



(10) **DE 11 2018 005 018 B4** 2021.02.18

(12) **Patentschrift**

(21) Deutsches Aktenzeichen: **11 2018 005 018.1**
 (86) PCT-Aktenzeichen: **PCT/IB2018/059157**
 (87) PCT-Veröffentlichungs-Nr.: **WO 2019/102362**
 (86) PCT-Anmeldetag: **21.11.2018**
 (87) PCT-Veröffentlichungstag: **31.05.2019**
 (43) Veröffentlichungstag der PCT Anmeldung
 in deutscher Übersetzung: **16.07.2020**
 (45) Veröffentlichungstag
 der Patenterteilung: **18.02.2021**

(51) Int Cl.: **G06F 21/00 (2013.01)**
G06F 21/32 (2013.01)

Innerhalb von neun Monaten nach Veröffentlichung der Patenterteilung kann nach § 59 Patentgesetz gegen das Patent Einspruch erhoben werden. Der Einspruch ist schriftlich zu erklären und zu begründen. Innerhalb der Einspruchsfrist ist eine Einspruchsgebühr in Höhe von 200 Euro zu entrichten (§ 6 Patentkostengesetz in Verbindung mit der Anlage zu § 2 Abs. 1 Patentkostengesetz).

(30) Unionspriorität:
15/821,036 **22.11.2017** **US**

(72) Erfinder:
Sugawara, Masaya, Tokyo, JP; Yanagisawa, Takashi, Tokyo, JP

(73) Patentinhaber:
International Business Machines Corporation, Armonk, N.Y., US

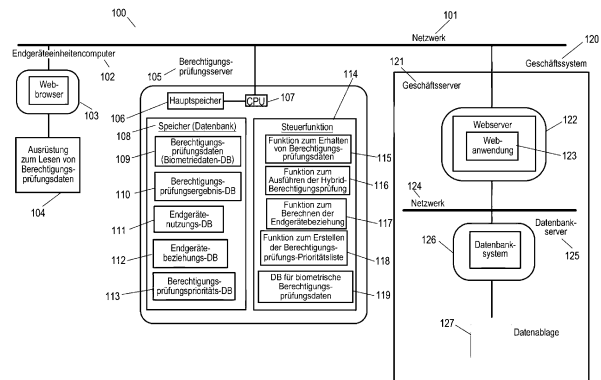
(56) Ermittelte Stand der Technik:

(74) Vertreter:
Richardt Patentanwälte PartG mbB, 65185 Wiesbaden, DE

US	2009 / 0 161 921	A1
US	2011 / 0 182 480	A1
US	2015 / 0 254 445	A1
US	2017 / 0 262 719	A1
US	2017 / 0 308 694	A1
US	2017 / 0 330 028	A1

(54) Bezeichnung: **BERECHTIGUNGSPRÜFUNG VON BENUTZERN AN MEHREREN ENDGERÄTEN**

(57) Zusammenfassung: Ein Berechtigungsprüfungssystem, das eine Berechtigungsprüfungs-Prioritätsliste benutzt, die auf dynamischer und virtueller Gruppierung von Endgeräten beruht die zur Berechtigungsprüfung verwendet werden wobei das System zu einer Effizienzverbesserung der Berechtigungsprüfungs-Prioritätsabfolge bei der 1:N-Berechtigungsprüfung und bei der Hybrid-Berechtigungsprüfung führt, indem die Berechtigungsprüfungslogik zwischen 1:1- und 1:N-Berechtigungsprüfung umgeschaltet wird. Maskieren zuvor angemeldeter Benutzer für die Berechtigungsprüfungs-Prioritätsliste bei 1:N-Berechtigungsprüfung verbessert die Effizienz der Berechtigungsprüfungs-Prioritätsabfolge bei der 1:N-Berechtigungsprüfung.



Beschreibung

Technisches Gebiet

[0001] Die vorliegende Erfindung ist auf ein Berechtigungsprüfungssystem gerichtet, das in einem IT-System auf der Grundlage biometrischer Daten eine Berechtigungsprüfungsverarbeitung des Systems dynamisch optimiert, indem sich das Berechtigungsprüfungssystem auf eine Verteilung der Benutzernutzung von Endgeräten stützt, wodurch eine Leistungsverbesserung der Berechtigungsprüfungsverarbeitung erreicht wird.

HINTERGRUND

[0002] Die dem Stand der Technik entsprechende Berechtigungsprüfung in IT-Systemen auf der Grundlage biometrischer Daten beinhaltet in der Regel, dass eine auf Kennwörtern beruhende Berechtigungsprüfung der Identität eines Benutzers wie zum Beispiel einer Benutzerkennung durch eine Berechtigungsprüfung ersetzt wird, die auf einer Eigenschaft beruht, die dem Benutzer angeboren ist, wie zum Beispiel Fingerabdrücke oder Netzhautmuster oder andere auf diesem Gebiet bekannte Eigenschaften. Diese angeborenen Eigenschaften werden üblicherweise als „biometrische Daten“ bezeichnet. In diesem Kontext nimmt die Berechtigungsprüfungsverarbeitung die Form einer sogenannten „1:1-Berechtigungsprüfung“ an, bei der biometrische Daten des Benutzers zum Zeitpunkt eines Berechtigungsprüfungsprozesses mit registrierten Daten dieses einen Benutzers verglichen werden.

[0003] Den jüngsten Tendenzen bei den steigenden Anforderungen an das Sicherheitsniveau von IT-Systemen folgend spielt eine hochgenaue Berechtigungsprüfung bei der biometrischen Berechtigungsprüfung eine wichtige Rolle.

[0004] Diese Art der hochgenauen Berechtigungsprüfung, die biometrische Berechtigungsprüfung, erfordert für den Betrieb jedoch einen Leistungsaufwand der System-CPU und führt manchmal zu einer langen Berechtigungsprüfungszeit. Da die biometrische Berechtigungsprüfung einen Vergleich von Eingaben und den Daten zwischen Differenzdaten erfordert, ist die Rechenlast für einen derartigen Prozess hoch, und die Berechtigungsprüfungszeit ist lang.

[0005] Bei einigen Umgebungen könnte ein einzelnes Endgerät durch viele Benutzer gemeinsam genutzt werden. Zum Beispiel könnten Registrierkassen im Supermarkt oder Check-In-Terminals am Flughafen durch mehr als einen Kassierer oder Angestellten der Fluggesellschaft genutzt werden.

[0006] Die Erkennung von Benutzern in einer derartigen Umgebung könnte so erfolgen, dass sich jeder Benutzer abmelden muss, wenn er das Endgerät verlässt, und sich jeder neue Benutzer anmelden muss, bevor er das Endgerät nutzen kann. Wenn jeder Benutzer seine Kennung vor der biometrischen Berechtigungsprüfung eingeben muss, wird diese Berechtigungsprüfung als „1:1-Berechtigungsprüfung“ bezeichnet. In diesem Fall würde die Berechtigungsprüfung durch Abgleichen zwischen angegebenen Daten vorgenommen werden und zu einer Transaktion mit konstanter Last veranlasst führen.

[0007] Die Anforderung, dass sich Benutzer häufig an- und abmelden müssen, kann bei Umgebungen mit gemeinsam genutzten Endgeräten problematisch sein, bei denen sich Kassierer oder Angestellte von Fluggesellschaften oder dergleichen an einem einzigen Endgerät mehrfach abwechseln, um zu vermeiden, dass lange Warteschlangen von Kunden entstehen. In diesem Fall ist es wünschenswert, dass sich nicht jeder Benutzer an- und abmelden muss, sondern stattdessen ein einziges gemeinsames Benutzerkonto und nicht ein einzelner Benutzer zum Anmelden am Endgerät verwendet wird, und anschließend eine biometrische Berechtigungsprüfung verwendet wird, sobald der Benutzer das Endgerät zu nutzen beginnt, an dem bereits eine Anmeldung erfolgte. Die Anzahl möglicher registrierter Benutzer für ein beliebiges Endgerät in einer derartigen Umgebung könnte in die Hunderte gehen, wobei alle ein einziges gemeinsames Benutzerkonto nutzen. Das Durchführen der Berechtigungsprüfung der Benutzer am gemeinsamen Benutzerkonto wird als „1:N-Berechtigungsprüfung“ bezeichnet, wobei ein Benutzerkonto „N“ mögliche Nutzer hat.

[0008] Es wird klar sein, dass aufgrund der ureigenen Art der Berechtigungsprüfung, die auf von den Benutzern abgeleiteten biometrischen Daten beruht, die Berechtigungsprüfung schnell durchgeführt werden muss, wenn eine Leistungsverbesserung erreicht werden soll, wenn bei jedem Benutzer lediglich die herkömmliche auf der Benutzerkennung beruhende Anmeldung und Abmeldung verlangt wird. Darüber hinaus muss dieser Prozess durchgeführt werden, während sich das System im Vergleich zur normalen 1:1-Berechtigungsprüfung in einem

stark belasteten Zustand befindet, der verständlicherweise und unausweichlich zu Verzögerungen bei den erforderlichen Prozessen führt.

[0009] Da diese Art der Nutzung eine schnelle Berechtigungsprüfung erfordert, besteht ein Bedarf an einer schnellen Verarbeitung unter Verwendung der biometrischen Berechtigungsprüfung.

[0010] Viele bestehende Konzepte realisieren eine Beschleunigung bei der 1:N-Berechtigungsprüfung über verschiedene Ansätze. In den folgenden Erläuterungen werden bestehende Erfindungen, die auf Ansätze zur Beschleunigung der 1:N-Berechtigungsprüfung gerichtet sind, in solche klassifiziert, die Bedeutung für die vorliegende Erfindung haben, und in solche, die wenig oder keine Bedeutung für die vorliegende Erfindung haben. Diese bestehenden Systeme können unter die folgenden Klassen fallen:

[0011] Auf Berechtigungsprüfungslogik beruhende Beschleunigung: Beschleunigung durch parallele Berechtigungsprüfungsverarbeitung, um mehrere Berechtigungsprüfungsprozesse auszuführen, mehrstufige Berechtigungsprüfung durch Erstellung repräsentativer Daten usw. Die Beschleunigung der Berechtigungsprüfung bei der Parallelverarbeitung ist nicht dazu gedacht, die gesamte Systemlast zu reduzieren, die im Zusammenhang mit der Berechtigungsprüfung steht. Eine Beschleunigung über repräsentative Daten berücksichtigt nicht die ungleichmäßige Verteilung der Prozesse und Aufgaben im Zusammenhang mit der Berechtigungsprüfung bei Benutzern. Ob repräsentative Daten erstellt werden können, hängt von Varianten ab, die bei der biometrischen Berechtigungsprüfung von Benutzern festgestellt werden.

[0012] Techniken im Zusammenhang mit biometrischen Berechtigungsprüfungsdaten: Funktionen im Zusammenhang mit dem Erhöhen der Genauigkeit biometrischer Berechtigungsprüfungsdaten und dem Bereitstellen zusätzlicher Informationen für den Hauptzweck der Verbesserung der Genauigkeit der biometrischen Berechtigungsprüfung zwischen mehreren Einheiten. Der Hauptzweck besteht darin, die Genauigkeit der Berechtigungsprüfung zum Zeitpunkt des Durchführens der 1:N-Berechtigungsprüfung anstelle der Beschleunigung der Berechtigungsprüfung an sich zu verbessern.

[0013] Verringern des Datenbereichs mit Hilfe eindeutiger Informationen: Beschleunigung durch Verringern des Bereichs von Berechtigungsprüfungsdaten durch Inhalte von Betriebsprozessen und -aufgaben für jeden Benutzer, indem die Dienst- und Endgeräteerkennung des bei dem Dienst verwendeten Endgeräts verwendet wird. Das Konzept der Beschleunigung und des Suchens nach jedem Benutzer unter Verwendung des Dienstes auf der Grundlage der Endgeräte ist als Beschleunigungskonzept nicht zufriedenstellend, da Benutzer zu diesem Zeitpunkt nicht bewusst die Randbedingung des Gedankens berücksichtigen, dass eindeutige Endgeräte in einer Umgebung vorliegen, in der an mehreren gemeinsam genutzten Endgeräten gemeinsame Benutzerkonten verwendet werden.

[0014] Optimierung durch Ähnlichkeit: Auf der Grundlage der Ähnlichkeit bei den erhaltenen biometrischen Informationen werden Punktbewertungen berechnet, um eine Unterbrechung und Beschleunigung der Berechtigungsprüfung zu erreichen. Die Verwendung der Ähnlichkeit ist ein Beschleunigungskonzept, das von den biometrischen Informationen der Benutzer abhängt, was sehr flexibel ist, aber keinerlei Auswirkungen einbezieht, die im Kontext dieses Falles wesentlich sind.

[0015] Zu bestehenden beispielhaften Fällen von Konzepten und den Problemen der Konzepte der jeweiligen bestehenden Erfindungen gehören folgende:

[0016] Beschleunigung der Berechtigungsprüfung durch Umschalten zwischen 1:1-Berechtigungsprüfung und 1:N-Berechtigungsprüfung: Dieses Verfahren ist auf ein Konzept der Beschleunigung durch Unterscheidung und Umschalten zwischen Prozessen der 1:1-Berechtigungsprüfung und 1:N-Berechtigungsprüfung gerichtet. Das bestehende Beschleunigungskonzept durch Umschalten zwischen 1:1- und 1:N-Berechtigungsprüfungen ist unter der Ermittlungsbedingung realisiert, dass das Vorliegen oder Fehlen einer der Berechtigungsprüfung zu unterziehenden beliebigen Eingabe einer Kennung ermittelt wird, die durch den Benutzer als Bedingung für das Verwenden der 1:1-Berechtigungsprüfung eingegeben wird. Bei der Umgebung, bei der eine Beschleunigung erreicht werden sollte, wird angenommen, dass Zugriffe durch Benutzer unter Verwendung des gemeinsamen Benutzerkontos vorgenommen werden.

[0017] Beschleunigung durch Gruppieren: Bei dem Beschleunigungsansatz durch Gruppieren handelt es sich um ein Konzept, das eine Beschleunigung realisiert, indem ein Gruppieren zahlreicher Datenelemente durchgeführt wird, die der Berechtigungsprüfung unterzogen werden, und die Priorität in der Reihenfolge der Berechtigungsprüfung und dergleichen verwaltet. Dieser Ansatz kann wie folgt charakterisiert werden:

[0018] A) Zu verwenden beim Verringern des Datenbereichs, der in aufeinanderfolgenden Berechtigungsprüfungsrounds durchsucht werden soll, indem einfach eine Liste von Datenelementen erstellt wird, deren Berechtigungsprüfung erfolgreich war. Hierbei tritt ein Problem in der Umgebung mit einem gemeinsamen Benutzerkonto und mehreren Benutzern auf, bei der angenommen wird, dass alle der 1:N-Berechtigungsprüfung unterliegenden Benutzer die Berechtigungsprüfung täglich durchführen, und bei dem Prinzip einfache Ergebnisse der erfolgreichen Berechtigungsprüfung nicht zum Suchen nach Beschleunigungsmöglichkeiten verwendet werden können.

[0019] B) Ausführen eines vorgegebenen Gruppierens zum Zeitpunkt der Registrierung der Berechtigungsprüfung. Bei der Zielumgebung handelt es sich um eine Umgebung, bei der zwischen oder unter gruppierten Benutzern eine weitere Beschleunigung erforderlich ist. Dementsprechend ist eine Beschleunigung durch Sortieren zum Zeitpunkt der Registrierung der Berechtigungsprüfung als Beschleunigung in der Zielumgebung nicht zufriedenstellend.

[0020] C) Konzept im Zusammenhang mit der Umkonfiguration gruppierter Daten. Hierbei handelt es sich um ein Konzept, das im Zusammenhang mit der Aufrechterhaltung der Optimierung der Konfiguration der Gruppensdaten steht und keinen erheblichen Beitrag zu einer Umgebung liefert, in der Zielgruppen im Wesentlichen feststehen.

[0021] D) Konzept im Zusammenhang mit dem Durchsuchen anhand von Eigenschaftsdaten beim Gruppieren. Wirksam bei erheblichen Unterschieden in den Merkmalen von biometrischen Berechtigungsprüfungsdaten bei der Berechtigungsprüfung anhand von Gesichtern und dergleichen, aber nur eingeschränkte Auswirkungen bei der Berechtigungsprüfung anhand von Fingerveinen und dergleichen.

[0022] Erhöhen des Wirkungsgrads durch Gruppieren von Berechtigungsprüfungsdaten derselben Person bei der 1:N-Berechtigungsprüfung. Trägt zu einer Zunahme bei den Berechtigungsprüfungsdaten derselben Person bei, hat jedoch nur begrenzte Auswirkungen auf die Zunahme der Gruppensdaten.

[0023] Ansätze zur Beschleunigung durch Gruppieren und 1:N-Umschalten und andere relevante Ansätze liegen je nach den Problemen reichlich vor, die durch Erfindungen nach dem Stand der Technik behandelt werden.

