(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
13. Oktober 2011 (13.10.2011)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2011/124221 A2

(51) Internationale Patentklassifikation: Nicht klassifiziert

(21) Internationales Aktenzeichen: PCT/DE2011/075063

(22) Internationales Anmeldedatum:
3. April 2011 (03.04.2011)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2010 016 324.4 5. April 2010 (05.04.2010) DE

(72) Erfinder; und
(71) Anmelder : FREY, Tim [DE/DE]; Auweg 12, 74855 Haßmersheim (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts (Regel 48 Absatz 2 Buchstabe g)*

(54) Title: SYSTEM, METHOD AND ARRANGEMENTS FOR SECURING RESOURCES

(54) Bezeichnung : SYSTEM, VERFAHREN UND ANORDNUNGEN ZUM ABSICHERN VON RESSOURCEN

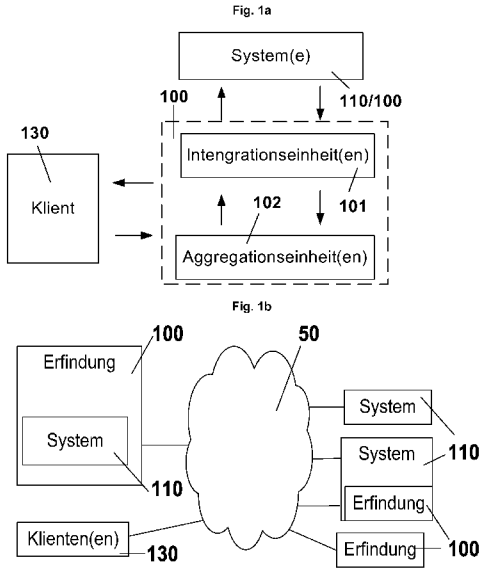


Fig 1.
110 System(s)
130 Client
101 Integration unit(s)
102 Aggregation unit(s)
100 Invention

(57) Abstract: The invention (100) relates to a system, method and/or arrangements for securing access to resources (111), especially access via a computer network (50), the system or an arrangement comprising the following: a. at least one means for integration which allows access to at least one or several means that are used to influence access decisions relating to the access to at least one resource (111); b. at least one means for aggregation which allows aggregated access rights to be calculated, at least one means for access decision being used for calculation.

(57) Zusammenfassung: Die vorliegende Erfindung (100) betrifft ein System, Verfahren und/oder Anordnungen für das Absichern von Zugriffen auf Ressourcen (111), insbesondere für Zugriffe über ein Computernetzwerk (50), wobei das System oder eine Anordnung folgendes Aufweisen: a. Zumindest ein Mittel zur Integration, das es ermöglicht, auf zumindest ein oder mehrere Mittel zuzugreifen, die genutzt werden, um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource (111) zu beeinflussen; b. Zumindest ein Mittel zur Aggregation, das es ermöglicht, aggregierte Zugriffsrechte zu berechnen, wobei bei der Berechnung, zumindest ein Mittel zur Zugriffsentscheidung verwendet wird.

WO 2011/124221 A2

System, Verfahren und Anordnungen zum Absichern von Ressourcen

1. Technisches Gebiet

Die vorliegende Erfindung betrifft Systeme, Verfahren und Anordnungen, die zum Absichern von Ressourcen, insbesondere in hochskalierbaren Szenarien, mit Computernetzwerken verwendet werden können. Dabei wurde die Erfindung, insbesondere unter Betrachtung des Internets und darin vorkommender Plattformen, gemacht.

2. Stand der Technik

Ein Beispiel für ein modernes Sicherheitssystem ist Spring Security. Diese verfügt über Mittel, die es ermöglichen, ein Java Programm über Annotationen abzusichern. Dabei können in Spring Security Zugriffskontrolllisten für einzelne Objekte, die von Klassen erzeugt wurden, hinterlegt werden. Das System verfügt dazu über eine zentrale Zugriffskontrolllistenablage (ACL Ablage), in der die Zugriffskontrolllisten in einer Datenbank abgelegt werden. Diese werden dann beim Zugriff auf Ressourcen genutzt, um den Zugriff auf Erlaubnis zu prüfen. Dabei können die einzelnen Zugriffskontrolllisten auf weitere Zugriffskontrolllisten in der zentralen Ablage verweisen, von denen sie die Inhalte erben. Aufgrund dessen werden dann bei einer Zugriffsüberprüfung die Zugriffskontrolllisten, von denen Rechte geerbt wurden, mit einbezogen. Ein Problem von Spring Security ist dabei, dass es nur eine interne Ablagestelle besitzt und keine weiteren Systeme oder Zugriffslistenarten benutzen kann. Da im Normalfall in einer Systemlandschaft verschiedene Technologien eingesetzt werden, ist somit Spring Security isoliert von den anderen Systemen zu betrachten, da diese nicht zusammen arbeiten. Ein weiteres Problem ist, dass bei Zugriffsentscheidungen, bei denen Zugriffskontrolllisten, die von anderen Zugriffskontrolllisten Rechte erben, auch immer die Zugriffskontrolllisten, von denen Rechte ererbt wurden, geladen und mit ausgewertet werden müssen. Diese und weitere Einschränkungen machen ein solches System unflexibel und schwer skalierbar.

Apache Shiro (http://cwiki.apache.org/confluence/display/SHIRO/Index) ist ein Sicherheitssystem für verschiedene Programmierplattformen, unterstützt aber keine Integration von weiteren Sicherheitssystemen und deren Zugriffskontrolllisten, die zum Beispiel Rechte voneinander erben.

Weitere Sicherheitssysteme sind dabei als ähnlich oder weniger mächtig zu Spring Security zu sehen.

Ein Beispiel einer Sprache für Zugriffskontrolllisten ist XACL. Diese löst aber auch nicht das Problem, heterogene Systeme mit verschiedenen Zugriffskontrolllisten durch ein System zu verwalten zu können.

