals. Die Besonderheit dabei ist, dass jene Daten, welche als Schlüssel für den Zugang dienen, immer getrennt bleiben von den Daten, mit welchen der Benutzer dann tatsächlich arbeitet. Das wird erreicht, indem für die Benutzererkennung ein anderer zentraler Rechner verwendet wird, als für die Anwendungen, welche nach erfolgter Erkennung zugänglich gemacht werden. Das ist bei Verwendung der Anlagenhardware durch mehrere Anbieter, welche darauf Software laufen haben, aus Datenschutzgründen sehr vorteilhaft. Die Benutzerkennung ist in einem zentralen Datenspeicher abgelegt und wird im Bedarfsfall unter automatisiertem, elektronischem Austausch von Information mit einer an einem Endgerät aktuell aufgenommenen Benutzerkennung verglichen. Über weitere Details dieses Informationsaustausches oder der Benutzerverwaltung wird nichts ausgesagt.

[0005] Die EP 1 460 508 A1 beschreibt die Zugangskontrolle zu einer Datenverarbeitungsanlage, welche auch verteilt angeordnet sein kann. Zugang wird gewährt, wenn ein einzugebendes Identifikationsmerkmal, welches auch ein biometrisches Merkmal sein kann, mit einem Merkmal zusammenpasst, welches auf einem mitgeführten, per Funk kommunizierenden Datenträger gespeichert ist. Diese Methode ist gegenüber einer Zugangskontrolle, welche allein auf einem mitgebrachtem Schlüssel aufbaut, sicherer. Weiters ist vorteilhaft, dass für die Entscheidungsfindung ob Einlass gewährt wird oder nicht, keine Kommunikation mit einem zentralen Server erforderlich ist. Nachteilig ist, dass ein Teil ähnlich einem Schlüssel mitgeführt werden muss.

[0006] Die WO 2004/034335 A1 beschreibt ein mehrstufiges Zutrittskontrollsystem für ein Gebäude. Das System besteht aus einem zentralen Rechner und damit über Datenkanäle verbunden lokalen, speicher- und rechenfähigen Prüfstellen an den einzelnen Eingängen. Zur Überprüfung der Identität einer Zutritt begehrenden Person werden lokal aufgenommenen Daten an den zentralen Rechner gesandt und dort mit zentral gespeicherten Kennzeichnungsdaten verglichen. Abhängig von der Übereinstimmung wird ein entsprechendes Signal an die jeweilige Prüfstelle gesandt. An den einzelnen Prüfstellen sind weder Identifizierungsdaten zu den einzelnen Personen noch Daten über die Zutrittsfrequenz gespeichert. Das System braucht zur Überprüfung der Zutrittsberechtigung einer Person eine aufrechte Datenverbindung zum Server. Über diese Datenverbindung muss im Fall des Zutrittsbegehrens auch die zur Überprüfung der Identität erforderliche Information über ein biometrisches Merkmal, also eine relativ große Datenmenge, übertragen werden. Dass das System nur für lokal begrenzte Anwendungsfälle gedacht und auch nur dafür gut verwendbar.

[0007] Die GB 2 331 825 A beschreibt ein Erkennungssystem für Personen zwecks Zugriff von außen auf eine in einem zentralen Server angelegte Datenbank. Dabei wird ein Fingerprint verwendet, welcher im zentralen Server und auf einer mitzubringenden Karte gespeichert ist. Am lokalen Terminal wird erst ein aktuell vor Ort aufzunehmender Fingerprint mit dem auf der Karte gespeicherten verglichen, dann wird alles an den Server gesandt und dort nochmals mit gespeicherten Daten verglichen. Wenn alles passt wird vom Server ein Signal an

das lokale Terminal gesandt auf welches hinauf Zugriff auf die zentrale Datenbank ermöglicht wird. Das System bietet eine hohe Sicherheit auch gegen Manipulationen durch Dritte am Datenübertragungsnetz. Zur Überprüfung der Identität der um Zutritt ansuchenden Person ist ein Datenaustausch mit dem zentralen Server erforderlich, wobei zudem je Identifizierungsvorgang eine erhebliche Datenmenge übertragen werden muss. Damit ist für diesen Vorgang das Vorhandensein einer funktionstüchtigen Datenverbindung zwischen lokalem Terminal und zentralem Server eine wesentliche Grundvoraussetzung.