[0024] Diese bestehenden Patentveröffentlichungen hängen jedoch oftmals von den speziellen Problemen ab, auf die sie angewendet werden, und stellen nicht zwangsläufig eine flexible Lösung bereit, die für alle vorstellbaren Fälle gilt. In der Technik besteht daher ein Bedarf zur Lösung des oben genannten Problems.

[0025] Die US 2017 0308694 A1 offenbart ein System und Verfahren zur biometrischen Echtzeit-Authentifizierung, wobei das System ein lokales Gerät, einen entfernten Server, eine Datenbank und eine Zugangskontrollvorrichtung umfasst. Das lokale Gerät empfängt eine biometrische Eingabe von einem Benutzer und führt eine lokale Verifizierung auf Grundlage einer oder mehrerer biometrischer Vorlagen durch, die vorübergehend in einem Cache-Speicher des lokalen Geräts gespeichert sind. Der Server empfängt die biometrische Eingabe vom lokalen Gerät und führt eine Fernverifizierung auf Grundlage einer oder mehrerer in der Datenbank gespeicherter biometrischer Vorlagen aus, wenn die lokale Verifizierung fehlschlägt. Die Zugangskontrollvorrichtung steuert den Zugriff auf eine Ressource auf Grundlage eines vom lokalen Gerät empfangenen Befehls. Das lokale Gerät initiiert einen Löschmodus für jede Vorlage im Cache-Speicher auf Grundlage des Zeitablaufs, der seit der letzten vom entsprechenden Benutzer angeforderten Zugriffsanforderung verstrichen ist.

[0026] Die US 2017 0330028 A1 offenbart ein computerimplementiertes Verfahren zur Erkennung von Gesichtsbildern mit einem mehrstufigen Gesichtsverifizierungsprozess, um die Geschwindigkeit und Genauigkeit eines Gesichtserkennungsvorgangs zu verbessern. Ein Gesichtserkennungsmodul kann mehrere Stufen beinhalten, wobei eine Teilmenge von Daten rekursiv analysiert wird, um die Geschwindigkeit der Gesichtserkennungsprozesse zu verbessern. Die mehreren Stufen können in einer Schnell-zu-langsam- und Grob-zu-fein-Anordnung eingerichtet werden, sodass in jeder aufeinanderfolgenden Stufe eine Übereinstimmungsentcheidung getroffen werden kann.

[0027] Die US 2017 0262719 A1 offenbart ein biometrisches Authentifizierungssystem, umfassend ein Informationsterminal mit ID-Informationen, ein Erfassungsterminal, das biometrische Informationen erfasst, und eine Vorrichtung zur Authentifizierungsverarbeitung. Die Verarbeitungsvorrichtung beinhaltet: einen ersten Teil, der die ID und Standortinformationen auf dem Informationsterminal erfasst; einen zweiten Teil, der mit dem Erfassungsterminal kommuniziert, um die biometrischen Informationen zu erfassen; einen ersten Speicherteil

zum Speichern einer Angabe, dass sich das Informationsterminal innerhalb eines vorbestimmten Bereichs befindet; einen zweiten Speicherteil, der die ID und biometrische Referenzinformationen speichert; und einen Controller. Der Controller steuert Folgendes: Erfassen der ID-Informationen und des Standorts des Informationsterminals, wenn sich das Informationsterminal innerhalb eines vorbestimmten Bereichs befindet; Angeben, dass sich das Informationsterminal und das Erfassungsterminal innerhalb des vorbestimmten Bereichs befinden; und Vergleichen der biometrischen Informationen mit den biometrischen Referenzinformationen in Verknüpfung mit den ID-Informationen auf dem Informationsterminal.

[0028] Die US 2015 0254445 A1 offenbart eine biometrische Authentifizierungsvorrichtung, aufweisend Verarbeitungsvorrichtungen, denen abzugleichende biometrische Daten zugeordnet sind, eine Speichereinheit, die eine Verteilung der biometrischen Daten für jede einer Vielzahl von Qualitätsstufen und einen Zeitablauf für die Authentifizierungsverarbeitung, der für einen Authentifizierungsprozess jeder der Verarbeitungsvorrichtungen erforderlich ist, speichert, und eine Verwaltungseinheit. Die Verwaltungseinheit extrahiert erste und zweite Verarbeitungsvorrichtungen aus den Verarbeitungsvorrichtungen auf Grundlage der Authentifizierungsverarbeitungszeit, kennzeichnet ein Qualitätsniveau, für das eine Differenz zwischen den Verteilungen der ersten und zweiten Verarbeitungsvorrichtungen größer oder gleich einem Schwellenwert ist, und tauscht die biometrischen Daten mit dem gekennzeichneten Qualitätsniveau zwischen den ersten und zweiten Verarbeitungsvorrichtungen aus.

[0029] Die US 2011 0182480 A1 offenbart ein 1:N-Identifikationssystem. Ein Authentifizierungs-Client beinhaltet mindestens einen Sensor zur Eingabe biometrischer Informationen und eine Funktion zur Merkmalsextraktion. Eine Datenbank beinhaltet eine Anmelder-ID und registrierte Vorlagen von biometrischen Informationen mindestens einer Art für jeden Anmelder und beinhaltet eine Bewertungstabelle. Ein Authentifizierungsserver beinhaltet eine Funktion zum Setzen einer früheren Wahrscheinlichkeit, eine 1:N-Schnellabgleichsfunktion zum sukzessiven Abgleich des Merkmals mit den registrierten Vorlagen der Anmelder und zum Unterbrechen der Abgleichsverarbeitung, wenn die Anzahl der Abgleiche einen vorbestimmten Schwellenwert überschritten hat, eine Funktion zum Berechnen eines Delta-Scores unter Verwendung eines durch den 1:N-Schnellabgleich erhaltenen Scores und unter Verwendung der Bewertungstabelle, eine Funktion zur Berechnung nachträglicher Wahrscheinlichkeiten zum Berechnen jeweiliger nachträglicher Wahrscheinlichkeiten der Anmelder auf der Grundlage des Scores und des Delta-Scores, und eine Funktion zur Identifizierung von Benutzern des Authentifizierungsobjekts.

[0030] Die US 2009 0161921 A1 offenbart ein Authentifizierungssystem, ausgebildet zum Vergleichen, auf der Grundlage von Informationen über Zonen, in denen man davon ausgeht, dass sich darin derzeit eine Vielzahl von Registranten befindet, von charakteristischen Daten eines zu authentifizierenden Benutzers mit charakteristischen Daten von Registranten, von denen man annimmt, dass sie sich in einer Zone befinden, die der Terminalvorrichtung entspricht, die die charakteristischen Daten des zu authentifizierenden Benutzers liest.

KURZDARSTELLUNG

[0031] Unter einem ersten Blickwinkel betrachtet stellt die vorliegende Erfindung ein mittels Computer realisiertes Verfahren zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten bereit, wobei das Verfahren die Schritte aufweist: a) durch einen Computer Empfangen von Benutzereingaben, um eine Berechtigungsprüfung auf einem Zielendgerät zu starten, die biometrische Eingaben vom Benutzer aufweist; b) durch den Computer Ermitteln, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde; c) wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer Ausführen einer 1:1-Berechtigungsprüfung des Benutzers; d) wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer: i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster; ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle; iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist und bei dem es sich nicht um den Benutzer handelt, der gegenwärtig die Berechtigungsprüfung am Zielendgerät startet; iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungstabelle; v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähr-

ren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle.

[0032] Unter einem weiteren Blickwinkel betrachtet stellt die vorliegende Erfindung ein Computersystem zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten bereit, das einen Computer aufweist, der mindestens einen Prozessor, einen oder mehrere Speicher und ein oder mehrere durch einen Computer lesbare Speichermedien aufweist, auf denen Programmanweisungen gespeichert sind, die durch den Computer ausführbar sind zum a) Empfangen von Benutzereingaben, die biometrische Eingaben vom Benutzer aufweisen, durch den Computer, um die Berechtigungsprüfung auf einem Zielendgerät zu starten; b) Ermitteln durch den Computer, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde; c) wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer Ausführen einer 1:1-Berechtigungsprüfung des Benutzers; d) wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer: i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster; ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle; iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist und bei dem es sich nicht um den Benutzer handelt, der gegenwärtig die Berechtigungsprüfung am Zielendgerät startet; iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungstabelle; v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle.

[0033] Unter einem weiteren Blickwinkel betrachtet stellt die vorliegende Erfindung ein Computerprogrammprodukt zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten bereit, wobei das Computerprogrammprodukt ein durch einen Computer lesbares Speichermedium aufweist, das durch eine Verarbeitungsschaltung gelesen werden kann und auf dem Anweisungen zur Ausführung durch die Verarbeitungsschaltung gespeichert sind, um ein Verfahren zum Durchführen der Schritte der Erfindung durchzuführen.

[0034] Unter einem weiteren Blickwinkel betrachtet stellt die vorliegende Erfindung ein Computerprogramm bereit, das auf einem durch einen Computer lesbaren Medium gespeichert ist und in den internen Hauptspeicher eines Digitalcomputers geladen werden kann, das Softwarecodeabschnitte aufweist, die beim Ausführen des Programms auf einem Computer zum Durchführen der Schritte der Erfindung dienen.

[0035] Gemäß einer Ausführungsform der vorliegenden Erfindung wird ein Verfahren zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten offenbart. Das Verfahren weist die Schritte auf: a) durch einen Computer Empfangen von Benutzereingaben, um eine Berechtigungsprüfung auf einem Zielendgerät zu starten, die biometrische Eingaben vom Benutzer aufweist; b) durch den Computer Ermitteln, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde; c) wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer Ausführen einer 1:1-Berechtigungsprüfung des Benutzers; und d) wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde. Durch den Computer: i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster; ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle; iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist und bei dem es sich nicht um den Benutzer handelt, der gegenwärtig die Berechtigungsprüfung am Zielendgerät startet; iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungstabelle; v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle.

[0036] Gemäß einer weiteren Ausführungsform der vorliegenden Erfindung wird ein Computerprogrammprodukt zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten offenbart. Das Computerprogrammprodukt nutzt einen Computer, der mindestens einen Prozessor, einen oder mehrere Speicher und ein oder mehrere durch einen Computer lesbare Speichermedien aufweist. Das Computerprogrammprodukt weist ein durch einen Computer lesbares Speichermedium auf, das darauf verkörperte Programmanweisungen aufweist. Die Programmanweisungen sind durch den Computer ausführbar, um ein Verfahren durchzuführen, das aufweist: a) Empfangen von Benutzereingaben, die biometrische Eingaben vom Benutzer aufweisen, durch den Computer, um die Berechtigungsprüfung auf einem Zielendgerät zu starten; b) Ermitteln durch den Computer, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde; c) wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer Ausführen einer 1:1-Berechtigungsprüfung des Benutzers; d) wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde. Durch den Computer: i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster; ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle; iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist und bei dem es sich nicht um den Benutzer handelt, der gegenwärtig die Berechtigungsprüfung am Zielendgerät startet; iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungstabelle; v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle.

[0037] Gemäß einer weiteren Ausführungsform der vorliegenden Erfindung wird ein Computersystem zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten offenbart. Das Computersystem weist einen Computer auf, der mindestens einen Prozessor, einen oder mehrere Speicher, ein oder mehrere durch Computer lesbare Speichermedien aufweist, auf denen Programmanweisungen gespeichert sind, die durch den Computer ausführbar sind, um die Programmanweisungen auszuführen. Die Programmanweisungen weisen auf: a) Empfangen von Benutzereingaben, die biometrische Eingaben vom Benutzer aufweisen, durch den Computer, um die Berechtigungsprüfung auf einem Zielendgerät zu starten; b) Ermitteln durch den Computer, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde; c) wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer Ausführen einer 1:1-Berechtigungsprüfung des Benutzers; d) wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde. Durch den Computer: i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster; ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle; iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist und bei dem es sich nicht um den Benutzer handelt, der gegenwärtig die Berechtigungsprüfung am Zielendgerät startet; iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungstabelle; v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle.

Figurenliste

[0038] Im Folgenden werden Ausführungsformen der vorliegenden Erfindung unter Bezugnahme auf die beigefügten Zeichnungen beispielhaft beschrieben, wobei:

Fig. 1 ein beispielhaftes Schema einer möglichen Systemkonfiguration einer Datenverarbeitungsumgebung darstellt, in der bevorzugte Ausführungsformen der vorliegenden Erfindung realisiert sein können.

Fig. 2 ein Flussdiagramm einer Berechtigungsprüfungsausführung gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung zeigt;

Fig. 3 ein Flussdiagramm einer Analyse von Berechtigungsprüfungsergebnissen gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung zeigt;

die **Fig. 4A** und **Fig. 4B** ein Beispiel der Relevanz zwischen Endgeräten gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung zeigen;

Fig. 5 ein Flussdiagramm der Aufrechterhaltung von Berechtigungsprüfungsergebnissen gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung zeigt;

Fig. 6 ein Flussdiagramm der Ausführung einer 1:N-Berechtigungsprüfung gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung zeigt;

Fig. 7 interne und externe Komponenten eines Client-Computers und eines Server-Computers veranschaulicht, in denen veranschaulichende Ausführungsformen realisiert sein können.

AUSFÜHRLICHE BESCHREIBUNG

[0039] Das vorliegende System schlägt neue Mittel zum Verbessern der Leistung der Berechtigungsprüfung eines Berechtigungsprüfungssystems vor, das eine große Anzahl von Berechtigungsprüfungen wie zum Beispiel biometrische Berechtigungsprüfungen unter Verwendung eines gemeinsamen Benutzerkontos zur Anmeldung am Endgerät durchführen muss.

[0040] Dieses System betrifft eine Verbesserung bei der 1:N-Berechtigungsprüfung, bei der ein Quelldatenelement, das eingegeben wurde, um der Berechtigungsprüfung unterzogen zu werden, mit mehreren oder zahlreichen Elementen registrierter Berechtigungsprüfungsdaten verglichen werden muss.

[0041] Das System erreicht eine Leistungsverbesserung der Berechtigungsprüfung durch Auswählen geeigneter Arten von Berechtigungsprüfungen und außerdem durch Optimieren der Berechtigungsprüfungsabfolge.

[0042] Als Optimierungselement bei der Berechtigungsprüfung wählt das System Berechtigungsprüfungsart und Berechtigungsprüfungsreihenfolge auf der Grundlage von Verteilungsdaten von Benutzern und Endgeräten aus.

[0043] Des Weiteren verbessert dieses System die Genauigkeit, um die Berechtigungsprüfungsdaten nicht nur aus Daten eines einzigen Endgeräts, sondern durch dynamisches Verwenden einer „gegenseitigen Verwendungskorrelation zwischen Endgeräten“ zu erhalten.

[0044] Darüber hinaus schlägt dieses System als Verfahren zur Optimierung der Berechtigungsprüfungsabfolge ein Modifizierungskonzept durch Konzentrieren auf die Berechtigungsprüfungssituation vor, in der Bediener mehrere Endgeräte gleichzeitig nutzen, während der Reihe nach umgeschaltet wird.

[0045] Funktionen des Verfahrens können jeweils die 1:N-Berechtigungsprüfung biometrischer Berechtigungsprüfung verbessern. Jedes der im Folgenden aufgeführten Merkmale trägt unabhängig zur Leistungsverbesserung bei. Daher kann eine jedem Verfahren entsprechende Leistungsverbesserung erreicht werden, selbst wenn nur zwei Elemente verwendet werden.

[0046] Zu diesen Merkmalen gehören eine Berechtigungsprüfungspriorität auf der Grundlage dynamischer und virtueller Gruppierung zur Berechtigungsprüfung verwendeter Endgeräte, die zu einer Effizienzverbesserung der Berechtigungsprüfungs-Prioritätsabfolge bei der 1:N-Berechtigungsprüfung führt, eine Hybrid-Berechtigungsprüfung durch Umschalten der Berechtigungsprüfungslogik zwischen 1:1- und 1:N-Berechtigungsprüfung, die die Selektivität der Berechtigungsprüfung verbessert, und Maskieren eines bereits angemeldeten Benutzers für die Berechtigungsprüfungs-Prioritätsliste bei der 1:N-Berechtigungsprüfung zur Effizienzverbesserung der Berechtigungsprüfungs-Prioritätsabfolge bei der 1:N-Berechtigungsprüfung. Zu den Merkmalen gehört außerdem das Erhalten von Berechtigungsprüfungsdaten, in denen die Berechtigungsprüfungsdaten der biometrischen Informationen des Benutzers bei der Ausführung der Berechtigungsprüfung des Benutzers gespeichert werden, sowie die Speicherung von Berechtigungsprüfungsdaten (zum Beispiel von biometrischen

Daten), der Berechtigungsprüfungsliste, von Benutzerinformationen, Endgeräteinformationen, Endgerätegruppierungsdaten usw.

[0047] Bei Betrachtung einer Ausführungsform von Berechtigungsprüfung in einem Fall, in dem ein gemeinsames Benutzerkonto genutzt wird und mehrere Benutzer mehrere gemeinsame Endgeräte nutzen, konzentriert sich dieses System auf die Fehlverteilung von Berechtigungsprüfungs-Nutzungszeitraum und die Verwendung von Endgeräten durch jeden Benutzer.