Dieser Erfindung liegt daher das technische Problem zu Grunde, es zu ermöglichen, Anordnungen, Verfahren und Systeme bereit zu stellen, die es ermöglichen Daten, die zur Zugriffskontrolle genutzt werden können, aus verschiedenen Systemen nutzen, wie auch verteilen zu können. Dabei stellt sich die Herausforderung, dass die verschiedenen Systeme anderen Spezifikationen folgen können und eigentlich nicht kompatibel sind.

Weiterhin sollen zusätzlich zu dieser Funktionalität noch weitere Funktionen durch die Erfindung eine gute Skalierbarkeit ermöglichen. Ferner soll die Erfindung auch in akuten und zukünftigen Anwendungsszenarien, insbesondere im hochdynamischen Internetumfeld eingesetzt werden können.

3. Zusammenfassung der Erfindung

Die vorliegende Erfindung 100 löst die oben beschriebenen Probleme. In einer Ausführungsform nach Patentanspruch 1 weist die Erfindung 100 auf:

a. Zumindest ein Mittel zur Integration, das es ermöglicht, auf zumindest ein oder mehrere Mittel zuzugreifen, die genutzt werden, um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource 111 zu beeinflussen;

b. Zumindest ein Mittel zur Aggregation, das es ermöglicht, aggregierte Zugriffsrechte zu berechnen, wobei bei der Berechnung, zumindest ein Mittel zur Zugriffsentscheidung verwendet wird.

Somit stellt die vorliegende Erfindung 100 ein System, Verfahren und eine Anordnung bereit, die es ermöglicht, verschiedenste Systeme 110, die auch Sicherheitsfunktionen enthalten können oder Verfahren zur Absicherung, miteinander zu integrieren und kombinieren, indem Aggregate von Rechten, über die Systemgrenzen eines Systems 110 hinweg, berechnet werden können. Unter Zugriffsrecht können dabei Erlaubnisse oder Verweigerungen zum Durchführen von Operationen verstanden werden. Beispielsweise können solche Rechte die Erlaubnisse zu lesen, schreiben, ändern, löschen oder auch administrieren sein. Dabei sind aber auch weitere komplexere Erlaubnisse oder Verweigerungen, wie autorisieren, genehmigen, ausführen, z.B. von Services oder Funktionen, ausführen mit Beschränkungen, ausführen mit beschränkter Ergebnismenge, abhängig von der Benutzerrolle und jeder weiteren Funktion denkbar, die in Programmen, insbesondere in betriebswirtschaftlichen, vorkommt.

Die Mittel, die zu Zugriffsentscheidungen genutzt werden 112, können verschiedenste Ressourcen 111 darstellen. Beispielsweise können solche Mittel 112 Zugriffskontrolllisten oder Teile derer sein. Oder auch komplette Sicherheitssysteme, andere Systeme 110 oder einzelne Teile derer. Auch können die verschiedenen Ausführungen der Erfindung 100 oder Teile derer selbst wiederum solche Mittel darstellen, um diese beispielsweise zu skalieren.

Aggregieren bedeutet dabei das Zusammenfassen von Rechten für eine spezielle Ressource 111. Eine Ressource 111 kann dabei zum Beispiel eine Datei oder jede andere Form eines Dokumentes oder einer Datenbasis sein, z.B. auch ein Platzhalter, an dessen Stelle es dem Klienten 130 erlaubt ist, Informationen zu speichern.

Solche Dokumente können zum Beispiel in einer Dokumentenbasis, auch als Datenbasis bezeichnet, in der die Dokumente abgelegt werden, vorkommen. Ein Beispiel für eine Dokumentenbasis ist ein Dateisystem. Jedoch kann eine Dokumentenbasis auch aktiv sein, beispielsweise kann die Datenbasis/Dokumentenbasis ein Webserver sein oder auch mehrere Webserver, wie das Internet. Dabei bezieht sich der Begriff Datenbasis auch auf mehrere Systeme 110 oder auch über Computernetzwerke gekoppelte Systeme. Der Begriff Dokument ist demnach ein Sammelbegriff für alle möglichen Ausgaben einer Datenbasis oder auch eine Zusammenstellung von durch einen Benutzer erzeugte Daten. Ein Dokument kann z.B. dynamisch von einer Datenbasis generiert werden, weshalb eine Datenbasis im Rahmen der vorliegenden Erfindung 100 als Quelle oder Kombination von Quellen oder Quellsystemen 110 anzusehen ist, von welchen Daten angefordert, geschrieben und/oder geändert werden können. Ein Dokument ist demnach eine logische Einheit, eine Partition, Komponente und/oder Unterteilung und trifft daher auch auf Teile von Dokumenten zu. Ausführungsformen der vorliegenden Erfindung 100 können dabei die Strukturinformationen der Datenbasis nutzen, um Zugriffe auf die Datenbasis oder darin vorkommende Dokumente zu verbessern und/oder zu beschleunigen. Als Datenbasis und somit als Dokumente können beispielsweise folgende Daten und zugehörige Systeme 110 oder Systeme 110 allein dienen: Hypertextdokumente, Word Dokumente, E-Mails, Webserver, Programmcode, wie Klassen oder Objekte oder auch andere Konstrukte, die bei der Programmierung oder daraus erzeugtem kompilierten Quelltext vorkommen, API-Aufrufe oder Rückgabewerte, Zugriffe auf Programmteile, Business Objekte,