[0008] Die WO 2001/091038 A1 beschreibt eine Anlage und ein Verfahren zur Kontrolle des Zutrittes von Personen zu gesicherten Gebäuden oder ähnlichen Arealen. Die Anlage besteht aus einem zentralen Server, aus einzelnen, lokal angeordneten Zutrittskontrolleinheiten und einem Kommunikationskanal zur Verbindung zwischen Server und Zutrittskontrolleinheiten. Von zutrittsberechtigten Mitarbeitern werden Stammdaten, welche auch Biometriedaten wie z.B. Fingerprint beinhalten erfasst, gespeichert und soweit für die Überprüfung vor Ort erforderlich, an die Zutrittskontrolleinheiten gesandt, dort wieder gespeichert und weiter dazu verwendet in dann vom Server unabhängiger Weise im Bedarfsfall Zutrittsbegehren zu prüfen. Gegenüber dem Server sind alle Zutrittskontrolleinheiten gleich. Eine Person kann nur entweder an allen Zutrittskontrolleinheiten Zutrittsmöglichkeit haben, oder an keiner. An jede dieser Einheiten wird der zur Prüfung der Zutrittsberechtigung erforderliche Datensatz von allen im System registrierten Personen gesandt. Damit wächst der Speicherplatzbedarf an jeder einzelnen Zutrittskontrolleinheit proportional mit der Anzahl der im Gesamtsystem erfassten Personen auch dann wenn an einzelnen Zutrittskontrolleinheiten nur ganz wenige berechtigte Personen tatsächlich Zutritt brauchen.

[0009] Von diesem Stand der Technik ausgehend liegt die der Erfindung zu Grunde liegende Aufgabe darin, wie die WO 2001/091038 A1 ein gemeinsames Kontrollsystem für Personen für zu autorisierende Tätigkeiten, wie z.B. das Passieren durch ein Tor, die Inbetriebnahme von Maschinen oder das Ein- und Ausschalten von Alarmsystemen, in beliebig weit voneinander und verteilt angeordneten Gebäuden und Räumen vorzuschlagen, wobei auch dann kontrollierte Autorisierung möglich sein soll, wenn zwischen den einzelnen Kontrollstellen und einem zentralen Server vorübergehend keine aufrechte Datenverbindung besteht. Gegenüber dem System entsprechend der WO 2001/091038 A1 soll das System besser für eine größere Gesamtanzahl an Kontrollstellen und berechtigten Personen ausbaubar sein, es soll mit einem kleineren Datenspeicher je Kontrollstelle das Auslangen gefunden werden und es soll in wirtschaftlich sinnvollem Rahmen um nützliche weitere Funktionen ergänzt werden.

[0010] Für das bessere Verständnis sei hiermit die Bedeutung einzelner Begriffe im Sinne dieses Beschreibung geklärt:

"Autorisierung" - ist die "kontrollierte Zuweisung von Zugriffsrechten". Dazu wird die Identität einer Person, welche Rechte begehrt überprüft, und es wird bei positivem Ergebnis eine Handlung gesetzt , durch welche diese Person die Rechte in Anspruch nehmen kann, beispielsweise wird eine Sperre geöffnet.

"Kontrollstelle" - ist einer von mehreren Orten an denen Autorisierung stattfindet.

"Terminal" - ist ein technisches Gerät, welches als Teil des Kontrollsystems an einer Kontrollstelle angeordnet ist.