[0048] Anschließend nutzt dieses System diese Fehlverteilung, um die Leistung der Berechtigungsprüfung zu verbessern. Zunächst wird das Berechtigungsprüfungsergebnis in einer tatsächlichen Umgebung aufgezeichnet, und anschließend werden die Daten analysiert, um eine Berechtigungsprüfungspriorität je Endgerät und Nutzungszeitraum zu ermitteln und schließlich eine derartige Prioritätstabelle zu speichern.

[0049] Während der Berechtigungsprüfung liest das System die Prioritätstabelle entsprechend dem Endgerät und Nutzungszeitraum aus. Eine Berechtigungsprüfung erfolgt bevorzugt mit einer minimalen Anzahl von Berechtigungsprüfungen unter Verwendung der auf einer ungleichmäßigen Verteilung beruhenden Prioritätstabelle.

[0050] Im tatsächlichen Gebrauch nutzen Benutzer oftmals mehrere Endgeräte, an denen sich Benutzer unter freier Verwendung eines gemeinsamen Benutzerkontos anmelden konnten. Um eine Optimierung entsprechend der Nutzungssituation des Endgeräts durchzuführen, es ist daher effektiv, die Endgeräte als Datenzusammenfassungsziel zu gruppieren.

[0051] In der Vergangenheit wurden als Gruppierungsverfahren ein Gruppieren auf der Grundlage des physischen Standorts des Endgeräts und ein Gruppieren nach den Informationen über die Organisation vorgeschlagen, zu der das Endgerät gehört. Bei diesen Verfahren handelt es sich jedoch um Gruppierungsverfahren, die entsprechend der tatsächlichen Nutzungsform von Benutzern kein optimiertes Mittel bilden.

[0052] Als Mittel zum Lösen des Problems des bestehenden Gruppierungskonzepts erreicht das vorliegende System eine Optimierung der Berechtigungsprüfungsabfolge, die nicht nur Nutzungsdaten von einem einzelnen Endgerät berücksichtigt, sondern auch diejenigen von Endgeräten, bei denen eine Abhängigkeitsbeziehung untereinander besteht, indem ein dynamisches Verhältnis zwischen Endgeräten und virtueller Gruppierung der Endgeräte berechnet wird.

[0053] Insbesondere schlägt dieses System vor, die Bewegung von Benutzern zwischen Endgeräten zu verwenden, um eine Abhängigkeitsbeziehung zwischen den Endgeräten zu berechnen. Ungeachtet der physischen Nähe des Endgeräts ist somit die Abhängigkeit beim Gebrauch dieser Endgeräte hoch, wenn ein einzelner Benutzer mehrere Endgeräte häufig nutzt, indem er sich zwischen den jeweiligen Endgeräten bewegt.

[0054] Außerdem ist es durch dynamisches Berechnen der Abhängigkeit unter Verwendung von Daten in einem zurückliegenden feststehenden Zeitraum möglich, eine Optimierung der Berechtigungsprüfung entsprechend der Nutzungstendenz eines Endgerätebenutzers durchzuführen.

[0055] Unter Ausnutzung dieser Abhängigkeit verwendet dieses System Nutzungsdaten von allen Endgeräten mit dynamischer Abhängigkeit und berechnet das Ergebnis mit Korrelationsfaktor als Gewichtungsfaktoren, um eine geeignete Berechtigungsprüfungsabfolge zu erhalten.

[0056] **Fig. 1** stellt ein beispielhaftes Schema einer möglichen Systemkonfiguration einer Datenverarbeitungsumgebung dar, in der veranschaulichende Ausführungsformen realisiert sein können.

[0057] **Fig. 1** ist ein beispielhaftes Schema einer bereitgestellten möglichen Datenverarbeitungsumgebung, in der veranschaulichende Ausführungsformen realisiert sein können. Es sollte klar sein, dass die **Fig. 1** lediglich beispielhaft und nicht als Aussage über Einschränkungen oder stillschweigende Einschränkungen hinsichtlich der Umgebungen gedacht ist, in denen unterschiedliche Ausführungsformen realisiert werden können. An den abgebildeten Umgebungen können viele Abänderungen vorgenommen werden.

[0058] Unter Bezugnahme auf **Fig. 1** handelt es sich bei dem Netzwerkdatenverarbeitungssystem **100** um ein Netzwerk aus Computern, in dem veranschaulichende Ausführungsformen realisiert sein können. Das Netzwerkdatenverarbeitungssystem **100** enthält mindestens ein Netzwerk **101**, bei dem es sich um das Medium handelt, das Datenaustauschverbindungen zwischen verschiedenen Einheiten und Computern bereitstellt, die

innerhalb des verteilten Netzwerkdatenverarbeitungssystems **100** miteinander verbunden sind. Das Netzwerk **101** kann Verbindungen wie z.B. drahtgebundene oder drahtlose Datenaustauschverbindungen oder Lichtwellenleiter beinhalten.

[0059] Bei dem dargestellten Beispiel sind ein Endgeräteeinheitencomputer **102**, ein Berechtigungsprüfungs-Servercomputer **105**, ein Geschäftssystem **120** einschließlich eines Geschäftsservers **121** über ein Netzwerk **124** mit einem Datenbankserver **125** und einer Datenablage (Repository) **127** verbunden. Bei anderen beispielhaften Ausführungsformen kann ein Netzwerkdatenverarbeitungssystem **51** weitere Client- oder Einheitencomputer, Speichereinheiten oder Datenablagen, Servercomputer und andere, nicht gezeigte Einheiten beinhalten.

[0060] Der Endgeräteeinheitencomputer **102** kann einen Webbrowser **103** enthalten, der eine Schnittstelle beinhalten kann, die Befehle und Dateneingaben von einem Benutzer aufnehmen kann. Der Endgeräteeinheitencomputer **102** kann außerdem einen Prozessor und zugehörige Sensoren **104** beinhalten, um Berechtigungsprüfungsdaten von einem Benutzer zu lesen und zu empfangen. Die Befehle können Anmeldeinformationen betreffen. Bei der Schnittstelle kann es sich zum Beispiel um eine Befehlszeilenschnittstelle, eine grafische Benutzeroberfläche (graphical user interface, GUI), ein Natural User Interface (NUI) oder um eine berührungsempfindliche Benutzeroberfläche (touch user interface, TUI) handeln. Der Endgeräteeinheitencomputer **102** beinhaltet einen Satz interner Komponenten **800a** und einen Satz externer Komponenten **900a**, die in **Fig. 7** weiter veranschaulicht sind.

[0061] Der Berechtigungsprüfungs-Servercomputer **105** beinhaltet einen Satz interner Komponenten **800b** und einen Satz externer Komponenten **900b**, die in **Fig. 7** weiter veranschaulicht sind. Bei dem dargestellten Beispiel stellt der Servercomputer **105** dem Endgeräteeinheitencomputer **102** Informationen wie zum Beispiel Boot-Dateien, Betriebssystemabbilder und Anwendungen bereit. Der Berechtigungsprüfungs-Servercomputer **105** kann die Informationen lokal berechnen oder die Informationen von anderen Computern im Netzwerk **101** extrahieren. Der Berechtigungsprüfungs-Servercomputer **105** enthält außerdem vorzugsweise ein Berechtigungsprüfungsprogramm **66**. Der Berechtigungsprüfungs-Servercomputer **106** enthält mindestens einen Prozessor **107** und einen zugehörigen Hauptspeicher **106**, der mit einer Datenablage **108** verbunden ist. Der Prozessor **107** führt Steuerfunktionen **114** aus. Die Datenablage **108** enthält vorzugsweise Berechtigungsprüfungsdaten, zum Beispiel in einer Datenbank **109** für biometrische Daten, eine Berechtigungsprüfungs-Ergebnisdatenbank **110**, eine Endgerätenutzungsdatenbank **111**, eine Endgerätebeziehungsdatenbank **112** und eine Berechtigungsprüfungs-Prioritätsdatenbank **113**. Zu den Steuerfunktionen **114** gehören, ohne darauf beschränkt zu sein, Merkmale zum Erhalten von Berechtigungsprüfungsdaten **115**, Funktionen zum Ausführen der Hybrid-Berechtigungsprüfung **116**, Funktionen zum Berechnen einer Endgerätebeziehung **117**, Funktionen zum Erstellen einer Berechtigungsprüfungs-Prioritätsliste **118** und eine Datenbank **119** für biometrische Berechtigungsprüfungsdaten.

[0062] Das Geschäftssystem **120** weist einen Geschäftsserver **121**, zum Beispiel einen Webserver **122**, mit einer Webanwendung **123** auf. Der Geschäftsserver **121** ist über ein internes Netzwerk **124** mit einem Datenbankserver **125** verbunden, der ein Datenbanksystem **126** und eine zugehörige Datenablage **127** beinhaltet. Der Webserver **122** und der Datenbankserver **125** beinhalten einen Satz interner Komponenten **800b** und einen zweiten Satz externer Komponenten **900b**, die in **Fig. 7** veranschaulicht sind. Der Webserver **122** und der Datenbankserver **125** können die Informationen lokal berechnen und die Informationen von anderen Computern im Netzwerk **124** und Netzwerk **101** extrahieren.

[0063] Programmcode und Programme wie zum Beispiel das Berechtigungsprüfungsprogramm **66** können auf mindestens einer von einer oder mehreren durch einen Computer lesbaren physischen Speichereinheiten **830**, die in **Fig. 7** gezeigt sind, auf mindestens einer von einer oder mehreren transportablen, durch einen Computer lesbaren physischen Speichereinheiten **936**, wie in **Fig. 7** gezeigt, oder in der Datenablage **108** gespeichert sein oder zur Verwendung auf einen Endgeräteeinheitencomputer **102**, einen Berechtigungsprüfungs-Servercomputer **105** oder einen Geschäftsservercomputer **121** heruntergeladen werden. Zum Beispiel können Programmcode und Programme wie zum Beispiel das Berechtigungsprüfungsprogramm **66** auf mindestens einer von einer oder mehreren Speichereinheiten **830** auf dem Berechtigungsprüfungs-Servercomputer **105** gespeichert sein und zur Verwendung auf den Endgeräteeinheitencomputer **102** über das Netzwerk **101** heruntergeladen werden. Alternativ kann es sich bei dem Berechtigungsprüfungs-Servercomputer **105** um einen Webserver handeln, und der Programmcode und die Programme wie zum Beispiel das Berechtigungsprüfungsprogramm **66** können auf mindestens einer der einen oder der mehreren Speichereinheiten **830** auf dem Berechtigungsprüfungs-Servercomputer **105** gespeichert sein und durch den Endgeräteeinheitencomputer **102** aufgerufen werden. Ebenso handelt es sich bei dem Geschäftsserver vorzugsweise um einen Web-

server **122**. Bei anderen beispielhaften Ausführungsformen können der Programmcode und Programme wie zum Beispiel das Berechtigungsprüfungsprogramm **66** auf mindestens einer von einer oder mehreren durch einen Computer lesbaren Speichereinheiten **830** auf dem Endgeräteeinheitencomputer **102** gespeichert oder auf zwei oder mehr Server verteilt sein.

[0064] Bei dem dargestellten Beispiel handelt es sich bei dem Netzwerkdatenverarbeitungssystem **100** um das Internet, wobei das Netzwerk **101** für eine weltweit verteilte Ansammlung von Netzwerken und Gateways steht, die zum Datenaustausch untereinander die Protokollreihe des Transmission Control Protocol/Internet Protocol (TCP/IP) nutzen. Das Herzstück des Internets bildet ein Hauptstrang (Backbone) aus schnellen Datenübertragungsleitungen zwischen Hauptknoten bzw. Host-Computern, die aus tausenden von Computersystemen für Wirtschaft, Behörden und Bildungsinstitutionen sowie anderen Computersystemen bestehen, die Daten und Nachrichten weiterleiten. Selbstverständlich kann das Netzwerkdatenverarbeitungssystem **100** auch in Form einer Anzahl unterschiedlicher Arten von Netzwerken realisiert sein, zum Beispiel in Form eines Intranets, eines lokalen Netzwerks (local area network, LAN) oder eines Weitverkehrsnetzwerks (wide area network, WAN). **Fig. 1** ist als Beispiel und nicht als Einschränkung der Architektur der unterschiedlichen veranschaulichenden Ausführungsformen gedacht.

[0065] **Fig. 7** veranschaulicht interne und externe Komponenten eines Endgeräteeinheitencomputers **102**, eines Berechtigungsprüfungs-servers **105**, eines Geschäftsservercomputers **121** und eines Datenbankservercomputers **125**, in denen veranschaulichende Ausführungsformen realisiert sein können. In **Fig. 7** beinhalten ein Endgeräteeinheitencomputer **102**, ein Berechtigungsprüfungs-Servercomputer **105**, ein Geschäftsservercomputer **121** und ein Datenbankservercomputer **125** jeweilige Sätze interner Komponenten **800a**, **800b** und externer Komponenten **900a**, **900b**. Jeder der Sätze interner Komponenten **800a**, **800b** beinhaltet einen oder mehrere Prozessoren **820**, einen oder mehrere durch einen Computer lesbare RAMs **822** und einen oder mehrere durch einen Computer lesbare ROMs **824** an einem oder mehreren Bussen **826**, ein oder mehrere Betriebssysteme **828** und eine oder mehrere durch einen Computer lesbare physische Speichereinheiten **830** auf. Das eine oder die mehreren Betriebssysteme **828** und das Berechtigungsprüfungsprogramm **66** sind zur Ausführung durch einen oder mehrere der Prozessoren **820** über einen oder mehrere der RAMs **822** (die normalerweise Cache-Speicher beinhalten) auf einer oder mehreren der durch einen Computer lesbaren physischen Speichereinheiten **830** gespeichert. Bei der in **Fig. 7** veranschaulichten Ausführungsform handelt es sich bei jeder der durch einen Computer lesbaren physischen Speichereinheiten **830** um eine Magnetplattenspeichereinheit einer internen Festplatte. Alternativ handelt es sich bei jeder der durch einen Computer lesbaren physischen Speichereinheiten **830** um eine Halbleiterspeichereinheit wie zum Beispiel einen ROM **824**, einen EPROM, einen Flash-Speicher oder um eine beliebige andere durch einen Computer lesbare physische Speichereinheit, auf der ein Computerprogramm und digitale Daten gespeichert sein können.

[0066] Jeder Satz interner Komponenten **800a**, **800b** beinhaltet außerdem ein Lese/Schreib-Laufwerk oder eine Lese/Schreib-Schnittstelle **832** zum Lesen von einer oder mehreren bzw. Schreiben auf eine oder mehrere transportable, durch einen Computer lesbare physische Speichereinheiten **936** wie z.B. CD-ROM, DVD, Memory-Stick, Magnetband, Magnetplatte, optische Platte oder Halbleiterspeichereinheit. Das Berechtigungsprüfungsprogramm **66** kann auf einer oder mehreren der transportablen, durch einen Computer lesbaren physischen Speichereinheiten **936** gespeichert sein, über ein Lese/Schreib-Laufwerk oder eine Lese/Schreib-Schnittstelle **832** gelesen und auf ein oder mehrere Festplattenlaufwerke **830** geladen werden.

[0067] Jeder Satz interner Komponenten **800a**, **800b** beinhaltet außerdem einen Netzwerkadapter oder eine Netzwerkschnittstelle **836** wie z.B. eine TCP/IP-Adapterkarte. Das Berechtigungsprüfungsprogramm **66** kann von einem externen Computer über ein Netzwerk (zum Beispiel das Internet, ein lokales Netzwerk oder ein anderes Weitverkehrsnetzwerk) und über den Netzwerkadapter oder die Netzwerkschnittstelle **836** auf den Endgeräteeinheitencomputer **102** und den Berechtigungsprüfungs-Servercomputer **105** heruntergeladen werden. Vom Netzwerkadapter oder von der Netzwerkschnittstelle **836** wird das Berechtigungsprüfungsprogramm **66** auf das Festplattenlaufwerk **830** geladen. Das Berechtigungsprüfungsprogramm **66** kann von einem externen Computer über ein Netzwerk (zum Beispiel das Internet, ein lokales Netzwerk oder ein anderes Weitverkehrsnetzwerk) und über den Netzwerkadapter oder die Netzwerkschnittstelle **836** auf den Berechtigungsprüfungs-Servercomputer **105** heruntergeladen werden. Vom Netzwerkadapter oder von der Netzwerkschnittstelle **836** wird das Berechtigungsprüfungsprogramm **66** auf das Festplattenlaufwerk **830** geladen. Das Netzwerk kann Kupferleitungen, Lichtwellenleiter, drahtlose Übertragung, Router, Firewalls, Switches, Gateway-Computer und/oder Edge-Server aufweisen.

[0068] Jeder der Sätze externer Komponenten **900a**, **900b** beinhaltet einen Computeranzeigemonitor **920**, eine Tastatur **930** und eine Computermaus **934**. Jeder der Sätze interner Komponenten **800a**, **800b** beinhaltet

außerdem Einheitentreiber **840**, die die Schnittstellen zum Computeranzeigemonitor **920**, zur Tastatur **930** und zur Computermaus **934** bilden. Die Einheitentreiber **840**, das Lese/Schreib-Laufwerk oder die Lese/Schreib-Schnittstelle **832** und der Netzwerkadapter oder die Netzwerkschnittstelle **836** weisen Hardware und Software auf (die auf der Speichereinheit **830** und/oder im ROM **824** gespeichert sind).