wie z.B. Belege, oder Stammdaten, Application Server, SAP Systeme, Data Warehouses, Textdokumente, Bilder, Audiodateien, Social Networks, Videos, Blogs, Twitter, Social Networks, mobile Geräte, wie beispielsweise Handys, Peer-to-Peer-Netzwerke, Eingabegeräte, Dateisysteme, Datenbanken, Suchmaschinen, Server, Router, Maschinen, Sensoren, Testsysteme, Debugger, Menschen und/oder Automobile. Sofern die vorliegende Erfindung 100 in einem Computernetzwerk 50 eingesetzt wird, kann dieses Netzwerk und dessen Teilnehmer die Rolle der Datenbasis einnehmen, im Internet z.B. das Internetnetzwerk selbst, Peer-to-Peer-Netzwerke, Webserver, Internetseiten, Klienten, mobile Klienten 130 (z.B. Mobiltelefone, Notebooks, PDAs, etc.) und weitere Akteure. Eine Internetseite kennzeichnet dabei ein Dokument, das über das Internet erreichbar ist, und kann verschiedene Inhalte umfassen, die dort auftreten, wie z.B. für Hypertextdokumente, Videos, Bilder und weitere Dokumente, die Hyperlinks beinhalten können. Der Begriff Internetseite kann auch für mehrere Dokumente stehen, z.B. alle oder ein Teil der Seiten unter einer bestimmten Domain. Somit ist der Begriff Internetseite auch ein Sammelbegriff für das, was allgemein Website oder Webseite genannt wird, d.h. ein Sammelbegriff für einen gesamten Internetauftritt, z.B. ein Auftritt eines Unternehmens, einer Organisation, einer Privatperson, eines Vereins, einer Interessensgruppe oder zu einem bestimmten Zweck, z.B. Verkauf, Handel, Information, Diskussion, Austausch, Vergnügen, Suche, Vermittlung etc. Eine solche Internetseite kann über verschiedene Protokolle übertragen werden, z.B. TCP/IP, HTTP, HTTPS, FTP, POP3, SMTP und andere Protokolle, die zur Kommunikation in Computernetzwerken 50 eingesetzt werden.

Indem Ressourcen 111 Klassen oder auch Objekte aus Programmen sein können, ist es somit möglich, Zugriffsrechte mit diesen zu assoziieren. Rechte können dabei Rollen oder Zugriffsrechte sein, die spezifizieren, welche Operationen mit oder auf der Ressource 111 durchgeführt werden. Dies ist sehr vorteilhaft, da somit Rollen auch mit Objektinstanzen verknüpft werden und vererbt werden können. Somit ist es dadurch möglich, Role Based Access Control auf Objekt und nicht nur auf Klassenebene durchzuführen (Instance Role Based Access Control -IBAC).

Dieses IBAC macht es möglich, Zugriffsentscheidungen auf bestimmte Ressourcen 111 aufgrund von Hierarchien von Rechten oder Rollen, die nur für eine spezielle Ressource 111 oder Ressourcenhierarchie gelten und in dieser mit zumindest einem Klienten 130 verknüpft sind, zu treffen.

Hierbei können die Rechte, die Aufgrund von Aggregationen bestimmt wurden, gespeichert werden. Dadurch ist es möglich, die aggregierten Rechte bei einer Zugriffsentscheidung zu nutzen. Die Aggregatbildung selbst kann über Regeln oder auch über Programme stattfinden. Dabei ist es auch möglich, dass zur weiteren Beschleunigung der Aggregatbildung Warteschlangen mit Nachrichten verwendet werden, um die Parallelverarbeitung noch weiter zu erhöhen.

Dies ist gegenüber dem Stand der Technik ein großer Vorteil, da somit erstmals Beziehungen, wie zum Beispiel Vererbung, von Zugriffskontrolllisten über verschiedene Systeme 110 hinweg möglich sind. Dies wird realisierbar, weil verschiedenste Integrationseinheiten und Mittel zum Zugriff kombiniert werden können. Dabei können durch die Erfindung 100 die ererbten Rechte durch zumindest eine Aggregationseinheit 102 berechnet werden und durch die Integrationseinheit 101 gespeichert werden. So können beispielsweise schon vorhandene Systeme 110 oder Datenbasen, wie z.B. Image Server oder Video Streaming Server genutzt werden, und die einzelnen Ressourcen, wie Bilder, Videos, Verzeichnisse oder andere Dokumente können Rechte aus einem anderen System, wie zum Beispiel der Programmlogik erben.

Besonders vorteilhaft ist beim Bilden der Aggregate auch die Tatsache, dass nicht zwingend nur eine Aggregationseinheit 102 vorhanden ist, sondern es von diesen mehrere geben kann. Dies ermöglicht es, dass eine verteilbare Verarbeitung stattfinden kann und somit eine hohe Skalierbarkeit gewährleistet ist.

Zudem kann die Erfindung 100, wie in Fig. 1b zu sehen, natürlich auch direkt mit einem oder mehreren Systemen 110 zusammen wirken. Beispielsweise kann diese Teil eines Systems 110

oder ein System 110 kann auch ein Teil dieser sein. Dies ermöglicht eine nahtlose Integration mit weiteren Systemen 110. Dadurch könnte die Erfindung 100 selbst wiederum z.B. als Sicherheitssystem dienen, das in Kombination mit weiteren Erfindungen 100 oder Systemen 110 eingesetzt wird. Dies ermöglicht, dass die Erfindung 100 nicht zwingend nur als ein System 110 umgesetzt werden kann. Vielmehr kann sie als eine Vielzahl von Systemen 110, die miteinander z.B. durch die Integrationseinheit 101und Aggregationseinheit 102 kommunizieren, realisiert werden. Dadurch ergibt sich eine besonders vorteilhafte Verteilbarkeit, wie zum Beispiel in einem Computernetzwerk 50 über mehrere Server.

In einem weiteren Aspekt der Erfindung 100 können die Systeme, die Mittel zur Zugriffsentscheidung 112 beinhalten, von der Erfindung 100 über zumindest ein Computernetzwerk, wie zum Beispiel das Internet, angesprochen werden. Dies ermöglicht es, dass die Erfindung 100 besonders bevorzugt in heterogenen verteilten Systemlandschaften eingesetzt werden kann.