[0011] Zur Lösung der Aufgabe wird eine Anlage verwendet, bei welcher an jeder Kontrollstelle ein Terminal angeordnet ist, welches eine Identifizierungseinrichtung, eine Sperrenbetätigungseinrichtung und eine Datenaufzeichnungseinrichtung umfasst. Diese Terminals sind über ein Datenverarbeitungssystem, welches einen einzelnen Zentralserver und mehrere darunter angeordnete Terminalserver umfasst, vernetzt. Im Zentralserver sind die erforderlichen Informationen über alle Gebäude und zutrittsberechtigten Personen - des Weiteren vereinfacht "Mitarbeiter" genannt - gespeichert. In den einzelnen Terminals ist die für den autarken Betrieb des jeweiligen Terminals erforderliche Teilmenge dieser Informationen ebenfalls gespeichert. Die hierarchisch zwischen den Terminals und dem Zentralserver liegenden Terminalserver steuern den Datentransfer zwischen dem Zentralserver und jeweils einer Teilmenge der Terminals. Erfindungsgemäß ist vorgesehen, dass an die einzelnen Terminals nur Informationen bezüglich jener Mitarbeiter gesandt werden und dort gespeichert werden, welche an den jeweiligen Kontrollstellen tatsächlich Berechtigungen haben. Weiters ist erfindungsgemäß vorgesehen, dass an den einzelnen Terminals die Daten wer, wann und wo die Berechtigung ausgeübt hat, erfasst und an den zentralen und Server gesandt werden. Sollte die Datenverbindung zwischen einem Terminal und dem Server ausfallen, werden die zwischenzeitlich am Terminal anfallenden derartigen Daten am Terminal zwischengespeichert bis die Datenverbindung wieder aufrecht ist und sie an den Server mitgeteilt werden.

Die Erfindung wird an Hand einer beispielhaften Zeichnung im Detail erklärt:

[0012]

Fig. 1: zeigt ein Überblicksschaltbild für eines repräsentativen Ausschnittes eines erfindungsgemäßen Kontrollsystems.

[0013] In dem je vernetzten Zutrittkontrollsystem nur einmal erforderlichen Zentralserver 1 ist eine zentrale Datenbank mit allen für das Zutrittsystem erforderlichen

Terminal- und Miterbeiterstammdaten eingerichtet. Terminals und Mitarbeiter sind in dem Datenverarbeitungssystem eindeutig identifizierbar registriert. Zu jedem Mitarbeiter ist festgelegt, zu welchen Zeiten er welches Terminals durchschreiten kann, bzw. zu jedem Terminal ist festgelegt, wann es durch welchen Mitarbeiter durchschritten werden kann. Darüber hinaus umfassen die Stammdaten je Mitarbeiter zumindest einen eindeutigen Namen und eine eindeutige Identifizierungsinformation. Diese Identifizierungsinformation kann beispielsweise eine komprimierte Information sein, welche durch einen Bildverarbeitungsalgorithmus aus einem Bild eines Fingerabdrucks des Mitarbeiters gewonnen wird.

[0014] Der Zentralserver 1 ist mit mehreren Terminalservern 2 verbunden. Bei räumlicher Nähe kann diese Verbindung über ein LAN gebildet sein. Ein LAN (Lokal Area Network) in diesem Sinne ist eine Vernetzungsmethode zwischen zueinander in näherer Umgebung befindlichen Computern. Zurzeit ist eine dafür häufig konkret angewandte Technologie der sogenannte Ethernet-Standard. Bei größerer Entfernung - es kann über Kontinente reichen - kann die Verbindung über einen VPN-Kanal im Internet hergestellt werden. Ein VPN-Kanal in diesem Sinne ist ein Datenübertragungsprotokoll, durch welches ein Informationsfluss über ein an sich öffentliches Datennetz so abgewickelt wird, dass es für die beteiligten Partner so erscheint, als würden sie nur über ein intern zugänglichen Datennetz miteinander kommunizieren. Derartige Übertragungsmethoden sind Stand der Technik und brauchen hier nicht weiter beschrieben zu werden.

[0015] Ein Terminalserver 2 stellt über ein LAN die Weitere Datenverbindungen zu geografisch in der Nähe befindliche LAN/RS485-Konvertern 3 her. An diesen Konvertern 3 erfolgt eine Übersetzung der Datenübertragung zwischen dem im LAN angewandten Format und dem einfacher zu verkabelnden, sehr robusten, aber nicht so schnellen Format RS485. In diesem Format wird der Datenaustausch mit den einzelnen Terminals 4 abgewickelt.