[0069] Das Berechtigungsprüfungsprogramm **66** kann in verschiedenen Programmiersprachen geschrieben sein, unter anderem in maschinennahen, höheren, objektorientierten oder nicht objektorientierten Sprachen. Alternativ können die Funktionen eines Berechtigungsprüfungsprogramms **66** ganz oder teilweise mit Hilfe von Computerschaltungen und oder mit Hilfe anderer Hardware (nicht gezeigt) realisiert sein.

[0070] Die Merkmale des Systems werden im Folgenden ausführlicher beschrieben.

Berechtigungsprüfungsdaten erhalten:

[0071] Der zeitliche Ablauf der Ausführung der Operationen bei der Verarbeitung dieses Mechanismus ist im Flussdiagramm von **Fig. 2** „Ausführung der Berechtigungsprüfung“ beschrieben.

[0072] Das System beginnt mit dem am gemeinsamen Benutzerkonto angemeldeten gemeinsamen Endgerät. Ein Benutzer startet eine Operation, die eine Berechtigungsprüfung erfordert - zum Beispiel möchte ein Kassierer gekaufte Waren scannen, oder ein Manager möchte eine Preissenkung eines Artikels an einer Registrierkasse genehmigen, an der ein Kassierer einen Warenkorb mit Lebensmitteln eingibt usw.

[0073] Der neue Benutzer gibt seine oder ihre biometrischen Daten in der nach dem Stand der Technik bekannten Art und Weise ein, zum Beispiel durch Auflegen des Daumens auf einen Fingerabdruckscanner.

[0074] Unter Bezugnahme auf **Fig. 2** empfängt der Endgeräteeinheitencomputer **102** Eingaben eines Benutzers zum Starten einer Berechtigungsprüfung an einem Endgerät (Schritt **202**), und der Endgeräteeinheitencomputer **102** empfängt biometrische Eingaben von einem Benutzer (Schritt **204**), und das Verfahren endet.

[0075] Das System geht anschließend zur Hybrid-Berechtigungsprüfung von **Fig. 3** über, wie nachstehend beschrieben.

[0076] Bei einem herkömmlichen System werden Anmeldeinformationen als Berechtigungsprüfungsprotokoll aufgezeichnet. Um jedoch die Verlaufsdaten der Ausführung von Berechtigungsprüfungen als Basisdaten zum Verbessern der Leistung und Effizienz der Berechtigungsprüfung zu verwenden, müssen Personendaten anhand jedes notwendigen Elements gesammelt werden, um den Berechtigungsprüfungsverlauf anhand jeder Berechtigungsprüfungszeit und jedes Zielendgeräts abrufen zu können. Daher ist es wünschenswert, die als „Benutzerinformationsdatenbank, Benutzerinformationstabelle“ beschriebenen Elemente in der Datenbank als Beispiel gespeicherter Daten zu speichern.

Hybrid-Berechtigungsprüfungsdaten ausführen:

[0077] Im Falle der gemeinsamen Nutzung eines gemeinsamen Benutzerkontos mit mehreren Personen wird eine Berechtigungsprüfung durch eine sogenannte 1:N-Berechtigungsprüfung durchgeführt, bei der zur Berechtigungsprüfung eingegebener Daten mehrere Überprüfungsziele bestehen.

[0078] Zum Durchführen der 1:N-Berechtigungsprüfung müssen zwangsläufig ein großes Datenvolumen aus einer Datenbank geladen und diese Berechtigungsprüfungsdaten übertragen werden. Die Datenübertragung geschieht während einer mehrmaligen Ausführung der Berechtigungsprüfung. Aus diesem Grund verlängert sich die Verarbeitungszeit im Vergleich zur 1:1-Berechtigungsprüfung, bei der die Eingabe und das Überprüfungsziel nur für eine bestimmte Anmeldung gelten.

[0079] Als Lösungsverfahren für diese Situation erhöht das System der vorliegenden Erfindung die Leistung der Berechtigungsprüfung, indem es sich auf die Fehlverteilung der Berechtigungsprüfung als Reproduzierbarkeit der Berechtigungsprüfung für dieselbe Person am selben Endgerät konzentriert.

[0080] Ein Verfahren zum Festlegen der Ausführung von 1:1-Berechtigungsprüfung besteht darin, die Zeit (den Zeitüberschreitungswert) seit der vorhergehenden Berechtigungsprüfung durch denselben Benutzer festzulegen, oder anhand der Eingabe der anderen Kennungsinformationen festzustellen, dass sich ein anderer Benutzer anmeldet.

[0081] Wenn es sich bei den für das System verwendeten Endgeräten jedoch um ein Front-End-Terminal handelt, das für einen Kunden vorgesehen ist, ist es schwierig, einen einfachen Zeitüberschreitungswert zu setzen, um die Beendigung der Endgerätenutzung festzulegen, da der Schalterdienst nicht einfach als Aufgabe zur Nutzung des Endgeräts angegeben werden kann. Darüber hinaus ist die Kennungseingabe zum Unterscheiden von Benutzern auch schwierig, wenn mehrere Benutzer das Front-End-Endgerät in der Nutzungsumgebung verwenden. Daher können bestehende 1:1- und 1:N-Berechtigungsprüfungs-Umschaltverfahren bei dieser Umgebung nicht angewendet werden.

[0082] Daher führt das System der vorliegenden Erfindung eine vorläufige Berechtigungsprüfung durch, um eine angenäherte Ermittlung vorzunehmen, ob es sich bei dem Benutzer, der sich gerade am Endgerät anmeldet, um denselben Benutzer handelt, der die vorhergehende Berechtigungsprüfung an dem Endgerät ausgeführt hat.

[0083] Die Geschwindigkeit der Berechtigungsprüfung 6 hängt von der Detailliertheit der Realisierungsform der Berechtigungsprüfung ab. Zunächst wird als vorläufige Berechtigungsprüfung ermittelt, ob es sich um denselben Benutzer handelt, der zuvor auf Berechtigung geprüft wurde. Nachdem diese Ermittlung vorgenommen wurde, wird ermittelt, ob eine Berechtigungsprüfungsumschaltung stattfinden sollte. Die Verwendung dieser groben Berechtigungsprüfung stellt kein Sicherheitsrisiko dar.

[0084] Wenn festgestellt werden kann, dass es sich bei dem Benutzer um denselben Benutzer handelt, der während der vorhergehenden Anmeldung auf Berechtigung geprüft wurde, wird eine 1:1-Berechtigungsprüfung durchgeführt, indem der Cache-Speicher der Daten zum Prüfen des vorhergehenden Benutzers auf Berechtigung verwendet wird.

[0085] Wenn nicht festgestellt werden kann, dass die vorherige Anmeldung und Berechtigungsprüfung für denselben Benutzer erfolgten, oder wenn derselbe Benutzer nicht in der 1:1-Berechtigungsprüfung auf Berechtigung geprüft werden kann, wird eine Abfolge zum Ausführen einer normalen 1:N-Berechtigungsprüfung durchgeführt. Dadurch verbessert das System die Geschwindigkeit einer wiederholten Berechtigungsprüfung durch denselben Benutzer, die den Großteil der Anwendungsfälle bildet.

[0086] Die Berechtigungsprüfungsausführungslogik selbst kann die bestehende Berechtigungsprüfungslogik wie z.B. ein biometrisches Berechtigungsprüfungsverfahren nutzen.

[0087] Die Operationen, durch die sich die Berechtigungsprüfung im vorliegenden System auszeichnen, bestehen aus den folgenden beiden Teilen.

Ausführung von 1:1- und 1:N-Berechtigungsprüfung einschließlich vorläufiger Berechtigungsprüfung

[0088] **Fig. 3** zeigt ein Flussdiagramm, das die Auswahl von 1:1- oder 1:N-Berechtigungsprüfung veranschaulicht.

[0089] Nach dem Empfangen biometrischer Eingaben von einem Benutzer und von Anmeldeinformationen von einem Benutzer aus **Fig. 2** ermittelt das Berechtigungsprüfungsprogramm **66**, ob die Biometriedaten anzeigen, dass es sich bei dem Benutzer, der sich gerade am Endgerät beim System anmeldet, um denselben Benutzer handelt, der zuletzt durch das System auf Berechtigung geprüft wurde (Schritt **220**).

[0090] Wenn es sich bei dem Benutzer nicht um denselben Benutzer handelt, der zuvor durch das System auf Berechtigung geprüft wurde, oder der Benutzer nicht auf Berechtigung geprüft werden kann (Schritt **220**), führt das Berechtigungsprüfungsprogramm **66** eine 1:N-Berechtigungsprüfung aus (Schritt **222**), und das Verfahren geht zu **Fig. 6** über, die nachfolgend weiter erörtert wird.

[0091] Wenn es sich bei dem Benutzer um denselben Benutzer handelt, der zuvor durch das System auf Berechtigung geprüft wurde (Schritt **220**), führt das Berechtigungsprüfungsprogramm **66** eine 1:1-Berechtigungsprüfung aus (Schritt **224**).

[0092] Wenn die Berechtigungsprüfungsinformationen für den Benutzer nicht akzeptiert werden (Schritt **226**), geht das Verfahren zu Schritt **222** der Ausführung der 1:N-Berechtigungsprüfung über, und das Verfahren geht zur **Fig. 6** über, die nachfolgend weiter erörtert wird.

[0093] Wenn die Berechtigungsprüfungsinformationen für den Benutzer akzeptiert werden (Schritt **226**), wird das Berechtigungsprüfungsergebnis in einer Berechtigungsprüfung-Ergebnistabelle gespeichert (Schritt **228**), das Berechtigungsprüfungsprogramm **66** gewährt dem Endgerät Zugriff für den Benutzer (Schritt **230**) und das Verfahren endet.

Funktion zur Ausführung der 1:N-Berechtigungsprüfung mit Maskenfunktion der Berechtigungsprüfung-Prioritätsliste, um eine Berechtigungsprüfung für den gerade angemeldeten Benutzer an einem anderen Endgerät auszuschließen

[0094] Beim Empfangen einer Berechtigungsprüfungsanforderung führt das System eine vorläufige Berechtigungsprüfung durch, die bei hoher Geschwindigkeit mit grober Detailliertheit ausgeführt werden kann, indem die eingegebenen der biometrischen Berechtigungsprüfungsinformationen und die vorherigen Berechtigungsprüfungsinformationen verwendet werden.

[0095] Diese Berechtigungsprüfung ist nicht die endgültige Berechtigungsprüfung, sondern die Ermittlung einer Möglichkeit, ob es sich um denselben Benutzer wie beim vorhergehenden Mal handelt.

[0096] Wenn festgestellt wird, dass die Wahrscheinlichkeit hoch ist, dass es sich um denselben Benutzer handelt, wird eine 1:1-Berechtigungsprüfung ausgeführt, indem die Daten des Benutzers verwendet werden, der sich das letzte Mal angemeldet hat. Wenn andererseits festgestellt wird, dass es sich sehr wahrscheinlich um einen anderen Benutzer handelt, geht die Ausführung zur Ausführung der 1:N-Berechtigungsprüfung über.

Ausführung der 1:N-Berechtigungsprüfungsfunktion mit Maskenfunktion der Berechtigungsprüfung-Prioritätsliste, um eine Berechtigungsprüfung für den gerade angemeldeten Benutzer an einem anderen Endgerät auszuschließen

[0097] Bei der 1:N-Berechtigungsprüfung wird die Berechtigungsprüfung auf der Grundlage der eingegebenen biometrischen Berechtigungsprüfung und der Berechtigungsprüfung-Prioritätsliste der Reihe nach ausgeführt.

[0098] Bei der Berechtigungsprüfung-Prioritätsliste handelt es sich jedoch um eine Liste, die auf dem zurückliegenden Berechtigungsprüfungsstatus beruht. Aus diesem Grund wird möglicherweise eine unnötige Berechtigungsprüfungsverarbeitung durchgeführt, da der gegenwärtig am anderen Endgerät angemeldete Benutzer mit einer höheren Priorität in der Berechtigungsprüfung-Prioritätsliste eingestuft wird.

[0099] Daher wird die gelesene Berechtigungsprüfung-Prioritätsliste als zeitweilige Berechtigungsprüfung-Prioritätstabelle angelegt. Da es sich hierbei um eine zeitweilige Tabelle handelt, ist der Hauptspeicher zum Speichern einer derartigen Tabelle bevorzugt.

[0100] Als Nächstes wird anhand der Berechtigungsprüfungsergebnisdaten nach den aktuellen Anmeldedaten gesucht, danach werden die ermittelte Benutzerkennung aus der zeitweiligen Berechtigungsprüfungstabelle gelöscht und die Berechtigungsprüfungsausführung als aussagefähige Tabelle neu geschrieben.

[0101] Abschließend wird die Berechtigungsprüfung in der Reihenfolge der in der Liste der aktualisierten zeitweiligen Berechtigungsprüfung-Prioritätstabelle beschriebenen Daten ausgeführt.

Endgerätebeziehungen berechnen

[0102] Bei der 1:N-Berechtigungsprüfung ist die Gültigkeit der Prioritätsliste der wichtigste Faktor beim Verbessern der Effizienz der Berechtigungsprüfung.

[0103] Zur Erhöhung der Genauigkeit der Liste von Berechtigungsprüfungsprioritäten muss die Lokalisierung der Berechtigungsprüfung-Prioritätsliste erweitert werden. Das heißt, dass es sich nicht um die Prioritätsliste im gesamten System handelt, sondern um die Prioritätenlistenstellung in der Gruppe oder auf der Endgeräteebene.

[0104] In diesem Fall besteht als nachteilige Auswirkung zum Zeitpunkt der Verwendung der Berechtigungsprüfungspriorität Redundanz durch Erweiterung der Örtlichkeit. Dieses vorliegende System konzentriert sich auf die Tatsache, dass eine Verringerung dieser Redundanz zu hoher Geschwindigkeit beiträgt.

[0105] Insbesondere im Falle einer Umgebung unter Verwendung eines gemeinsamen genutzten Endgeräts nutzt derselbe Benutzer mehrere Endgeräte. Infolgedessen ist eine Registrierung desselben Benutzers in den Prioritätslisten eine Situation, die in der Regel bei dieser Art von Anwendungsfall auftreten kann.

[0106] Andererseits gibt es unter dem Gesichtspunkt der Berechtigungsprüfung keinen Nutzungsmodus, bei dem derselbe Benutzer gleichzeitig an mehreren Endgeräten auf Berechtigung geprüft wird und sich anmeldet.

[0107] Zum Zeitpunkt der Berechtigungsprüfungsausführung kann beim Lesen der Berechtigungsprüfungspriorität keine Berechtigungsprüfung des Benutzers stattfinden, der am anderen Endgerät angemeldet ist. Daher verbessert das System der vorliegenden Erfindung die Leistung der Berechtigungsprüfung, indem der Benutzer, der sich am anderen Endgerät anmeldet, von der Berechtigungsprüfungsprioritätsliste ausgeschlossen wird, die auf diesem Standort beruht.

[0108] Das Entfernen (Maskieren) aus der Liste ändert sich dynamisch anhand der Benutzernutzungssituation zum Zeitpunkt des Auftretens der Berechtigungsprüfungsanforderung. Daher kopiert das System der vorliegenden Erfindung die Berechtigungsprüfungsprioritätsliste als zeitweilige Tabelle, um eine zeitweilige Änderung dieser Tabelle zu ermöglichen, und führt anschließend eine Berechtigungsprüfung unter Verwendung dieser zeitweiligen Berechtigungsprüfungsprioritätsliste aus, um eine Berechtigungsprüfung anhand des Nutzungszustands vorzunehmen.

[0109] Zu den Funktionen dieses Elements gehören eine Berechtigungsprüfungsdaten-Erfassungsfunktion, eine Endgerätebeziehungs-Berechnungsfunktion und eine Endgerätebeziehungsdaten-Speicherfunktion.

Beispiel eines Konzepts zur Verwaltung von Endgerätegruppierungen

[0110] Es folgt ein Beispiel der Funktionsweise des Konzepts zur Verwaltung von Endgerätegruppierungen. Das Verfahren zum Berechnen der Endgeräterelevanz (Endgerätebeziehung) ist lediglich ein Beispiel, wobei ein anderes Verfahren zum Berechnen der Endgeräterelevanz verwendet werden könnte, das auf dem Berechtigungsprüfungsprotokoll jedes Endgeräts beruht.

[0111] Für das Zielendgerät werden Daten darüber erfasst, an welchem Endgerät sich der Benutzer befindet, der die nächste Berechtigungsprüfung ausgeführt hat. Eine Funktion führt die erfassten Ergebnisse für einen bestimmten Zeitraum zusammen und berechnet den Endgeräterelevanzindex jedes Endgeräts in Bezug auf andere Endgeräte. Das Berechnungsergebnis ist ein Verhältnis (%), an welchem Endgerät sich der am betreffenden Endgerät angemeldete Benutzer am nächsten Endgerät angemeldet hat. Dieses Berechnungsergebnis wird in der „Endgerätebeziehungs-DB: Endgerätebeziehungstabelle“ gespeichert.