Ferner kann die Erfindung über zumindest einen Erbschaftsbaum verfügen. Ein solcher macht es möglich, die Vererbungsstruktur bzw. Vererbungsstrukturen abzubilden. Dies kann zum Beispiel beim Berechnen der Aggregate genutzt werden, um zu bestimmen, welche „Zugriffsentscheidungsmittel 112“ bei der Aggregatbildung berücksichtigt werden müssen. Besonders vorteilhaft ist ein solcher Erbschaftsbaum dabei, dass somit Vererbung auch über verschiedene Systeme 110 hinweg, die selbst keine Vererbung unterstützen, abgebildet werden kann. Beispielsweise kann somit durch Aggregate in fremde nicht erbschaftsfähige Systeme 110 auch eine Erbschaftsfunktion hinzugefügt werden. Ein weiterer Vorteil des Erbschaftbaumes ist die Möglichkeit, dass auch mehrere eingesetzt werden können wie in Fig. 2a gezeigt. Dort ist zu sehen wie verschiedene Systeme 110 - 200, 210, 220 verschiedene Erbschaftsbäume besitzen und von Knoten in einem Erbschaftsbaum auf Knoten in weiteren verwiesen wird. Dies ermöglicht es besonders die Aggregation in Kombination mit Erbschaftsbäumen zu skalieren. Ein weiterer Vorteil von solchen Bäumen ist, dass die in den Bäumen vorhandene Information bei der Berechnung von Aggregaten verwendet werden kann. Beispielsweise um Abhängigkeiten zu erkennen und Ablaufpläne für die Aggregatbildung zu erzeugen.

In einer weiteren Ausführung können in Programmen Mittel definiert werden, die bei der Zugriffsentscheidung berücksichtigt werden. Solche Mittel können zum Beispiel Annotationen oder auch Aspekte sein. Somit können beispielsweise Ausdrücke angegeben werden, welche Rollen oder Erlaubnisse welche Zugriffe auf zumindest eine Ressource 111 haben. Beispielsweise können somit Methoden einer Klasse oder die Klasse selbst über Annotationen zugriffsbeschränkt werden. Durch die Fähigkeit Aggregate zu bilden ist es zudem möglich, „virtuelle Ressourcen“ im Programmquelltext zu definieren. Beispielsweise Bilder, die auf einem Image Server zu finden sind. Dabei können solche Bilder als „normale Objekte im Objektorientierten Sinne“ im Programmquelltext vorkommen. Das physische Bild auf dem Image Server erbt die Rechte vom virtuellen Objekt. Dadurch ist es möglich, dass bei der Aggregatbildung die Rechte im Image Server somit vom „virtuellen Objekt“ geerbt werden. Bei einer solchen Aggregatbildung ist es zudem möglich, zudem weitere Mittel, die im Programmquelltext definiert wurden, wie beispielsweise Inhalte von Annotationen oder Aspekten zu berücksichtigen.

Eine, besonders bevorzugt im dynamischen Internetumfeld, wie Web.2.0, eingesetzte Variante der Erfindung 100, besitzt die Fähigkeit, dass dynamisch Integrationsmittel eingebunden oder entfernt werden können. Dies ermöglicht eine besonders flexible Anpassung ohne die Notwendigkeit die Erfindung 100 selbst anpassen zu müssen, sofern ein neues System 110 eingebunden werden soll, da somit erst zur Laufzeit die benötigten Integrationsmittel geladen werden können.

Ferner kann die Erfindung 100 über Mittel verfügen, dass Aktualisierungen von „Mitteln zur Zugriffskontrolle“ erkannt werden. Dies kann dazu genutzt werden, dass beispielsweise ein Prozess zur Aggregatbildung für Objekte, die vom betroffenen Objekt erben, durchgeführt oder aktualisiert wird. Diese Fähigkeit ermöglicht es somit besonders dynamisch und flexibel Mittel zur Zugriffs-

entscheidung 112 zu aktualisieren, da somit auch Aktualisierungen in fremden Systemen 110 erkannt werden können.

Eine weitere Fähigkeit, die sich durch die Fähigkeiten der Erfindung 100 ergibt ist die Möglichkeit, dass auf Ressourcen 111 nicht über ein zentrales Sicherheitssystem zugegriffen werden muss, wie dies heutzutage zum Beispiel bei Spring Security der Fall ist. Vielmehr kann ein Klient 130 direkt auf Ressourcen 111 zugreifen, die in einem System 110 vorhanden sind, das die Mittel zur Zugriffsentscheidung 112 auswerten kann, wie es zum Beispiel in Fig. 1e-g gezeigt wird. Dabei können die Mittel zur Zugriffsentscheidung 112 zum Beispiel durch die Erfindung 100 aktualisiert werden. Dieser direkte Zugriff erspart einen Umweg der Datenpakete aus den eigentlichen Systemen 110 über die Erfindung 100 oder ein anderes Sicherheitssystem.

Eine bevorzugte Variante der Erfindung 100 kann zudem über kryptographische Mittel verfügen oder diese nutzen. Diese können zum Beispiel dazu genutzt werden, um dem Klienten 130 ein Geheimnis mitzuteilen, das dazu dient, verschiedene Zugriffe auf zumindest eine Ressource 111 auszuführen. Dabei könnte ein solcher Zugriff auch zeitlich begrenzt werden. Dies kann dazu genutzt werden, somit auch weitere Fremdsysteme 110 einzusetzen. Beispielsweise könnte sich der Klient 130 somit über OpenID bei der Erfindung 100 authentifizieren und von der Erfindung 100 ein Geheimnis, mit dem er auf die benötigten Ressourcen 111 zugreifen kann, erhalten.

Somit könnte beispielsweise eine Anwendung erstellt werden, die zumindest eine bestehende Sicherheitsinfrastruktur, wie z.B. die der Amazon Webservices ACL Infrastruktur (http://aws.amazon.com/) ,der Google App Engine Infrastruktur(http://code.google.com/intl/de-DE/appengine/) oder ähnliches, nutzt. Durch diese oder eine Ähnliche könnte zumindest ein direkter Ressourcenzugriff durch den Klienten 130 ermöglicht werden, indem z.B. die kryptographischen Mittel der Plattform dazu verwendet werden, zumindest einem Klienten 130 ein Geheimnis mitzuteilen, durch das direkt auf zumindest eine Ressource 111 zugegriffen werden kann. Dabei könnte auch die Wirksamkeit des Geheimnisses temporär beschränkt oder/und an verschiedene Zugriffsoperationen gekoppelt werden.