[0016] Ein Terminal 4 ist im Bereich der Kontrollstellen, beispielsweise von zu kontrollierenden Türen bzw. Tore von Gebäuden oder Räumen angebracht. Zumindest im Fall von Türen bzw. Toren sollte es aus einer Inneneinheit 4.1, durch welche die Sperre betätigt wird und einer Außeneinheit 4.2, an welcher das Identifizierungsmerkmal der Durchgang begehrenden Mitarbeiter aufgenommen und mit gespeicherten Merkmalen verglichen wird bestehen. Über solch ein Terminal können drei Relais geschaltet und die damit verbundenen Aktionen wie zum Beispiel das Öffnen einer Tür durchgeführt werden.

[0017] Nachdem bei der Instandsetzung eines derartigen Kontrollsystems die erforderlichen Geräte montiert und die erforderlichen Leitungsverbindungen hergestellt sind, werden im Zentralserver 1 die einzelnen Geräte, also Terminals 4, LAN/RS485-Konverter 3 und Terminalserver 2 registriert. Dann werden die Stammdaten der einzelnen Mitarbeiter angelegt und es wird festgelegt, an welchen Terminals zu welchen Zeiten die einzelnen Mitarbeiter passieren dürfen. Diese Registrierungseingaben werden durch einen berechtigten Systemadministrator, welcher auf den Zentralserver 1 Zugriff hat, durchgeführt. Teil dieser Registrierungsarbeiten ist es auch, Identifizierungsinformationen der einzelnen Mitarbeiter anzulegen. Beispielsweise kann dies geschehen, indem ein Bild eines Fingerabdrucks der Mitarbeiter eingelesen wird, daraus werden spezielle Merkmale herausgefiltert und als biometrischer Schlüssel im Zentralserver 1 abgespeichert. Dabei ist es möglich von einem Mitarbeiter mehrere Finger als biometrische Schlüssel aufzunehmen. Jedem Finger wird ein Relais zugeordnet. Auf diese Weise können durch eine Person wählbar mehrere verschiedene Aktionen über ein Terminal ausgelöst werden. Das Anlegen der Daten und die Aufnahme des biometrischen Schlüssels können auch dezentral an einem PC, der mit entsprechender Software und Aufnahmegerät ausgestattet ist und über eine entsprechende Netzanbindung verfügt, erfolgen.

[0018] Sobald ein Mitarbeiter "angelegt" ist, sendet der Zentralserver 1 an die betroffenen Terminals 4 ein Informationspaket, welches aus dem im Datenverarbeitungssystem verwendeten Namen dieser Mitarbeiters, seinem biometrischen Schlüssel und der Information über die Zeiten, an denen ihm bestimmte Berechtigungen - wie zum Beispiel Durchlass - gewährt werden, besteht. Die betroffenen Terminals übernehmen diese Informationen als Arbeitsanweisung und speichern sie im Fall eines Tores auf einem jeweils in der Außeneinheit 4.2 angebrachten lokalen Datenspeicher.

[0019] Wenn ein Mitarbeiter an einem Terminal 4 Durchlass begehrt, gibt er an einer an der Außeneinheit 4.2 angebrachten, als dunkler, rechteckförmiger Streifen erkennbaren Scanvorrichtung ein Bild seines Fingers ein, indem er mit dem Finger langsam über diesen Streifen streicht. Die Außeneinheit verarbeitet dieses Bild in einer in ihr angebrachten lokalen Datenverarbeitungseinheit derart weiter, dass daraus spezielle Merkmale herausgefiltert werden, welche mit den gespeicherten biometrischen Schlüsseln, welche vom Zentralserver 1 früher mitgeteilt wurden, vergleichbar sind. In der lokalen Datenverarbeitungseinheit der Außeneinheit 4.2 werden die neu herausgefilterten Merkmale mit den gespeicherten Merkmalen von zum Durchgang berechtigten Mitarbeitern verglichen. Falls eine Übereinstimmung festgestellt wird, gilt der Mitarbeiter als erkannt und es wird Durchgang gewährt, indem ein entsprechendes Signal an die zugehörige Inneneinheit 4.1 gesandt wird, welche durch Schalten des entsprechenden Relais die gewünschte Aktion, in diesem Fall das Öffnen der Sperre, veranlasst. Durch die Aufteilung des Terminals 4 in eine Inneneinheit 4.1 und eine Außeneinheit 4.2 kann besser an die durch die Inneneinheit auszulösenden individuell sehr verschiedenen Sperren angepasst werden, als mit einer komplexeren Gesamteinheit.