[0112] Für das Endgerät (Y) lautet der Relevanzindex (%) des Endgeräts (X) = Anzahl von Anmeldungen am Endgerät Y nach dem Anmelden am Endgerät X innerhalb des angestrebten Zeitraums/Anzahl von Anmeldungen am Endgerät X innerhalb des betreffenden Zeitraums.

[0113] In einer Umgebung, in der Kundenaufgaben ausgeführt werden, während mehrere benachbarte gemeinsame Endgeräte gemeinsam genutzt werden, führt der Benutzer seinen Geschäftsvorgang am leeren Endgerät aus, ohne sich dessen bewusst zu sein, dass es sich um ein eindeutiges Endgerät handelt.

[0114] Unter derartigen Umständen führt die Erstellung einer Berechtigungsprüfungsprioritätsliste aus Nutzungsdaten lediglich eines einzigen Endgeräts nicht zur Erstellung einer Liste, die die tatsächliche Nutzung wiedergibt.

[0115] Daher erstellt das System die Prioritätsliste unter Verwendung relevanter Endgerätedaten mit einem gewichteten Faktor, nachdem ein dynamischer Beziehungsfaktor zwischen Endgeräten ermittelt wurde. Die **Fig. 4A** und **Fig. 4B** zeigen die Endgeräte **1** und **2**, bei denen die mit Kreisen versehenen Elemente „A“ eine Berechtigungsprüfung des Benutzers „A“ darstellen und die mit Kreisen versehenen Elemente „B“ eine Berechtigungsprüfung des Benutzers „B“ darstellen.

[0116] **Fig. 4A** zeigt einen Fall, bei dem die Relevanz zwischen dem Endgerät **1** und dem Endgerät **2** unabhängig vom physischen Standort des Endgeräts null beträgt.

[0117] **Fig. 4B** zeigt einen Fall, bei dem die Relevanz zwischen dem Endgerät **1** und dem Endgerät **2** unabhängig vom physischen Standort ziemlich hoch ist.

Berechtigungsprüfungs-Prioritätsliste erstellen

[0118] Fig. 5 zeigt ein Flussdiagramm eines Verfahrens zur Beziehungsanalyse und Prioritätslistenerstellung. Der Prozess von Fig. 5 kann täglich oder wöchentlich durchgeführt werden und muss nicht nach jeder Genehmigung durchgeführt werden, obwohl er nach jeder Genehmigung durchgeführt werden könnte, wenn Prozessressourcen dies zulassen.

[0119] In einem ersten Schritt berechnet das Berechtigungsprüfungsprogramm 66 auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle ein Endgerätenutzungsverhältnis je Zeitfenster und speichert das Endgerätenutzungsverhältnis je Zeitfenster in der Endgerätenutzungsverhältnistabelle (Schritt 280).

[0120] Das Berechtigungsprüfungsprogramm 66 berechnet eine Endgerätebeziehung und speichert die Endgerätebeziehung in der Endgerätebeziehungstabelle (Schritt 282).

[0121] Das Berechtigungsprüfungsprogramm 66 berechnet dann auf der Grundlage der Endgerätebeziehung, der Endgerätenutzungsverhältnistabelle und des Berechtigungsprüfungsergebnisses die Berechtigungsprüfungspriorität und speichert die Berechtigungsprüfungspriorität in der Berechtigungsprüfungs-Prioritätstabelle (Schritt 284), und das Verfahren endet.

[0122] Eine Berechtigungsprüfungs-Prioritätsliste wird für jedes entsprechende Endgerät erstellt. Die Berechtigungsprüfungs-Prioritätsliste des Zeitfensters X des Endgeräts (W) wird anhand der folgenden Prozedur berechnet:

Schätzung des Berechtigungsprüfungs-Nutzungsverhältnisses
je Zielzeitfenster des entsprechenden Endgeräts

[0123] Der Benutzer (Y) vermutete ein Berechtigungsprüfungs-Nutzungsverhältnis im Zeitfenster (X) des entsprechenden Endgeräts (W).

[0124] Schätzung des Berechtigungsprüfungs-Nutzungsverhältnisses je Zielzeitfenster des entsprechenden Endgeräts = (Relevanzindex (%) für das Zielendgerät (Z) des entsprechenden Endgeräts (W)) x (Prozentsatz der Nutzung (%) im Zeitfenster (X) des Zielendgeräts (Z)). Zu beachten ist, dass diese Berechnung sowohl für alle Zielendgeräte als auch alle Benutzer ausgeführt wird.

Erstellung der Prioritätsliste

[0125] Die Priorität des entsprechenden Endgeräts (W) im Zeitfenster (X) wird als Prioritätsliste erstellt, indem in absteigender Reihenfolge in Richtung des durch den Benutzer (Y) im Zeitfenster (X) des entsprechenden Endgeräts (W) vermuteten Berechtigungsprüfungs-Nutzungsverhältnisses sortiert wird.

Speicher und Datenbank

[0126] Die folgenden verschiedenen Tabellen zeigen Beispiele von Tabellen, die durch jeden Mechanismus in diesem System im Speicher gehalten werden. Es wird klar sein, dass die tatsächlichen Einzelheiten in einem System von der jeweiligen tatsächlichen Realisierungsform abhängen.

Tabelle E.1: Benutzerinformationsdatenbank - Benutzerinformationstabelle

Gemeinsame Benutzerkontokennung	Biometrische Daten						
	Datendatei A	Benutzername	Benutzer	...	Datendatei N	Benutzername	Benutzer
001	/xxx /123456_1	John Doe	A	...	/xxx /123456_N	Bill Clark	B
002	/xxx /234567_1	Bill Roe	E	...	/xxx /123456_1	John Doe	A
...		
00n	/xxx3452452_1	Jane Doe	D	...	/xxx /3452452_N	Bob Jones	XX

[0127] Zu beachten ist bei diesem Beispiel der Unterschied zwischen „Benutzern“, bei denen es sich um Personen mit ihren zugehörigen biometrischen Daten handelt (die beispielhaft mit den Buchstaben A bis XX gekennzeichnet sind), und „gemeinsamen Benutzerkontokennungen“, bei denen es sich um Systemkennungen handelt, die zum Anmelden bei einem Endgerät verwendet werden (die beispielhaft mit den Zahlen 001 bis 00n gekennzeichnet sind).

[0128] Jede gemeinsame Benutzerkontokennung könnte durch eine Anzahl unterschiedlicher Benutzer verwendet werden, wodurch mehrere Benutzer vorliegen können, die einer gemeinsamen Benutzerkontokennung zugehörig sind, wobei jeder Benutzer seine oder ihre eigenen (biometrischen) Berechtigungsprüfungsdaten hat. In der Benutzerinformationstabelle sind verschiedene Benutzer aufgeführt, die jeder Benutzerkennung zugehörig sind, und die biometrischen Daten, die zum Kennzeichnen dieses Benutzers verwendet werden.

[0129] Bei diesem System kann eine gemeinsame Benutzerkontokennung nur zum Anmelden an jeweils einem einzigen Endgerät verwendet werden, während ein Benutzer gleichzeitig an einer Anzahl von Endgeräten angemeldet sein kann - zum Beispiel in einem Fall, bei dem ein Hauptkassierer während einer Schicht von einer Registrierkasse zu einer anderen wechseln muss.

Tabelle E.2: Berechtigungsprüfungs-Ergebnisdatenbank-Berechtigungsprüfungs-Ergebnistabelle

Prozess-Nr.	Datum	Datum/Uhrzeit	Endgerät	IP-Adr.	Gemeinsame Benutzerkontokennung	Benutzer
201511230001	30.11.2016	10:11:12	1	192.10.1.1	001	B
201511230002	30.11.2016	10:11:15	1	192.10.1.1	001	C
201511230002	30.11.2016	10:11:15	1	192.10.1.1	001	A
...	
20151123000x	30.11.2016	10:15:33	1	192.10.1.1	002	C

[0130] Bei den Beispielen erfolgt die Kennzeichnung einzelner Endgeräte durch eine einfache Zahl 1 bis x an jeweils einer IP-Adresse, aber es wird klar sein, dass das Endgerät alternativ durch die IP-Adresse selbst, eine alphanumerische Kennung („Schuhabteilung“) oder einen Host-Namen oder eine Host-ID („Ithaca-Schuhregisterkasse 1“) gekennzeichnet sein kann.

Tabelle E.3: Endgerätenutzungsstatus-DB: Endgerätenutzungsverhältnis je Zeitfenster

Datum	Zeitfenster	Endgerät	Benutzer				
			A	B	C	...	XX
29.11.2016	09:00-10:00	1	15%	35%	25%	...	0 %
29.11.2016	09:00-10:00	2	50%	0 %	20%	...	0 %
...
29.11.2016	09:00-10:00	X	0%	0 %	0 %	...	100 %
...
29.11.2016	17:00-18:00	1	50%	25%	0 %	...	0 %
29.11.2016	17:00-18:00	2	0%	40%	30%	...	0 %
...
29.11.2016	17:00-18:00	X	0%	0 %	20%	...	60 %

[0131] Zu beachten ist bei dem Beispiel von Tabelle E.3, dass das Ergebnis ein Anmeldungs-nutzungsverhältnis von 15 % für Benutzer A und 35 % für Benutzer B und 25 % für Benutzer C in einem Zielzeitraum von 9:00 Uhr bis 10:00 Uhr an einem bestimmten Tag zeigt.

[0132] Diese Informationen können verwendet werden, um die Berechtigungsprüfungs-Prioritätstabelle einzurichten - denjenigen Benutzern, die das Endgerät höchstwahrscheinlich nutzen, wird innerhalb eines be-

stimmten Zeitfensters eine höhere Priorität für das Endgerät als Benutzern zugeordnet, die dieses Endgerät in diesem Zeitfenster weniger wahrscheinlich (oder so gut wie nicht) nutzen. Zur Berechtigungsprüfungs-Prioritätstabelle siehe die folgende Tabelle E.5.

Tabelle E.4: Endgerätebeziehungsdatenbank- Endgerätebeziehungstabelle

		Endgerät (Ziel für Beziehung)			
		1	2	...	X
Endgerät (Ursprung)	1	70%	20%	...	4%
	2	30%	50%	...	13%

	X	5%	14%	...	70%

[0133] In Tabelle E.4 beträgt das Beziehungsverhältnis von Endgerät 1 zu Endgerät 2 20 %. Dieses Verhältnis bedeutet, dass sich der Benutzer, der sich beim Endgerät 1 am Endgerät angemeldet hat, beim nächsten Anmelden zu 20 % beim Endgerät 2 anmeldet.

[0134] Die Endgerätebeziehungen aus dieser Tabelle können mit den Daten aus der Endgerätenutzungstabelle E.3 kombiniert werden, um die Gesamtpriorität zu ermitteln, die in der folgenden Tabelle E.5 gespeichert wird.

[0135] Diese Tabelle stellt Informationen über diejenigen Endgeräte bereit, die unter einigen bestimmten Gruppen genutzt werden, in denen Benutzer Endgeräte während eines bestimmten Zeitraums häufig wechseln. Die Prioritätensetzung berechnet nicht nur die Nutzung eines einzelnen Endgeräts sondern auch unter Berücksichtigung der Nutzung mehrerer Endgeräte. Und in dieser Situation werden Endgerätebeziehungsdaten aus Tabelle E.4 verwendet.

[0136] Endgerätenutzungsdaten für die Berechtigungsprüfungspriorität unter Berücksichtigung der Nutzung mehrerer Endgeräte und der Endgerätenutzungsbeziehung werden zum Beispiel durch die folgende Formel erhalten:

Geschätzte Endgerätenutzung für Endgerät (W) im Zeitfenster (T) = $\sum_{i=1}^x$ (Endgerätebeziehung zwischen Endgerät (W) und Endgerät (i) aus Tabelle E. 4 xx Endgerätenutzungsverhältnis für Endgerät (i) im Zeitfenster (T) aus Tabelle E.3),

wobei die Summierung auf alle Endgeräte angewendet wird, die mit „Endgerät 1“ bis „Endgerät x“ bezeichnet sind.

Tabelle E.5: Berechtigungsprüfungs-Prioritätsdatenbank-Berechtigungsprüfungs-Prioritätstabelle

Endgerät	Datum	Zeitfenster	Berechtigungsprüfungspriorität				
			Priorität 1	Priorität 2	Priorität 3	...	Priorität N
1	30.11.2016	09:00-10:00	Benutzer B	Benutzer C	Benutzer A	...	Benutzer G
2	30.11.2016	10:00-11:00	Benutzer B	Benutzer A	Benutzer Q	...	Benutzer XX
...
X	30.11.2016	23:00-24:00	Benutzer XX	Benutzer Q	Benutzer E	...	Benutzer FF

[0137] In Tabelle E.5 zeigt das Beispiel, dass die Berechtigungsprüfungspriorität für Endgerät 1 im Zeitfenster 9:00 Uhr bis 10:00 Uhr am 30.11.2016 den Benutzer B betrifft (auf der Grundlage seiner 35 % Nutzung dieses Endgeräts im selben Zeitfenster am vorhergehenden Tag), dann den Benutzer C (25 %), dann den Benutzer A (15 %) ... schließlich den Benutzer XX (der dieses Endgerät während des gesamten vorhergehenden Tages nicht genutzt hat).

Flussdiagramm des Verfahrens der 1:N-Berechtigungsprüfung

Figur 6 zeigt ein Flussdiagramm des Verfahrens der 1:N-Berechtigungsprüfung.

[0138] Bei diesem Beispiel steht die gemeinsame Benutzerkontokennung 001 für alle Benutzer in einer einzigen Gruppe - zum Beispiel für die Mitarbeiter der Schuhabteilung in einem Warenhaus. Die Schuhabteilung könnte eine Anzahl von Registrierkassenendgeräten aufweisen, die mit „Endgerät 1“ bis „Endgerät x“ bezeichnet sind, wobei bei Öffnung des Warenhauses alle Endgeräte in den Abteilungen durch die gemeinsame Benutzerkontokennung 001 geöffnet werden. Jeder der sechsundzwanzig Mitarbeiter in der Abteilung ist mit einem Buchstaben bezeichnet, zum Beispiel mit Benutzer „A“ ... Benutzer „Z“, und jeder der sechsundzwanzig Mitarbeiter hat zu Berechtigungsprüfungszwecken seine eigenen biometrischen Daten. Alle der sechsundzwanzig Mitarbeiter halten sich wahrscheinlich nicht in jedem beliebigen Zeitfenster im Warenhaus auf, da jeder seinen bzw. ihre eigene Arbeitszeit hat, wenn sie aber anwesend sind, müssen sie unter Umständen an einem beliebigen der Endgeräte 1 bis x auf Berechtigung geprüft werden (sich anmelden).

[0139] Jetzt möchte sich ein Benutzer (Benutzer M) am 30. November 2017 um 9:30 Uhr morgens an einem Zielendgerät anmelden, beispielsweise am Endgerät 1. Der Benutzer hat sich möglicherweise zuvor an einem oder mehreren anderen Endgeräten angemeldet. Der Benutzer gibt seine Berechtigungsprüfungsdaten ein (zum Beispiel legt er seinen Daumen auf ein Lesegerät oder gibt seinen Code am Tastenfeld der Registrierkasse ein).

[0140] Nach dem Stand der Technik würde das System dann den Berechtigungsprüfungsprozess für jeden der Benutzer (Benutzer A bis Z) in der Gruppe (gemeinsame Benutzerkontokennung 1, die Schuhabteilung) durchführen müssen, bis es eine Übereinstimmung bei den Biometriedaten für einen neuen Benutzer gefunden hat. Wenn die Biometriedaten anhand des Benutzernamens nacheinander angeordnet wurden, würde das System zum Beispiel jeden der Benutzer von Benutzer A bis Benutzer L durchlaufen, bevor es eine Übereinstimmung bei Benutzer M findet. Daher würde das System den Berechtigungsprüfungsprozess zwölf Mal durchlaufen. Es ist offensichtlich, dass dies bei größeren Gruppen eine erhebliche Zeit in Anspruch nehmen könnte.

[0141] Diese Situation kann verbessert werden, indem die Benutzer priorisiert werden, von denen erwartet werden könnte, dass es sich in einem bestimmten Zeitfenster an einem bestimmten Endgerät anmelden. Dies kann in einer Berechtigungsprüfungs-Prioritätstabelle gespeichert werden. Die Berechtigungsprüfungs-Prioritätstabelle enthält die folgenden Informationen:

Tabelle F.1: Berechtigungsprüfungs-Ergebnistabelle

End-gerät	Datum	Zeitfenster	Berechtigungsprüfungspriorität					
			Priorität 1	Priorität 2	...	Priorität n	...	Priorität x
1	30.11.2016	09:00-10:00	Benutzer B	Benutzer C	...	Benutzer M	...	Benutzer Q
2	30.11.2016	09:00-10:00	Benutzer A	Benutzer C	...	Benutzer D	...	Benutzer X
...
X	30.11.2016	09:00-10:00	Benutzer D	Benutzer B	...	Benutzer Q	...	Benutzer F

[0142] Ab dem Schritt **222** von **Fig. 3**, bei dem sich der Benutzer M am Endgerät **1** für die gemeinsame Benutzerkontokennung **001** anmelden möchte, ruft das Berechtigungsprüfungsprogramm **66** Einträge aus der Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät im aktuellen Zeitfenster ab (Schritt **302**).