Des Weiteren könnte durch die Erfindung 100 eine Vererbungsstruktur für die Ressourcen 111 und/oder die zugehörigen Mittel, die zur Zugriffskontrolle, wie ACLs heutzutage bei Amazon, realisiert werden. Dies würde es dann im Zusammenspiel mit Aggregaten ermöglichen, die Plattform um eine Vererbungsmöglichkeit durch die Erfindung 100 zu erweitern. Um dies weiter zu verbessern, könnten einzelne Teile oder die komplette Erfindung 100 somit auch als Teil einer solchen Plattform realisiert werden, und andere Teile könnten beispielsweise als API oder auch als Bibliothek oder eine Kombination aus API und Bibliothek Entwicklern oder Benutzern der Plattform zur Verfügung gestellt werden. Dies würde es ermöglichen, dass Programme, die für eine solche Plattform entwickelt werden, schon ein fertiges hochskalierbares Sicherheitssystem, das es ermöglicht, Vererbung durchzuführen, benutzen könnten.

In einem solchen Szenario, in dem die Erfindung 100 in einer solchen oder ähnlichen Cloud Computing Infrastruktur eingesetzt wird, ist es zudem möglich, dass zur Verbesserung weitere Services, die eine solche Plattform anbietet, genutzt werden können. Beispielsweise könnte die Aggregation massiv durch viele Instanzen parallelisiert werden.

Ferner können Informationen über den Klienten, sogenannte Klienteninformationen, bei der Zugriffsentscheidung genutzt werden. Klienteninformationen oder auch als Benutzerinformationen bezeichenbar sind dabei Informationen, die auf einen oder mehrere Benutzer/Klienten 130 oder auch auf eines oder mehrere Geräte, Anordnungen oder Verfahren bezogen sind. Klienteninformationen sind hierbei z.B. Daten über oder von Benutzern oder Apparaten, Anordnungen und Verfahren selbst. Dies können beispielsweise passive Daten, die zum Beispiel im Profil des Benutzers stehen, wie z. B. Heimatort, Gruppenmitgliedschaften, Freunde oder auch Daten, die zum Beispiel durch Analysen aufgedeckt wurden, sein. Andere Arten von Benutzerda-

ten können aktive Daten sein. Aktiv kann bedeuten, dass diese Daten erst zur Laufzeit existieren und sich besonders häufig ändern. Beispielsweise die aktuellen Koordinaten des Benutzers, wie z.B. GPS Koordinaten oder Zugangspunkt, dessen IP, Statusmeldung, Verbindungsgeschwindigkeit, Clienttyp. Aufgrund der Eigenschaften von Klienteninformationen ist oftmals weitere Information aus einer solchen Information ableitbar. Zum Beispiel im Standortumkreis aufgrund des Zugangspunktes, der GPS Koordinaten oder/und einer IP-Adresse. Solche ableitbare Information wird wiederum selbst auch als Klienteninformation bezeichnet.

Beispielsweise kann somit ein Klient 130 aufgrund seiner derzeitigen Position andere Geheimnisse mitgeteilt bekommen, wie wenn er sich an einer anderen Position befindet. Des Weiteren können somit die Klienteninformationen, auch zusammen mit weiteren Klienteninformationen oder anderen Daten zusammen, beachtet werden. Diese Fähigkeit, Klienteninformationen bei der Zugriffsentscheidung zu beachten, macht somit vielfältige neuartige Anwendungsfälle für Absicherungen möglich, und es können somit neuartige Zugriffsentscheidungen getroffen werden. Beispielsweise ist es somit möglich, den Zugriff von Klienten 130 auf Informationen von anderen Klienten 130, die sich in deren Nähe aufhalten zu beschränken.

Eine weitere Variante der Erfindung 100 unterstützt eine oder mehrere Rollen oder eine oder mehrere Hierarchien von Zugriffsrechten. Solche können zum Beispiel ausdrücken, welche Rechte oder Rollen andere Rechte oder Rollen beinhalten. Somit können zum Beispiel auch Rollen und Rechte einfacher vergeben und konfiguriert werden, da es nicht mehr nötig ist, alle Rechte und Rollen zu spezifizieren. Besonders vorteilhaft ist diese Variante im Zusammenspiel mit dem Assoziieren von Rechten auf bestimmte Ressourcen 111. Hierbei ist es Zugriffsentscheidungen auf bestimmte Ressourcen 111 aufgrund von Hierarchien und Rechten oder Rollen, die nur für eine spezielle Ressource 111 oder Ressourcenhierarchie, mit einem Klienten 130 verknüpft sind zu treffen. Dies unterscheidet die Beispielsweise stark von Spring Security wo solche Hierarchien nicht direkt für Ressourcen 111 definierbar sind.

Die vorliegende Erfindung 100 betrifft ferner ein Verfahren zum Absichern von Ressourcen, wobei das Verfahren die folgenden Schritte aufweist: a. Zugriff auf ein oder mehrere Mittel, die genutzt werden, um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource 111 zu beeinflussen; und b. Berechnung zumindest eines Aggregates, wobei bei der Berechnung zumindest ein Mittel zur Zugriffsentscheidung verwendet wird. Weitere vorteilhafte Ausführungsformen des erfindungsgemäßen Verfahrens finden sich in den weiteren abhängigen Ansprüchen.

Zuletzt stellt die vorliegende Erfindung 100 ein Computerprogramm bereit, das Instruktionen aufweist, um jedes hierin beschriebene Verfahren auszuführen.

4. Kurze Beschreibung der Zeichnungen

Fig. 1a-e: Anordnungen, Systeme und Interaktionen nach Ausführungsformen der vorliegenden Erfindung;

Fig. 2a-c: Erbschaftsmöglichkeiten nach Ausführungsformen der vorliegenden Erfindung;

Fig. 3a-d: Verfahren und Visualisierungen zur Aggregatbildung nach Ausführungsformen der vorliegenden Erfindung;

Fig. 4: Eine Integrationseinheit und Anordnung nach einer Ausführungsform der vorliegenden Erfindung;

Fig. 5: Verfahren und exemplarische Darstellung der Transformation zwischen verschiedenen Mitteln, die zur Zugriffsentscheidung genutzt werden, nach einer Ausführungsform der vorliegenden Erfindung;