[0020] Die Information dass der betreffende Mitarbeiter zu dem betreffenden Zeitpunkt am betreffenden Ter-

minal 4 eine Aktion ausgelöst hat, wird vom Terminal 4 über den übergeordneten LAN/RS485-Konverter 3 und den weiter übergeordneten Terminalserver 2 an den Zentralserver 1 mitgeteilt und dort aufgezeichnet.

[0021] Falls die Datenverbindung zwischen Terminal 4 und Zentralserver 1 nicht funktioniert, was zumindest temporär sicher nicht ausgeschlossen werden kann, ändert sich die den Mitarbeiter betreffende Funktion des Terminals überhaupt nicht. Die für das Prüfen und ggf. Gewähren von Rechten einzelner Mitarbeiter erforderlichen Daten befinden sich lokal im Terminal 4, und die erforderliche Datenverarbeitung erfolgt auch lokal im Terminal 4. Der einzige Unterschied zur Arbeitsweise bei bestehender Datenverbindung zum Zentralserver 1 besteht darin, dass die Information dass Mitarbeiter x zum Zeitpunkt y am Terminal z mittels biometrischen Schlüssels das Relais a betätigt hat, nicht sofort an den Zentralserver 1 mitgeteilt wird, sondern vorerst nur im Terminal 4 gespeichert wird und erst dann an den Zentralserver 1 mitgeteilt wird, wenn die Datenverbindung wieder funktioniert.

[0022] Wenn am Zentralserver 1 Daten, welche einzelne Terminals betreffen, geändert werden, während die Datenverbindung zu diesen Terminals unterbrochen ist, so arbeiten diese Terminals so lange entsprechend dem vorherigen Datenstand bis die Datenverbindung wieder hergestellt ist. Dann werden sie aktualisiert.

[0023] Durch die Arbeitsweise mit doppelt angelegten Daten, - einerseits am Zentralserver 1, andererseits an den betroffenen Terminals 4, - wird einerseits extrem gute Verwaltbarkeit der Daten, da über den Zentralserver 1 alle Daten editierbar sind, andererseits extreme Robustheit der Funktion erreicht, da die Terminals 4 auch dann ordnungsgemäß arbeiten, wenn die Datenübertragung - deren ununterbrochenes Funktionieren nicht gewährleistet werden kann - unterbrochen ist.

[0024] Vor allem um nicht jene Personen, welche nur in Einzelfällen spezifische Rechte an einem Terminal brauchen, in der Gesamtanlage registrieren zu müssen, aber auch aus Sicherheitsgründen ist es sinnvoll, an den einzelnen Gebäudestandorten direkte Zugriffsmöglichkeiten für berechtigte Mitarbeiter auf die dort vorhandenen Terminals vorzusehen. So können mittels Relaisschaltung zum Beispiel Tore kurzzeitig bei Ankommen einer Lieferung ohne vorhergehenden Identifizierungsvorgang geöffnet werden. Oder es kann kurzfristig der Zugang für einzelne Mitarbeiter auch dann gesperrt werden, wenn die Datenübertragung zum Zentralserver ausgefallen ist. Diese Zugriffsmöglichkeit ist am besten über PC-Arbeitsplätze, herstellbar, welche mit jenen Terminalservern 2 über LAN verbunden sind, welche auch die Verbindung zu den betroffenen Terminals 4 herstellen.