[0143] Die aus der Tabelle für das Zielendgerät extrahierten Informationen würden wie folgt lauten:

Tabelle F.1(a) - Berechtigungsprüfungs-Prioritätstabelle für Zielendgerät

Endgerät	Datum	Zeitfenster	Berechtigungsprüfungspriorität					
			Priorität 1	Priorität 2	..	Priorität n	...	Priorität x
1	30.11.2016	09:00-10:00	Benutzer B	Benutzer C	..	Benutzer M	...	Benutzer Q

[0144] Dies gibt an, dass sich der Benutzer M in der Liste auf der Priorität n für das Endgerät 1 in diesem Zeitfenster befindet. Wenn das Verfahren einfach diese Prioritätstabelle nutzt, würde das System lediglich (n - 1) Sätze von Berechtigungsprüfungsdaten überprüfen müssen, bevor Daten des Benutzers M erreicht werden. Unter der Voraussetzung, dass nur eine relativ kleine Teilmenge von Benutzern Priorität für dieses Endgerät zu diesem Zeitpunkt hat (d.h. (n - 1) < 12), würde dies die Anmeldezeit für Benutzer M verkürzen.

[0145] Beim aktuellen Verfahren wird der Berechtigungsprüfungsprozess jedoch verbessert, wie nachstehend erörtert. Das Berechtigungsprüfungsprogramm **66** liest aus der Berechtigungsprüfungs-Ergebnistabelle den Berechtigungsprüfungsstatus bei den anderen Endgeräten (Schritt **308**).

Tabelle F.2: Berechtigungsprüfungs-Ergebnistabelle

Prozess-Nr.	Datum	Datum/Uhrzeit	Endgerät	Benutzer
201511230001	30.11.2016	09:11:12	Endgerät 3	Benutzer A
201511230002	30.11.2016	09:11:15	Endgerät 11	Benutzer B
201511230003	30.11.2016	09:11:17	Endgerät 12	Benutzer C
201511230004	30.11.2016	09:13:20	Endgerät 8	Benutzer G
201511230005	30.11.2016	09:20:23	Endgerät 11	Benutzer D
201511230006	30.11.2016	09:25:29	Endgerät 11	Benutzer N
...

[0146] Somit stellt das Berechtigungsprüfungsprogramm fest, dass Benutzer A aktuell am Endgerät **3** angemeldet ist, die Benutzer B, D und N aktuell am Endgerät **11** angemeldet sind, Benutzer C aktuell am Endgerät **12** angemeldet ist und Benutzer G am Endgerät **8** angemeldet ist, wie oben angemerkt. Andere Benutzer sind an anderen Endgeräten angemeldet.

[0147] Der in Schritt **308** gelesene Berechtigungsprüfungsstatus wird anschließend verwendet, um eine zeitweilige Berechtigungsprüfungs-Prioritätstabelle zu erstellen, indem Prioritätsinformationen und ein Maskenstatus hinzugefügt werden, wie nachstehend angemerkt (Schritt **310**). Für jede Priorität werden weitere Daten hinzugefügt, um einen Maskenstatus anzugeben. Da der Maskenstatus zwei Zustände hat, definiert das Beispiel die Statuszustände als „wahr“ in der Bedeutung von „maskiert“ und „falsch“ in der Bedeutung von „nicht maskiert“. Es wird klar sein, dass ein beliebiger anderer Code für diese Funktion verwendet werden könnte, zum Beispiel eine einfache binäre Zahl 0 oder 1 usw.

[0148] Jeder Benutzer, der bereits bei einem anderen Endgerät angemeldet ist, wird maskiert - das heißt, es wird ihm bei diesem Beispiel ein Maskenwert „wahr“ zugewiesen. Bei Betrachtung lediglich der Maskierung für das Zielendgerät würde die Tabelle wie folgt lauten:

Tabelle F.3: Zeitweilige Berechtigungsprüfungs-Prioritätstabelle

Endgerät	...	Berechtigungsprüfungspriorität								
		Priorität 1	Maske für 1	Priorität 2	Maske für 2	...	Priorität n	Maske für n		
1	...	Benutzer B	Wahr	Benutzer C	Wahr	...	Benutzer M	Falsch	...	

[0149] Somit sind bei diesem Beispiel die ersten beiden Prioritätseinträge maskiert („wahr“), da diese Benutzer anderswo auf Berechtigung geprüft wurden. Angenommen wird, dass andere, als Priorität 3 bis (n - 1) priorisierte Benutzer ebenfalls angemeldet und somit ebenfalls ausgeblendet sind.

[0150] Zu beachten ist, dass bei Abmeldung eines Benutzers von einem Endgerät die Maskierung für diesen Benutzer in der Berechtigungsprüfungs-Prioritätstabelle an allen Stellen entfernt würde, an denen er auftritt.

[0151] Die „Berechtigungsprüfungs-Prioritätstabelle“ unterscheidet sich wie folgt von der „zeitweiligen Berechtigungsprüfungs-Prioritätstabelle“:

[0152] Statusänderung: Die Berechtigungsprüfungs-Prioritätstabelle enthält einen statischen Status zwischen dem Messintervall für Statistiken des Authentifizierungsbetriebs, stündlich, täglich oder wöchentlich. Andererseits kann die zeitweilige Berechtigungsprüfungs-Prioritätstabelle ihre Daten und ihren Maskierungsstatus anhand des Betriebs der Berechtigungsprüfungen dynamisch ändern.

[0153] Speicherort: Da die Berechtigungsprüfungs-Prioritätstabelle von statischer Art ist, sind diese Tabellen vorzugsweise in einer Datenablage oder einem Speichermedium gespeichert. Andererseits muss die zeitweilige Berechtigungsprüfungs-Prioritätstabelle in der Lage sein, ihren Maskierungsstatus rechtzeitig und schnell zu ändern, sodass diese Tabellen im Prozessor Hauptspeicher gespeichert sein sollten.

[0154] Erstellen der Tabelle: Die zeitweilige Berechtigungsprüfungs-Prioritätstabelle wird erstellt, in dem die Berechtigungsprüfungs-Prioritätstabelle wie oben angemerkt in geänderter Form aus dem Speicher in den Hauptspeicher geladen wird.

[0155] Das Berechtigungsprüfungsprogramm **66** führt dann unter Verwendung der zeitweiligen Berechtigungsprüfungs-Prioritätstabelle eine 1:N-Berechtigungsprüfung durch (Schritt **312**).

[0156] Wenn sich Benutzer M am Endgerät 1 anzumelden versucht, versucht das System daher keine Berechtigungsprüfung mit Informationen des Benutzers B oder Informationen des Benutzers C oder beliebigen der anderen Benutzer in den Prioritäten 3 bis (n - 1). Diese Benutzer werden übersprungen („maskiert“), und das System geht direkt zur Priorität n - Benutzer N - über, der die Berechtigungsprüfung beim ersten Versuch erfolgreich durchläuft.

[0157] Dies verbessert die Leistung des Systems, da die Berechtigungsprüfung nicht gegen die biometrischen Daten eines beliebigen Benutzers durchgeführt werden muss, der bereits woanders angemeldet ist (deren Einträge maskiert sind), und die übrigen Benutzer anhand ihrer Priorität (Wahrscheinlichkeit, dass sich der Benutzer zu diesem Zeitpunkt an diesem Endgerät anmelden könnte), sodass das System die Berechtigungsprüfung zunächst für diejenigen Benutzer durchführen kann, die höchstwahrscheinlich versuchen, sich auf Berechtigung zu prüfen zu lassen.

[0158] Außerdem ist zu beachten, dass Benutzer M ebenfalls ausgeblendet werden würde, wenn er an einem anderen Endgerät angemeldet wäre - die Maske für Priorität n würde „wahr“ lauten. In diesem Fall würde sich Benutzer M nicht am Endgerät 1 auf Berechtigung prüfen lassen können. Dies würde die Sicherheit in Kraft setzen, indem ein Benutzer gezwungen wird, sich an einem der durch ihn genutzten Endgeräte abzumelden, bevor er sich anderswo anmeldet. Alternativ könnte das System so eingerichtet sein, dass ein Benutzer nach einem Zeitraum der Inaktivität automatisch abgemeldet wird, sodass das Aufheben der Maskierung automatisch erfolgen würde, wodurch sich ein Benutzer frei von Endgerät zu Endgerät bewegen kann, solange eine vorgegebene Zeit zwischen Anmeldungen liegt.

[0159] Wenn die Berechtigungsprüfung durch das Endgerät akzeptiert wurde (Schritt **314**), wird der Zugriff auf das Endgerät gewährt (Schritt **316**), wird das Berechtigungsprüfungsergebnis in der Berechtigungsprüfungstabelle gespeichert (Schritt **318**) und das Verfahren endet.

[0160] Wenn die Berechtigungsprüfung durch das Endgerät nicht akzeptiert wurde (Schritt **314**) wird das Berechtigungsprüfungsergebnis in der Berechtigungsprüfungstabelle gespeichert (Schritt **318**), wird eine Nachricht an das Endgerät gesendet, die anzeigt, dass die Berechtigungsprüfung nicht akzeptiert wurde (Schritt **320**), und das Verfahren endet.

Hauptelemente des Systems:

Element 1: Ausführungsmechanismus zur Verarbeitung der Hybrid-Berechtigungsprüfung

[0161] Als Reaktion auf die Berechtigungsprüfungsanforderung des Benutzers wird eine Berechtigungsprüfung durchgeführt, indem die eingegebenen biometrischen Informationen des Zielbenutzers mit gespeicherten biometrischen Berechtigungsprüfungs-Referenzdaten und gespeicherten Berechtigungsprüfungs-Referenzdaten der biometrischen Informationen auf Berechtigung geprüft werden. Dieses System realisiert die 1:1-Berechtigungsprüfung und auch die 1:N-Berechtigungsprüfung.

[0162] Der 1:N-Berechtigungsprüfungsprozess wird gemäß der relevanten Berechtigungsprüfungspriorität durch Endgeräte durchgeführt.

[0163] Außerdem wird bei dieser 1:N-Berechtigungsprüfung die gemeinsame Benutzerkontokennung bestätigt, die durch ein anderes Endgerät angemeldet wurde, wobei das durch das andere Endgerät angemeldete gemeinsame Benutzerkonto in der Berechtigungsprüfungs-Prioritätsliste maskiert wird, um es von den Berechtigungsprüfungszielen auszuschließen.

Element 2: Endgeräterelevanz-Berechnungsfunktion

[0164] Eine Berechnung der dynamischen Gruppierung von Endgeräten, d.h. von Abhängigkeitsbeziehungen zwischen Endgeräten auf der Grundlage der Berechtigungsprüfungsergebnisdaten im Benutzerendgerät, wird gespeichert.

Element 3: Funktion zum Erstellen der Berechtigungsprüfungs-Prioritätsliste

[0165] Erstellt und speichert eine Berechtigungsprüfungs-Prioritätsliste für jede vordefinierte Bedingung, zum Beispiel Zeit, auf der Grundlage des Berechtigungsprüfungsprotokolls bei jedem Endgerät und der Abhängigkeitsbeziehungsdaten zwischen den Endgeräten.

Andere Elemente

[0166] Bei der vorliegenden Erfindung kann es sich um ein System, ein Verfahren und/oder ein Computerprogrammprodukt in einem beliebigen möglichen Integrationsgrad technischer Einzelheiten handeln. Das Computerprogrammprodukt kann (ein) durch einen Computer lesbare(s) Speichermedium (oder -medien) beinhalten, auf dem/denen durch einen Computer lesbare Programmanweisungen gespeichert ist/sind, um einen Prozessor zu veranlassen, Aspekte der vorliegenden Erfindung auszuführen.

[0167] Bei dem durch einen Computer lesbaren Speichermedium kann es sich um eine physische Einheit handeln, auf der Anweisungen zur Verwendung durch eine Einheit zur Ausführung von Anweisungen aufbewahrt und gespeichert sein können. Bei dem durch einen Computer lesbaren Speichermedium kann es sich zum Beispiel, ohne auf diese beschränkt zu sein, eine elektronische Speichereinheit, um eine magnetische Speichereinheit, eine optische Speichereinheit, eine elektromagnetische Speichereinheit, eine Halbleiterspeichereinheit oder eine beliebige geeignete Kombination des Vorstehenden handeln. Zu einer nicht erschöpfenden Liste konkreter Beispiele des durch einen Computer lesbaren Speichermediums gehören die folgenden: eine transportable Computerdiskette, eine Festplatte, ein Direktzugriffsspeicher (RAM), ein Nur-Lese-Speicher (ROM), ein löschbarer programmierbarer Nur-Lese-Speicher (EPROM bzw. Flash-Speicher), ein statischer Direktzugriffsspeicher (SRAM), ein transportabler Compact-Disc-Nur-Lese-Speicher (CD-ROM), eine DVD (digital versatile disc), ein Speicher-Stick, eine Diskette, eine mechanisch codierte Einheit wie zum Beispiel Lochkarten oder erhabene Strukturen in einer Rille, auf denen Anweisungen gespeichert sind, und beliebige geeignete Kombinationen des Vorstehenden. Ein durch einen Computer lesbares Speichermedium im hierin verwendeten Sinne ist nicht so auszulegen, dass es sich dabei um flüchtige Signale handelt, beispielsweise um Funkwellen oder sich frei ausbreitende elektromagnetische Wellen, um elektromagnetische Wellen, die sich durch einen Hohlleiter oder andere Übertragungsmedien ausbreiten (z.B. Lichtimpulse, die ein Lichtwellenleiterkabel durchlaufen) oder um elektrische Signale, die über ein Kabel übertragen werden.

[0168] Hierin beschriebene durch einen Computer lesbare Programmanweisungen können über ein Netzwerk, zum Beispiel das Internet, ein lokales Netzwerk ein Weitverkehrsnetzwerk und/oder ein Drahtlosnetzwerk von einem durch einen Computer lesbaren Speichermedium auf betreffende Datenverarbeitungs-/Verarbeitungseinheiten oder auf einen externen Computer oder eine externe Speichereinheit heruntergeladen werden. Das

Netzwerk kann Kupferübertragungskabel, Lichtwellenleiter, Drahtlosübertragung, Router, Firewalls, Switches, Gateway-Computer und/oder Edge-Server aufweisen. Eine Netzwerkadapterkarte oder eine Netzwerkschnittstelle bei jeder Datenverarbeitungs-/Verarbeitungseinheit empfängt durch einen Computer lesbare Programm-Anweisungen aus dem Netzwerk und leitet die durch einen Computer lesbaren Programmanweisungen zur Speicherung in einem durch einen Computer lesbaren Speichermedium innerhalb der jeweiligen Datenverarbeitungs-/Verarbeitungseinheit weiter.

[0169] Bei durch einen Computer lesbaren Programmanweisungen zum Ausführen von Arbeitsschritten der vorliegenden Erfindung kann es sich um Assembler-Anweisungen, ISA-Anweisungen (Instruction-Set-Architecture), Maschinenanweisungen, maschinenabhängige Anweisungen, Mikrocode, Firmware-Anweisungen, zustandssetzende Daten oder entweder Quellcode oder Objektcode handeln, die in einer beliebigen Kombination aus einer oder mehreren Programmiersprachen geschrieben werden, darunter objektorientierte Programmiersprachen wie z.B. Smalltalk, C++ o.Ä. sowie prozedurale Programmiersprachen wie z.B. die Programmiersprache „C“ oder ähnliche Programmiersprachen. Die durch einen Computer lesbaren Programmanweisungen können vollständig auf dem Computer des Benutzers, teilweise auf dem Computer des Benutzers, als eigenständiges Softwarepaket, teilweise auf dem Computer des Benutzers und teilweise auf einem entfernt angeordneten Computer oder vollständig auf dem entfernt angeordneten Computer oder Server ausgeführt werden. Beim letztgenannten Szenario kann der entfernt angeordnete Computer mit dem Computer des Benutzers über eine beliebige Art von Netzwerk verbunden sein, unter anderem über ein lokales Netzwerk (Local Area Network, LAN) oder über ein Weitverkehrsnetzwerk (Wide Area Network, WAN), oder die Verbindung kann zu einem externen Computer hergestellt sein (beispielsweise über das Internet unter Nutzung eines Internet-Diensteanbieters (Internet Service Provider)). Bei einigen Ausführungsformen können elektronische Schaltungen, zu denen beispielsweise programmierbare Logikschaltungen, vor Ort programmierbare Schaltkreise (Field-Programmable Gate Arrays, FPGA) oder programmierbare logische Arrays (PLA) gehören, die durch einen Computer lesbaren Programmanweisungen ausführen, indem Zustandsinformationen der durch einen Computer lesbaren Programmanweisungen genutzt werden, um die elektronische Schaltung zu personalisieren, sodass Aspekte der vorliegenden Erfindung durchgeführt werden.