5. Detaillierte Beschreibung von bevorzugten Ausführungsformen

Sicherheitssysteme/System Bestandteile:
Grundlegend ist es bei Systemen 110 so, dass Mittel zur Zugriffsentscheidung 112 die Entscheidung über die Erlaubnis oder auch die teilweise Erlaubnis eines Zugriffs treffen und diesen somit Autorisieren. Diese könnten auch Mittel Zugriffskontrolle genannt werden. Dabei werden Mittel genutzt oder/und auch ausgewertet, die von den Mitteln zur Zugriffsentscheidung 112 zu den Fällen der Entscheidung in Betracht gezogen werden. Zur Vereinfachung werden in diesem Dokument diese zwei Arten von Mitteln, als Zugriffsentscheider 114 und Entscheidermittel 113, bezeichnet. Wobei Entscheidermittel 113, wie auch Zugriffsentscheider 114, jeweils auch für eine Mehrzahl von Zugriffsentscheidern 114, wie auch von Entscheidermitteln 113 stehen können. Dabei ist der Zugriffsentscheider 114 das Mittel, das zumindest eine Zugriffsentscheidung fällt. Dieser kann auch als „Mittel zur Zugriffsentscheidung 112" bezeichnet werden. Die Entscheidermittel 113 sind die Mittel, aufgrund derer die Entscheidung getroffen wird, wie zum Beispiel Ressourcen, wie Dokumente. Diese können auch als „Mittel", die zu Zugriffsentscheidungen genutzt werden" bezeichnet werden. Zugriffsentscheidungen können dabei auch eine Mehrzahl von Zugriffsentscheidungen bedeuten, zum Beispiel, indem mehrere kleinere Zugriffsentscheidungen zu einer großen Zugriffsentscheidung führen können. Da oftmals die Grenze zwischen diesen verschiedenen Mitteln nicht deutlich gezogen werden kann und in Sicherheitssystemen 110 eine Vermischung zwischen Entscheidermitteln 113, Zugriffsentscheider 114 und Zugriffsentscheidungen besteht, können diese generalisiert als Mittel zur Zugriffsentscheidung 112 bezeichnet und sämtliches Vorkommen der zuvor erwähnten Begriffe in diesem Dokument könnte durch „Mittel zur Zugriffsentscheidung 112" ersetzt werden. Der Grund, warum jedoch trotzdem die Worte Entscheidermittel 113, Zugriffsentscheidung und Zugriffsentscheider 114 teilweise genutzt werden ist dabei, dass diese Unterteilung eine einfachere Verständlichkeit der Erfindung 100 fördert. Deshalb werden im weiteren Verlauf, wenn es die Verständlichkeit fördert, die Begriffe Zugriffsentscheider 114 und Entscheidermittel 113 anstatt Mittel zur Zugriffsentscheidung 112 verwendet.

Fig. 1a
Fig.1a zeigt eine Ausführungsform der vorliegenden Erfindung 100. Dabei ist zu sehen, dass die Erfindung 100 über Mittel verfügt, wie zum Beispiel eine oder mehrere Integrationseinheiten 101, die es ermöglichten, dass die Erfindung 100 zusammen mit weiteren Sicherheitssystemen 110 oder Erfindungen 100 eingesetzt wird. Zusätzlich ist zu sehen, dass die Erfindung 100 auch über eines oder mehrere Mittel, die zum Bilden von zumindest einem Aggregat, auch im Zusammenspiel mit weiteren Bestandteilen der Erfindung, genutzt werden können, wie z.B. eine Aggregationseinheit 102, verfügen kann. Eine oder mehrere solcher Mittel zur Aggregation, wie zum Beispiel Aggregationseinheiten 102, können mit Mitteln zur Integration, wie zum Beispiel zumindest einer Integrationseinheit 101 zusammen wirken. Dieses Zusammenwirken kann zum Beispiel beim Erzeugen von Aggregaten von Entscheidermitteln 113 stattfinden. Beispielsweise können durch Integrationseinheiten 101 Aggregationseinheiten 102 Informationen über Aktualisierungen mitgeteilt werden oder Aggregationseinheiten 102 können Integrationseinheiten 101 nutzen, um auf Entscheidermittel 113 zuzugreifen. Ein solcher Zugriff kann zum Beispiel das Lesen, Schreiben, Aktualisieren oder auch die Analyse von Mitteln, die zur Zugriffskontrolle verwendet werden, sein.

In der Fig. 1a ist ferner zu sehen, dass ein oder mehrere Klienten 130 direkt auf die einzelnen Teile der Erfindung 100 zugreifen können, und somit sämtliche Funktionen, die durch diese Erfindung 100 offenbart wurden, direkt durch einen Klienten 130 nutzbar sind.

Klienten:
Klienten 130 sind dabei z.B. Menschen oder Menschengruppen, die technische Geräte nutzen, um mit Maschinen, Verfahren, anderen Klienten, Anordnungen oder auch über Computernetzwerken zu kommunizieren. Klienten 130 müssen nicht zwangsläufig Menschen sein. Vielmehr können Klienten 130 zum Beispiel Maschinen, Apparate und Verfahren, also auch Benutzergruppen sein.

Oftmals sind mit Klienten 130 auch Informationen, auch mit den technischen Geräten, die sie nutzen, assoziierbar. Weil ein Klient 130 einen Benutzer oder Benutzergruppen darstellen kann, der oder die zumindest ein technisches Gerät nutzen oder die Klienten 130 selbst eine oder mehrere Maschinen sind, wird daher im weiteren Verlauf nicht zwischen Benutzer (Menschen) und Klient unterschieden und das Wort Klient 130 auch zusätzlich als Äquivalent für Benutzer gebraucht und umgekehrt.