[0025] Natürlich ist es sinnvoll, die im Zentralserver 1 erforderliche Datenbank über Mitarbeiter und Gebäude so auszulegen, dass im Bedarfsfall auch weitere dazupassende nützliche Informationen über Mitarbeiter bzw. Gebäude abgespeichert werden können bzw. dass ein Datenaustausch mit diesbezüglichen Datenbanken möglich ist.

[0026] Die Erfindung ist auch mit Kontrollstellen sinnvoll kombinierbar an denen als Identifizierungsmerkmal nicht ein biometrisches Merkmal aufgenommen wird, sondern beispielsweise ein manuell einzugebendes Passwort oder ein aus einem mitzubringenden Datenspeicher auszulesendes Passwort, Nummer, Signal oder überhaupt ein mechanischer Schlüssel.

[0027] Das Kontrollsystem wurde hier vor allem an Hand des wichtigen Anwendungsfalles "Gewähren bzw. Verweigern von Zutritt und Aufzeichnen der Zutrittsdaten" beschrieben. Die Anwendungsbereiche können aber auch viele andere autorisierende Tätigkeiten wie zum Beispiel die Inbetriebnahme von Maschinen etc. betreffen. In diesem Sinne ist der in der Beschreibung und im folgenden Anspruch verwendete Begriff "Sperrenbetätigungsvorrichtung" etwas allgemeiner als jene Vorrichtung zu sehen, durch welche eine Tür entriegelt wird.

Patentansprüche

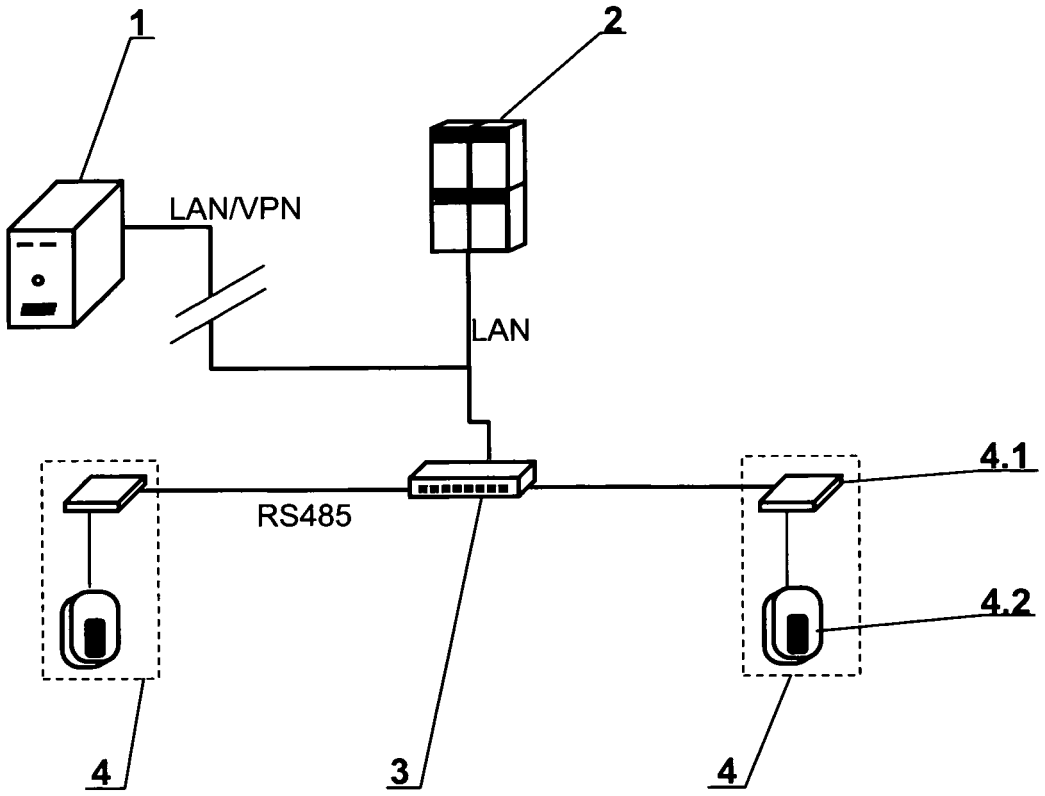
1. Kontrollsystem für zu autorisierende Tätigkeiten in verteilt angeordneten Gebäuden bzw. Räumen, wobei entsprechend einstellbaren Berechtigungen an Personen die Möglichkeit zu autorisierende Tätigkeiten zu verrichten gegeben oder verweigert wird, wobei an einzelnen Kontrollstellen ein Terminal angeordnet ist, welches eine Identifizierungseinrichtung für ein biometrisches Identifizierungsmerkmal, eine Sperrenbetätigungseinrichtung und eine Datenaufzeichnungseinrichtung umfasst, wobei die Anlage einen Zentralserver beinhaltet, in welchem die Information, welche Person durch welches biometrische Identifizierungsmerkmal erkennbar ist gespeichert wird, wobei zwischen dem Zentralserver und den einzelnen Terminals eine automatische Datenübertragungsverbindung eingerichtet ist, wobei die Information, welche zugangsberechtigten Personen durch welche Identifizierungsmerkmale erkennbar sind, automatisch vom Zentralserver über die Datenübertragungsverbindung an die Terminals mitgeteilt und dort gespeichert wird und dort unabhängig davon ob zum gegebenen Zeitpunkt die Datenübertragungsverbindung zum Zentralserver aufrecht oder unterbrochen ist, bei Ersuchen einer Person um Sperrenöffnung zur Überprüfung der Identität dieser Person angewendet wird, **dadurch gekennzeichnet dass** den einzelnen erfassten Personen konkret zugeordnet wird, an welchen konkreten Terminals (4) zu welchen Zeiten für sie die Sperre geöffnet werden kann, dass vom Zentralserver (1) an ein individuelles Terminal (4) nur bezüglich jener Teilmenge von insgesamt erfassten Personen Informationen gesandt werden, für welche genau an diesem individuellen Terminal (4) die Sperre geöffnet werden darf und dass das Terminal (4) die Information wann welche Person eine derartige Berechti-