[0170] Aspekte der vorliegenden Erfindung sind hierin unter Bezugnahme auf Flussdiagrammdarstellungen und/oder Blockschemata von Verfahren, Vorrichtungen (Systemen) und Computerprogrammprodukten gemäß Ausführungsformen der Erfindung beschrieben. Es wird klar sein, dass jeder Block der Flussdiagramme und/oder der Blockschemata und Kombinationen von Blöcken in den Flussdiagrammen und/oder Blockschemata durch einen Computerprogrammanweisungen realisiert werden kann bzw. können.

[0171] Diese Computerprogrammanweisungen können einem Prozessor eines Mehrzweckcomputers, eines Spezialcomputers oder anderer programmierbaren Datenverarbeitungsvorrichtungen bereitgestellt werden, um eine Maschine zu erzeugen, sodass die Anweisungen, die über den Prozessor des Computers oder anderer programmierbarer Datenverarbeitungsvorrichtungen ausgeführt werden, Mittel schaffen, um die in einem Block bzw. in den Blöcken des Flussdiagramms bzw. der Flussdiagramme und/oder des Blockschemas bzw. der Blockschemata angegebenen Funktionen/Aktionen zu realisieren. Diese durch einen Computer lesbaren Programmanweisungen können ebenfalls in einem durch einen Computer lesbaren Medium gespeichert sein, das einen Computer, andere programmierbare Datenverarbeitungsvorrichtungen oder andere Einheiten anweisen kann, in einer bestimmten Weise zu funktionieren, sodass das durch einen Computer lesbare Medium mit darauf gespeicherten Anweisungen ein Erzeugnis aufweist, das Anweisungen enthält, die die in einem Block bzw. in den Blöcken der Flussdiagramme und/oder der Blockschemata angegebene Funktion/Aktion realisieren.

[0172] Die durch einen Computer lesbaren Programmanweisungen können auch in einen Computer, in andere programmierbare Datenverarbeitungsvorrichtungen oder in andere Einheiten geladen werden, um zu bewirken, dass auf dem Computer, auf anderen programmierbaren Vorrichtungen oder anderen Einheiten eine Reihe von Arbeitsschritten ausgeführt wird, um einen mittels Computer realisierten Prozess zu schaffen, sodass die Anweisungen, die auf dem Computer, auf anderen programmierbaren Vorrichtungen oder Einheiten ausgeführt werden, die in einem Block bzw. in den Blöcken der Flussdiagramme und/oder der Blockschemata angegebenen Funktionen/Aktionen realisieren.

[0173] Die Flussdiagramme und Blockschemata in den Figuren veranschaulichen die Architektur, Funktionalität und Wirkungsweise möglicher Realisierungsformen von Systemen, Verfahren und Computerprogrammprodukten gemäß verschiedenen Ausführungsformen der vorliegenden Erfindung. In diesem Zusammenhang kann jeder Block in den Flussdiagrammen bzw. in den Blockschemata eine Steuerungskomponente, ein Segment oder einen Abschnitt von Anweisungen darstellen, das bzw. der eine oder mehrere ausführbare Anweisungen zur Realisierung der angegebenen Logikfunktion bzw. Logikfunktionen aufweist. Bei einigen alternati-

ven Ausführungen können die in dem Block angegebenen Funktionen in einer anderen Reihenfolge als in den Figuren gezeigt stattfinden. Beispielsweise können zwei hintereinander aufgeführte Blöcke tatsächlich im Wesentlichen gleichzeitig ausgeführt werden, oder die Blöcke können je nach der mit den Blöcken verbundenen Funktionalität manchmal in umgekehrter Reihenfolge ausgeführt werden. Darüber hinaus ist anzumerken, dass jeder Block der dargestellten Blockschemata und/oder Flussdiagramme sowie Kombinationen von Blöcken in den dargestellten Blockschemata und/oder Flussdiagrammen mit Hilfe zweckgebundener hardwaregestützter Systeme zur Ausführung der angegebenen Funktionen bzw. Aktionen oder mit Hilfe von Kombinationen aus zweckgebundener Hardware und zweckgebundenen Computeranweisungen realisiert werden kann bzw. können.

Patentansprüche

1. Verfahren zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten, wobei das Verfahren die Schritte aufweist:

- a) durch einen Computer ein Empfangen von Benutzereingaben, um eine Berechtigungsprüfung auf einem Zielendgerät zu starten, die biometrische Eingaben vom Benutzer aufweist;
- b) durch den Computer ein vorläufiges, angenähertes Prüfen, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde;
- c) wenn die vorläufige, angenäherte Prüfung ergibt, dass es sich bei dem Benutzer mit hoher Wahrscheinlichkeit um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer ein Ausführen einer 1:1-Berechtigungsprüfung des Benutzers;
- d) wenn die vorläufige, angenäherte Prüfung ergibt, dass es sich bei dem Benutzer nicht mit hoher Wahrscheinlichkeit um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer:
 - i) ein Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster;
 - ii) ein Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle;
 - iii) ein Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist;
 - iv) ein Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, wobei die 1:N-Berechtigungsprüfung nicht gegen die biometrischen Daten der maskierten Benutzer durchgeführt wird;
 - v) ein Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer ein Gewähren des Benutzerzugriffs auf das Zielendgerät und ein Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle; wobei die Berechtigungsprüfungspriorität für die Berechtigungsprüfungs-Prioritätstabelle durch die Schritte ermittelt wird, die aufweisen:
 - durch den Computer ein Berechnen eines Endgerätenutzungsverhältnisses je Zeitfenster auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle und ein Speichern als Endgerätenutzungsverhältnistabelle;
 - durch den Computer ein Berechnen einer Endgerätebeziehung und ein Speichern als Endgerätebeziehungstabelle; und
 - durch den Computer ein Berechnen der Berechtigungsprüfungspriorität auf der Grundlage der Endgerätebeziehungstabelle, der Endgerätenutzungsverhältnistabelle und des Berechtigungsprüfungsergebnisses und ein Speichern der Berechtigungsprüfungspriorität in der Berechtigungsprüfungs-Prioritätstabelle.

2. Verfahren nach Anspruch 1, wobei das Endgerätenutzungsverhältnis je Zeitfenster auf einem Relevanzindex der Anzahl von Anmeldungen eines Benutzers an dem Endgerät innerhalb eines Zeitfensters für das Endgerät und dem Prozentsatz der Nutzung des Endgeräts in einem Zeitfenster beruht.

3. Verfahren nach einem der Ansprüche 2 oder 1, wobei es sich bei der Berechtigungsprüfungspriorität um eine Wahrscheinlichkeit handelt, mit der ein Benutzer das Zielendgerät während eines bestimmten Zeitfensters nutzt.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei bei akzeptierter 1:1-Berechtigungsprüfung ein Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle und ein Gewähren des Zugriffs auf das Zielendgerät erfolgt.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei bei verweigerter 1:1-Berechtigungsprüfung ein Zurückkehren zu Schritt d) i) des Abrufens von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster erfolgt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Berechtigungsprüfungs-Prioritätsliste auf einem früheren Berechtigungsprüfungsstatus von Benutzern in Bezug auf ein Endgerät beruht.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei die zeitweilige Berechtigungsprüfungstabelle im Hauptspeicher gespeichert ist und die Berechtigungsprüfungs-Prioritätstabelle in einer Datenablage gespeichert ist.

8. Computersystem zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten, das einen Computer aufweist, der mindestens einen Prozessor, einen oder mehrere Speicher, ein oder mehrere durch Computer lesbare Speichermedien aufweist, auf denen Programmanweisungen gespeichert sind, die durch den Computer ausführbar sind zum

a) Empfangen von Benutzereingaben, die biometrische Eingaben vom Benutzer aufweisen, durch den Computer, um die Berechtigungsprüfung auf einem Zielendgerät zu starten;

b) vorläufiges, angenähertes Prüfen durch den Computer, ob die vom Benutzer empfangenen biometrischen Eingaben angeben, dass derselbe Benutzer eine Berechtigungsprüfung auf dem Zielendgerät startet, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde;

c) Ausführen einer 1:1-Berechtigungsprüfung des Benutzers durch den Computer, wenn die vorläufige, angenäherte Prüfung ergibt, dass es sich bei dem Benutzer mit hoher Wahrscheinlichkeit um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde;

d) wenn die vorläufige, angenäherte Prüfung ergibt, dass es sich bei dem Benutzer nicht mit hoher Wahrscheinlichkeit um denselben Benutzer handelt, der zuletzt durch den Computer für das Zielendgerät auf Berechtigung geprüft wurde, durch den Computer:

i) Abrufen von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster;

ii) Lesen eines Berechtigungsprüfungsstatus an anderen Endgeräten als dem Zielendgerät auf der Grundlage einer Berechtigungsprüfungs-Ergebnistabelle;

iii) Erstellen einer zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, die aufweist: Prioritätsinformationen für Benutzer für jedes Endgerät, Zeit, Endgeräteinformationen und Maskierung von Benutzern an Endgeräten auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle, wobei die Maskierung auf jeden Benutzer zutrifft, der bereits an Endgeräten angemeldet ist;

iv) Ausführen einer 1:N-Berechtigungsprüfung des Benutzers unter Verwendung der zeitweiligen Berechtigungsprüfungs-Prioritätstabelle, wobei die 1:N-Berechtigungsprüfung nicht gegen die biometrischen Daten der maskierten Benutzer durchgeführt wird;

v) Ermitteln, ob die 1:N-Berechtigungsprüfung akzeptiert wurde; und

v) wenn die 1:N-Berechtigungsprüfung akzeptiert wurde, durch den Computer Gewähren des Benutzerzugriffs auf das Zielendgerät und Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle; wobei die Berechtigungsprüfungspriorität für die Berechtigungsprüfungs-Prioritätstabelle durch die Programmanweisungen ermittelt wird, die aufweisen:

durch den Computer ein Berechnen eines Endgerätenutzungsverhältnisses je Zeitfenster auf der Grundlage der Berechtigungsprüfungs-Ergebnistabelle und ein Speichern als Endgerätenutzungsverhältnistabelle;

durch den Computer ein Berechnen einer Endgerätebeziehung und ein Speichern als Endgerätebeziehungstabelle; und

durch den Computer ein Berechnen der Berechtigungsprüfungspriorität auf der Grundlage der Endgerätebeziehungstabelle, der Endgerätenutzungsverhältnistabelle und des Berechtigungsprüfungsergebnisses und ein Speichern der Berechtigungsprüfungspriorität in der Berechtigungsprüfungs-Prioritätstabelle.

9. Computersystem nach Anspruch 8, wobei das Endgerätenutzungsverhältnis je Zeitfenster auf einem Relevanzindex der Anzahl von Anmeldungen eines Benutzers an dem Endgerät innerhalb eines Zeitfensters für das Endgerät und dem Prozentsatz der Nutzung des Endgeräts in einem Zeitfenster beruht.

10. Computersystem nach Anspruch 8 oder 9, wobei es sich bei der Berechtigungsprüfungspriorität um eine Wahrscheinlichkeit handelt, mit der ein Benutzer das Zielendgerät während eines bestimmten Zeitfensters nutzt.

11. Computersystem nach einem Ansprüche 8 bis 10, wobei bei akzeptierter 1:1-Berechtigungsprüfung ein Speichern des Berechtigungsprüfungsergebnisses in der Berechtigungsprüfungs-Ergebnistabelle und ein Gewähren des Zugriffs auf das Zielendgerät erfolgt.

12. Computersystem nach einem Ansprüche 8 bis 11, wobei bei verweigerter 1:1-Berechtigungsprüfung ein Zurückkehren zu Schritt d) i) des Abrufens von Einträgen aus einer Berechtigungsprüfungs-Prioritätstabelle für das Zielendgerät in einem aktuellen Zeitfenster erfolgt.

13. Computersystem nach einem Ansprüche 8 bis 12, wobei die Berechtigungsprüfungs-Prioritätsliste auf einem früheren Berechtigungsprüfungsstatus von Benutzern in Bezug auf ein Endgerät beruht.

14. Computersystem nach einem Ansprüche 8 bis 13, wobei die zeitweilige Berechtigungsprüfungstabelle im Hauptspeicher gespeichert ist und die Berechtigungsprüfungs-Prioritätstabelle in einer Datenablage gespeichert ist.

15. Computerprogrammprodukt zur Berechtigungsprüfung von Benutzern an mehreren Endgeräten, wobei das Computerprogrammprodukt aufweist:
ein durch einen Computer lesbares Speichermedium, das durch eine Verarbeitungsschaltung gelesen werden kann und auf dem Speicheranweisungen zur Ausführung durch die Verarbeitungsschaltung gespeichert sind, um ein Verfahren nach einem der Ansprüche 1 bis 7 durchzuführen.

16. Computerprogramm, das auf einem durch einen Computer lesbaren Medium gespeichert ist, in den internen Hauptspeicher eines Digitalcomputers geladen werden kann und Softwarecodeabschnitte zum Durchführen des Verfahrens nach einem der Ansprüche 1 bis 7 aufweist, wenn das Programm auf einem Computer ausgeführt wird.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