Aggregate:
Aggregate sind dabei Entscheidermittel 113, die aus bereits vorhandenen Entscheidermitteln 113 oder auch Ressourcen, wie z.B. weiteren Dokumenten berechnet wurden. Zum Beispiel können Aggregate von Mitteln zur Zugriffsentscheidung als die Summe von erlaubten Rechten für Klienten 130 abzüglich der Verweigerungen für Klienten 130 gesehen werden. Dabei können als weitere Ressourcen 111 z.B. Rahmenbedingungen, wie zum Beispiel hierarchische Berechtigungen oder auch hierarchische Rollen oder weitere Mittel, die zur Zugriffsentscheidung bei deren Erzeugung oder Aktualisierung beachtet werden. Dabei können z.B. sämtliche, in diesem Dokument besprochene, Merkmale die bei der Aggregatbildung oder Schritte dieser darstellen, berücksichtigt werden, dazu dienen, Aggregate von „normalen" Entscheidermitteln 113 abzugrenzen. Zum Beispiel kann ein Aggregat gegebenenfalls für zumindest ein Zielsystem in ein passendes Format transformiert sein, wobei beim Erzeugen des Aggregates und der gegebenenfalls anfallenden Transformation in passendes Format für das Zielsystem auch weitere Rahmenbedingen, wie zum Beispiel Regeln, Computerprogramme, Systeme 110 oder Informationen über Klienten 130 in verschiedenen Systemen 110, verwendet werden können. Besonders bevorzugt können solche Aggregate Optimierungen für verschiedenste Anwendungsfälle im Vergleich zu den Entscheidermitteln 113 oder Ressourcen, aus denen sie erzeugt wurden, beinhalten. Im Gegensatz zu einem normalen Mittel, das zu Zugriffsentscheidungen genutzt wird, kann ein Aggregat auch zusätzlich oder alternativ durch weitere Merkmale gekennzeichnet sein. Zum Beispiel kann damit eine schnellere Zugriffsentscheidung bei zumindest einem Zugriff, im Gegensatz zu zumindest einer Zugriffsentscheidung aufgrund zumindest eines zuvor vorhandenen Entscheidermittels 113, das zur Erzeugung des Aggregates berücksichtigt wurde, möglich sein. Oder/und es werden weniger oder keine Ressourcen 111 von zumindest einem Zugriffsentscheider 114, im Gegensatz zu zumindest einer Zugriffsentscheidung, aufgrund zumindest eines zuvor vorhandenen Entscheidermittels 113, das zur Erzeugung des Aggregates berücksichtigt wurde, benötigt. Wobei solche Ressourcen, beispielsweise Speicher oder Prozessorlast sein können, aber auch Dokumente oder Regeln, die bei der Zugriffsentscheidung zur Entscheidung der Zugriffsfrage genutzt werden. Oder/und es ist kein Auswerten von weniger Regeln oder Computerprogrammen, im Gegensatz zu zumindest einer Zugriffsentscheidung, aufgrund zumindest eines zuvor vorhandenen Entscheidermittels 113, das zur Erzeugung des Aggregates berücksichtigt wurde, möglich. Des weiteren können Aggregate auch, z.B. zumindest eine optimierte Form dahingehend welche Zugriffe besonders oft durchgeführt werden, beispielsweise bei der Nutzung von Klientinformationen, im Vergleich mit zumindest einer Zugriffsentscheidung, aufgrund zumindest eines zuvor vorhandenen Entscheidermittels 113, das zur Erzeugung des Aggregates berücksichtigt wurde, darstellen. Eine weitere Möglichkeit ist, dass Aggregate es ermöglichen, an oder in Ressourcen, wie zum Beispiel Webservern, Zugriffsentscheidungen zu treffen, an denen diese bisher nicht möglich waren. In Kombination oder auch als Alternative können Aggregate auch Transformationen und somit zum Beispiel eine Repräsentation von Entscheidermitteln 113, die sich zumindest in einem Ausdruck von zumindest einem zuvor vorhandenen Entscheidermittel 113, das zur Erzeugung des Aggregates berücksichtigt wurde, unterschieden. Ein solcher Ausdruck kann zum Beispiel sein, dass anstatt eines Benutzernamens eine BenutzerID im Aggregat angegeben ist.

Sicherheitssysteme/Systeme
Als die zuvor beschriebenen Sicherheitssysteme 110 oder auch oftmals Systeme 110 genannt, sind hierbei alle Apparate, Verfahren und Anordnungen zu verstehen die irgendwelche Mittel nutzen,

um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource 111 zu fällen oder selbst das Mittel oder einen Teil des Mittels darstellen, das bei einem Zugriff ausgewertet wird. Weil oftmals viele Systeme 110 Zugriffskontrolllisten bei Zugriffen auswerten können diese auch als Sicherheitssysteme 110 im Sinne der Erfindung 100 gesehen werden. Somit ist als Sicherheitssystem jedes System 110 zu sehen, das Sicherheitsfunktionen unterstützt. Dabei sind somit beispielsweise auch Programme, die Sicherheitsfunktionen oder auch die Erfindung 100 selbst als Sicherheitssystem zu sehen. Die Bezeichnung Sicherheitssystem ist somit vielmehr als logische Bezeichnung für zugriffskontrollfähige Systeme 110 oder Einheiten, die für die Sicherheit zuständig sind, wie zum Beispiel Zugriffskontrolllisten zu verstehen. Beispielswiese Webserver, wie Apache oder IIS, Windows Server, ERP- Systeme , Business Intelligence Systeme und viele andere.

Es ist nicht zwingend vorgegeben, so dass rein die Integrationseinheiten auf die Sicherheitssysteme 110 zugreifen können. Beispielsweise ist es denkbar, dass auch die Aggregationseinheiten selbst auf die Sicherheitssysteme 110 zugreifen können. Der Grund dafür ist, dass beispielsweise durch die Integrationseinheiten 101 Aktualisierungen aufgedeckt werden könnten und aufgrund deshalb Aggregationsverfahren in Aggregationseinheiten 102 begonnen werden, und diese keinen direkten Zugriff auf die Integratoren besitzen und direkt die Resultate der Aggregationsverfahren schreiben.

Eine weitere Fähigkeit über die die Erfindung 100 verfügen kann sind Mittel zur Zugriffsentscheidung 112. Also Zugriffsentscheider 114 und Entscheidungsmittel. Diese können alle in dieser Erfindung 100 beschriebenen Entscheidungsmittel auswerten und über Zugriffe entscheiden. Beispielsweise könnten solche Mittel nach dem Vorbild von Spring Security oder Apache Shiro erstellt, oder dortige bereits bestehende Mittel könnten dahingehend modifiziert werden um die erweiterten neuartigen Funktionen dieser Erfindung 100 mit derzeit existierenden zu kombinieren. Eine weitere Möglichkeit ist es, dieses andere bereits bestehende Sicherheitssystem dahingehend weiterzuentwickeln, dass sie die Funktionen dieser Erfindung 100 in einem oder mehreren Apparaten, Verfahren oder Anordnungen unterstützen. Somit ist diese Erfindung, wie auch die Weiterentwicklung für jedes Sicherheitssystem zu sehen und kann dabei über, für besonders solche Fälle spezialisierte, Mittel verfügen, um eine optimale Integration zu erreichen.