gung ausgeübt hat registriert, erforderlichenfalls lokal zwischenspeichert und dann über die Datenübertragungsverbindung automatisch an Zentralserver (1) mitteilt, wenn die Datenübertragungsverbindung zum Zentralserver (1) aufrecht ist.

2. Kontrollsystem nach Anspruch 1, **dadurch gekennzeichnet, dass** es dazu verwendet wird, das Passieren von Personen durch Tore zu verwalten.

3. Kontrollsystem nach Anspruch 2, **dadurch gekennzeichnet, dass** die Terminals (4) aus einer Inneneinheit (4.1) und einer Außeneinheit (4.2) bestehen, welche getrennt angeordnet sind, wobei die Hauptfunktion der Inneneinheit (4.1) darin liegt, die Sperre der Durchlassstelle anzusteuern, während es Funktionen der Außeneinheit sind, die Identifizierung von Personen durchzuführen und die damit zusammenhängenden Daten zu speichern.

Fig. 1



IN DER BESCHREIBUNG AUFGEFÜHRTE DOKUMENTE

Diese Liste der vom Anmelder aufgeführten Dokumente wurde ausschließlich zur Information des Lesers aufgenommen und ist nicht Bestandteil des europäischen Patentdokumentes. Sie wurde mit größter Sorgfalt zusammengestellt; das EPA übernimmt jedoch keinerlei Haftung für etwaige Fehler oder Auslassungen.

In der Beschreibung aufgeführte Patentdokumente

- EP 523908 B1 **[0002]**
- DE 29602655 U1 **[0003]**
- AT 410489 B **[0004]**
- EP 1460508 A1 **[0005]**
- WO 2004034335 A1 **[0006]**
- GB 2331825 A **[0007]**
- WO 2001091038 A1 **[0008] [0009] [0009]**