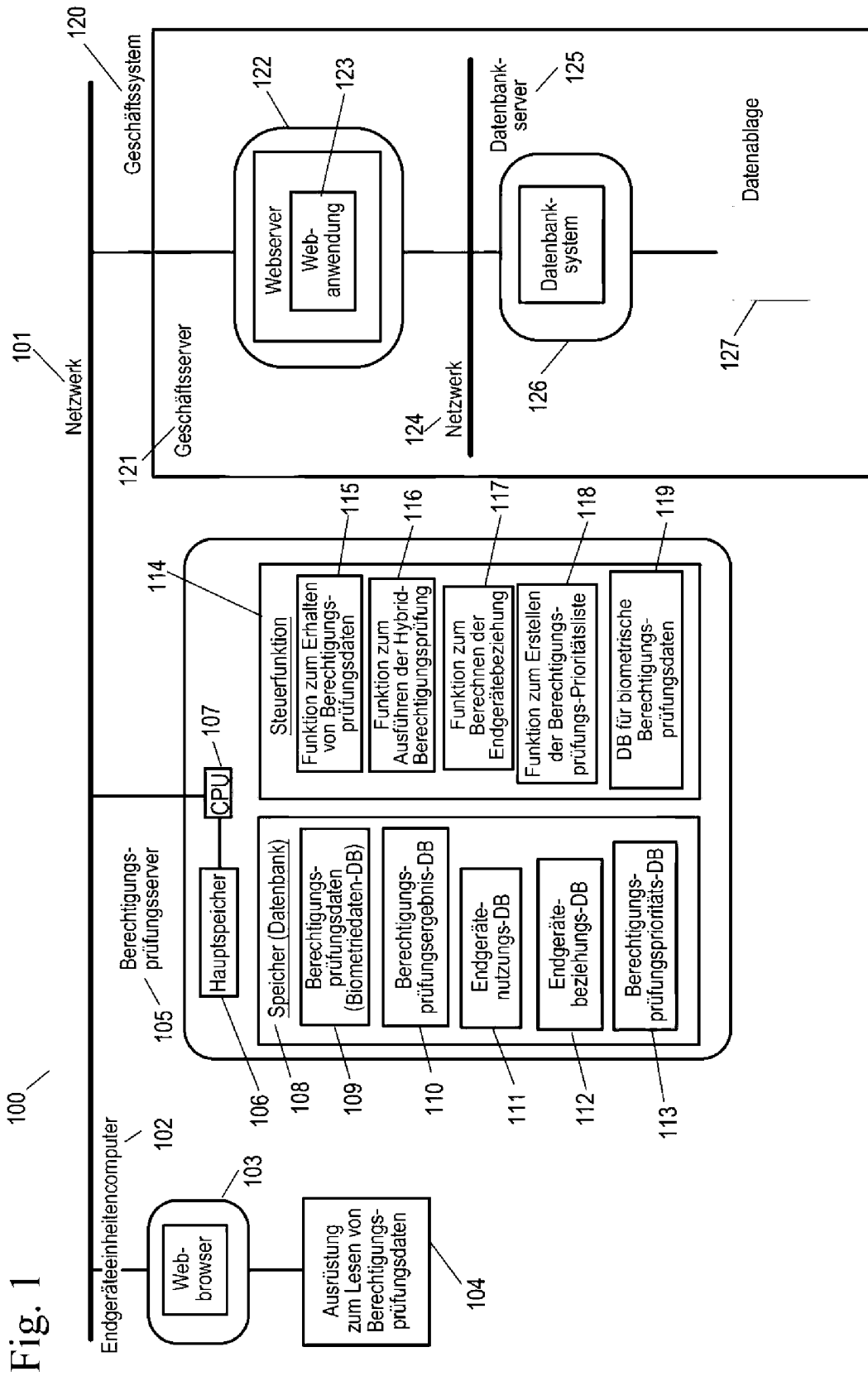


Fig. 2

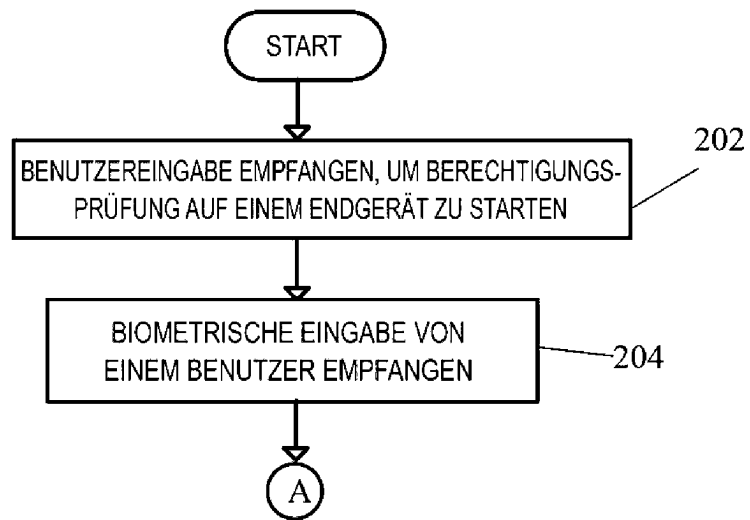


FIG 3, 6

Fig. 3

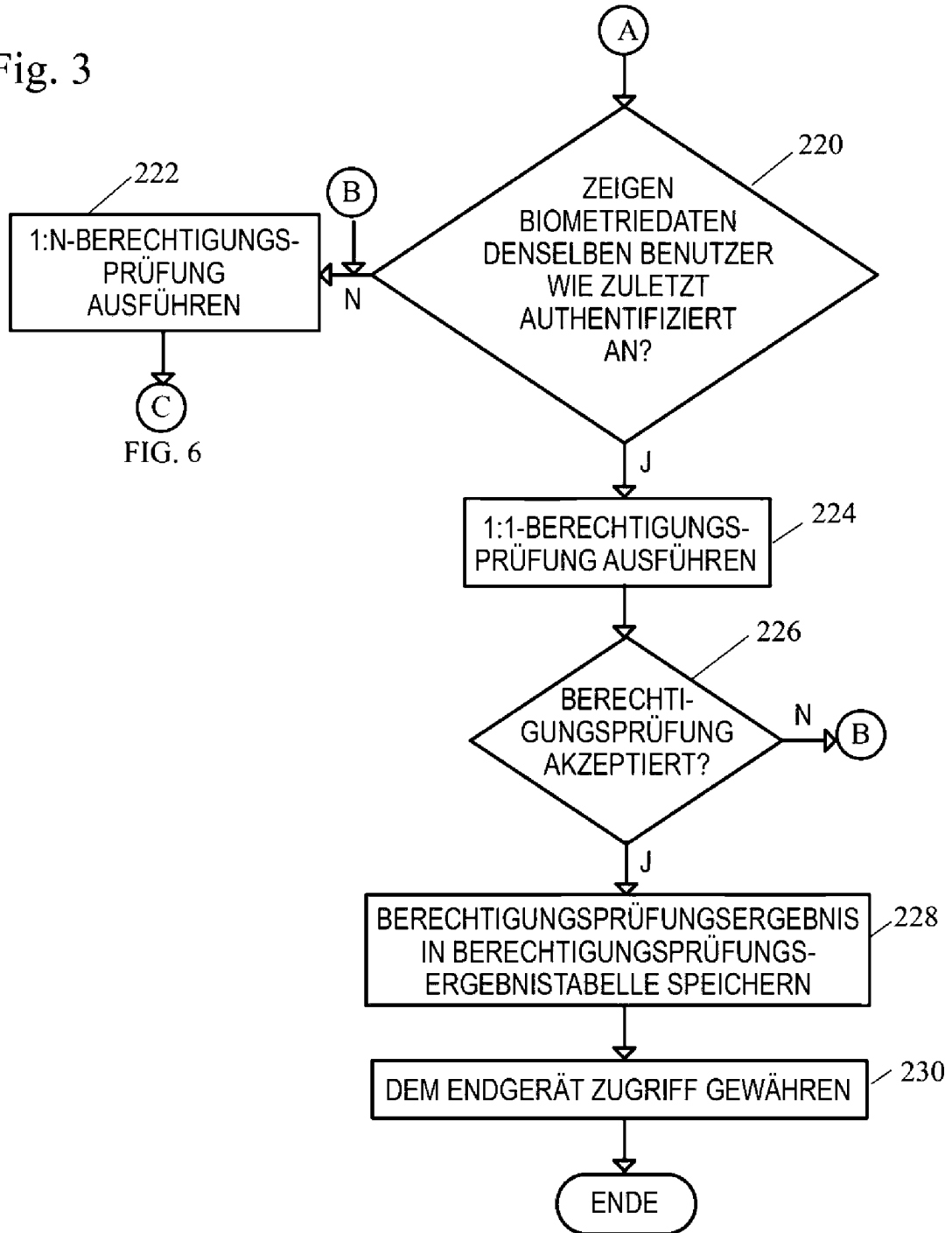


Fig. 4A

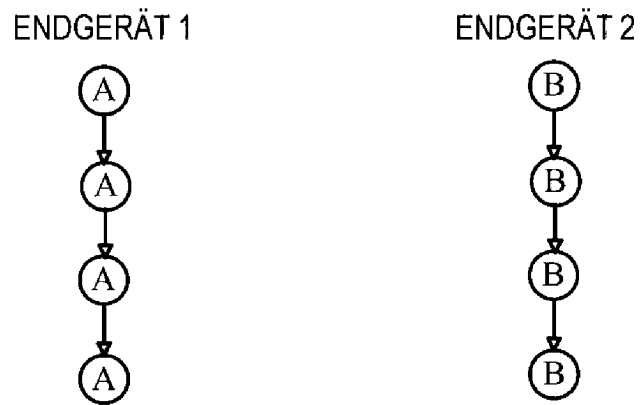


Fig. 4B

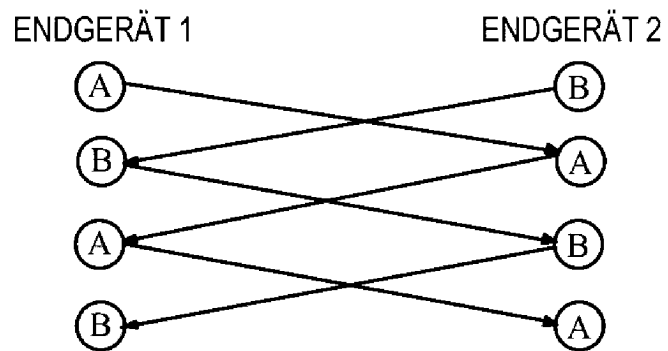


Fig. 5

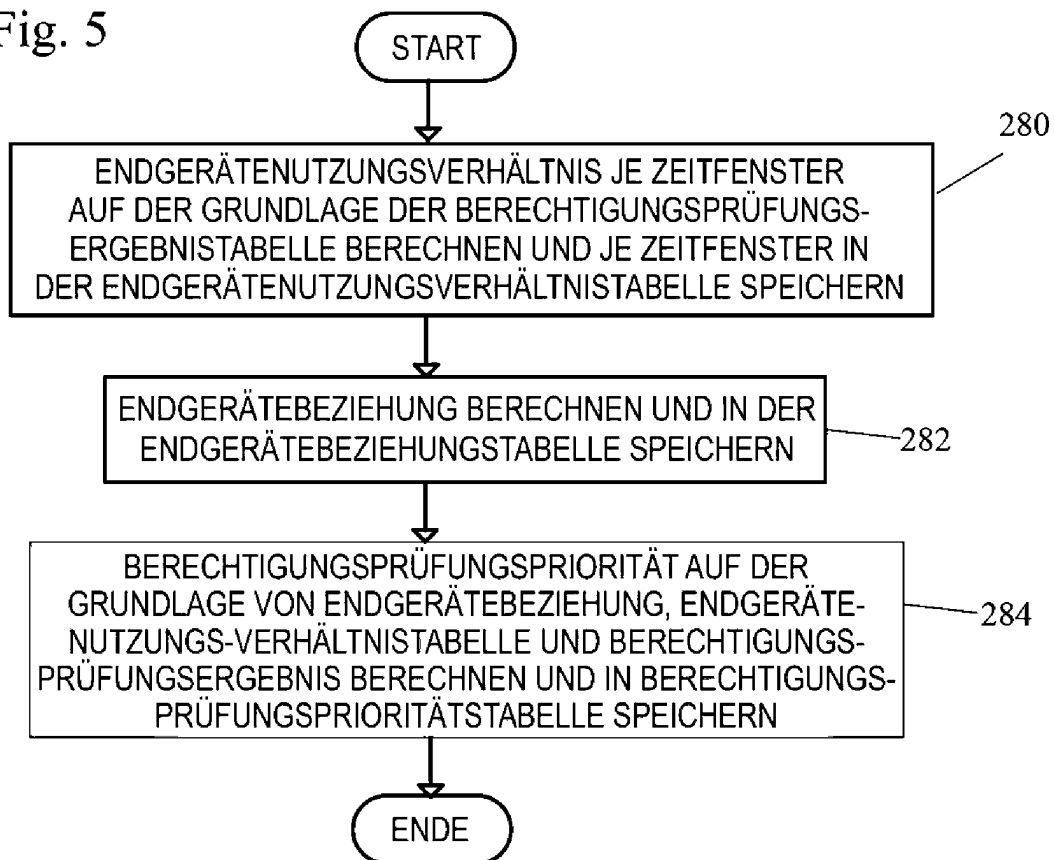
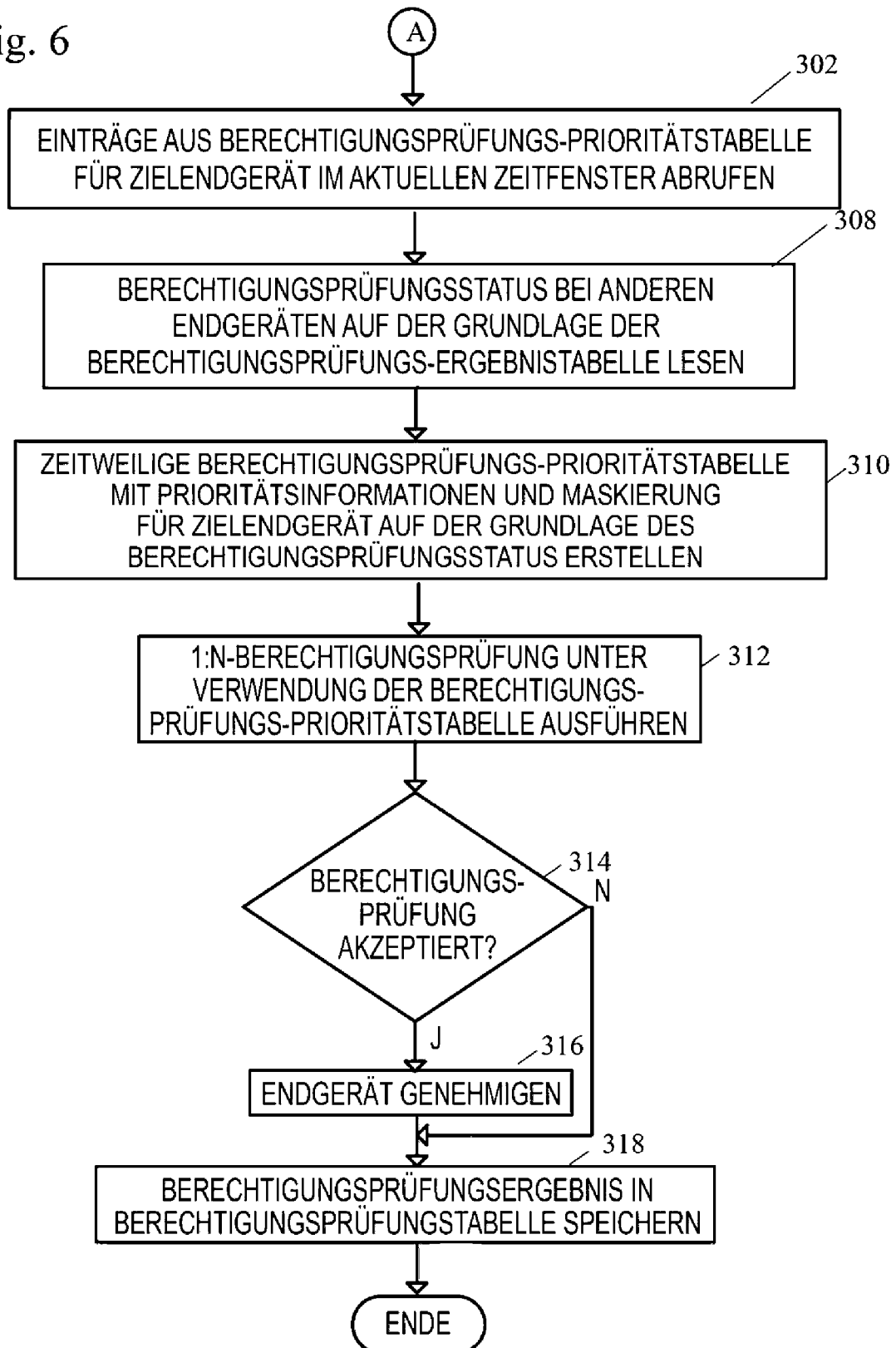


Fig. 6



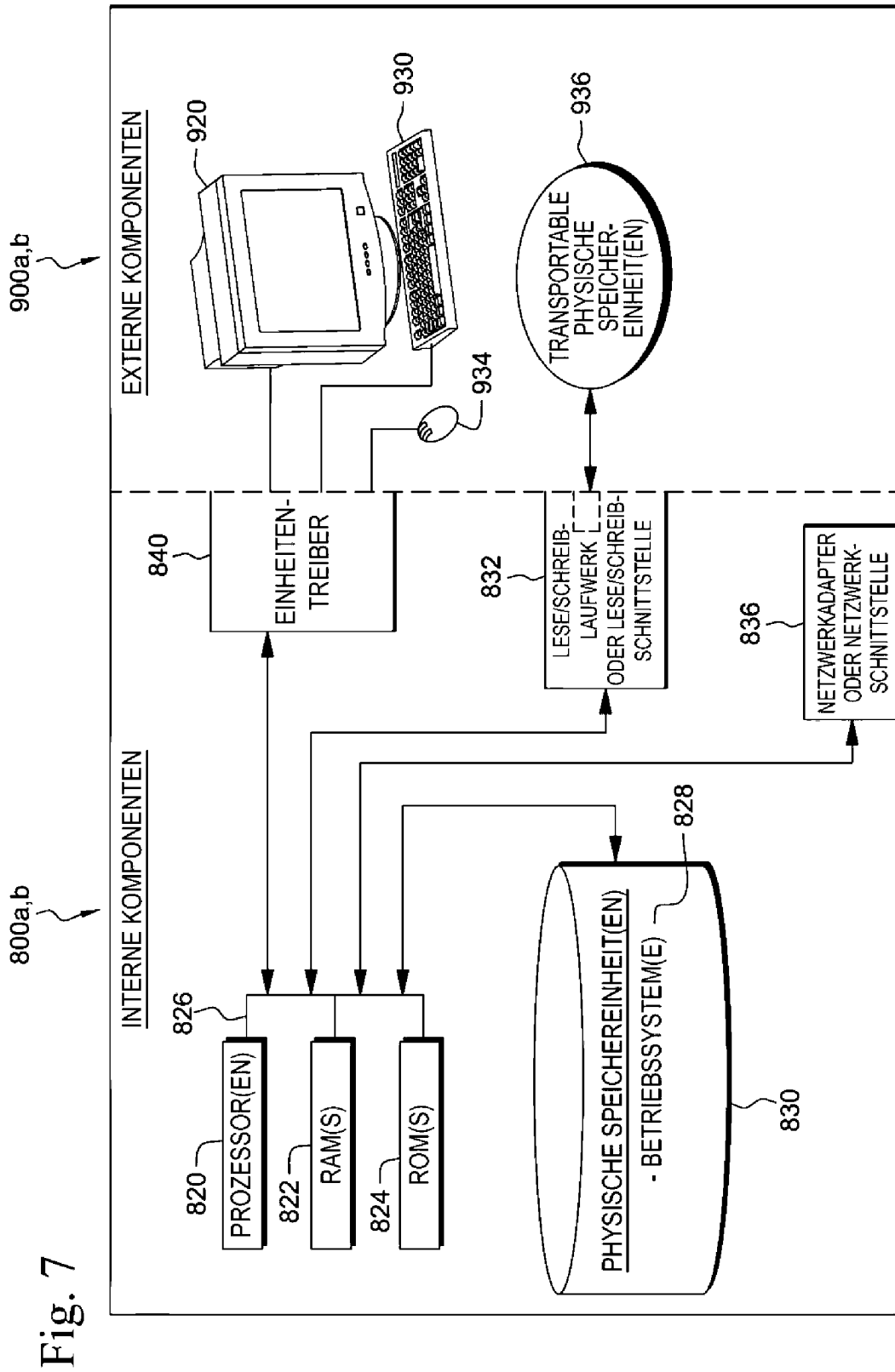


Fig. 7