Es gilt aber zu beachten, dass diese Erfindung 100 sich nicht nur für die Java Plattform oder die Java Enterprise Plattform umsetzen lässt. Vielmehr kann die Erfindung 100 auf den verschiedensten Plattformen realisiert werden. Beispielsweise auf der Dotnet Plattform oder auch in C++. Auch ist es denkbar, dass die Erfindung 100 als eine Kombination von verschiedenen Technologien umgesetzt wird.

Beispiele, Mittel zur Zugriffsentscheidung 112:
Die Mittel die von Sicherheitssystemen 110 oder der Erfindung 100 selbst genutzt werden, um Zugriffsentscheidungen zu treffen, können dabei vielfältig sein. Solche Mittel können zum Beispiel Zugriffskontrolllisten (engl. ACL, Access Control List), die heutzutage besonders häufig, wie zum Beispiel von Security oder auch einem Apache Webserver eingesetzt werden, sein. Aber auch Programme oder Tabellen in Datenbanken oder Internetseiten oder sämtliche Dokumente können solche Mittel sein. Ein weiteres Beispiel für solche Mittel können auch Annotationen sein oder Sicherheitsaspekte der Aspekt orientierten Programmierung. Somit können beispielsweise im Programmquelltext Ausdrücke angegeben werden, welche Rollen oder Erlaubnisse, welche Zugriffe auf zumindest eine Ressource 111 haben. Es können auch, z.B. durch solche Ausdrücke, direkt oder indirekt durch Systemlogik weitere Mittel, wie zum Beispiel Zugriffskontrolllisten spezifiziert werden, die bei der Zugriffsentscheidung genutzt werden. Ein weiteres Beispiel für solche Mittel zur Zugriffsentscheidung 112 können Klientinformationen sein.

Klientinformationen:
Aufgrund der vielfältigen Möglichkeiten, was oder wer ein Klient 130 sein kann, sind auch

Klienteninformationen als Informationen über Benutzer zu verstehen, wie auch die Information über technische Geräte. Klienteninformationen sind dabei Informationen, die auf einen oder mehrere Benutzer oder auch auf einen oder mehrere Klienten 130, Geräte oder Verfahren bezogen sind. Klienteninformationen sind also hierbei Daten über oder von Benutzern oder Apparaten und Verfahren selbst. Dies können beispielsweise passive Daten, die zum Beispiel im Profil des Benutzers stehen, wie z. B. Heimatort, Gruppenmitgliedschaften, Freunde oder auch Daten, die zum Beispiel durch Analysen aufgedeckt wurden, sein. Andere Arten von Benutzerdaten können aktive Daten sein. Aktiv kann bedeuten, dass diese Daten erst zur Laufzeit existieren und sich besonders häufig ändern. Beispielsweise die aktuellen Koordinaten des Benutzers, dessen IP, Statusmeldung, Verbindungsgeschwindigkeit, Clienttyp. Aufgrund der Eigenschaften von bisher gezeigter Klienteninformation ist oftmals weitere Information aus einer solchen Information ableitbar. Zum Beispiel im Standortumkreis aufgrund einer IP-Adresse. Solche ableitbare Information wird wiederum selbst auch als Klienteninformation bezeichnet.

Dabei kann z.B. auch eine Kombination der verschiedenen Möglichkeiten der Mittel zur Zugriffsentscheidung 112 zu zumindest einer Zugriffsentscheidung verwendet werden. Beispielsweise eine Kombination aus Zugriffskontrolllisten und Annotationen und Aspekten, wie bei Spring Security. Diese Erfindung 100 ermöglicht es nun, diesen Umstand bei der Aggregatbildung bzw. Aggregation zu beachten.

Somit ist es möglich, dass Informationen über Klienten, wie zum Beispiel dessen Standort in der Form von GPS Daten oder auch andere weiteren Daten aus dessen Profil, bei der Zugriffsentscheidung genutzt werden. Dies ermöglicht es z.B., dass die Erfindung 100 somit auch „Location based Access Control" unterstützen kann. Dabei können diese Daten mit weiteren Mitteln zur Zugriffsentscheidung kombiniert werden. Besonders vorteilhat hierbei ist, dass die Klienteninformationen als Mittel zur Zugriffsentscheidung 112 hierbei selbst in Aggregate einfließen können oder zusammen mit Aggregaten ausgewertet werden können. Für solche Szenarien kann die Erfindung 100 über weitere besonders hierfür spezialisierte Mittel verfügen. Beispielsweise können Aggregate dahingehend optimiert und gebildet werden, dass Zugriffsentscheidungen durch diese, besonders im Bezug auf Performanz, bei der Einbeziehung von Klienteninformationen, zum Beispiel zu den Aggregaten selbst, bei der eigentlichen Zugriffsentscheidung, getroffen werden können.

Zugriffskontrolllisten können des Weiteren mit den verschiedensten Ressourcen 111 assoziiert werden. Beispielsweise mit Klassen, Objekten und jeder Art von Dokumenten. Dadurch können die Rechte auf Ebene der verschiedensten Ressourcen 111 zugeordnet werden. Beispielsweise ist es damit möglich Rollen, Objektinstanzen bei einem Programm in einer objektorientierten Programmiersprache, wie z.B. Java oder Visual Basic, zuzuweisen.

Ressourcen 111 oder Zugriffskontrolllisten können zusätzlich in einer bevorzugten Ausführung Beziehungen zueinander haben, wie zum Beispiel Erbschaft. Eine solche Erbschaft kann zum Beispiel bedeuten, dass die Rechte einer Zugriffskontrollliste die Rechte einer oder mehrerer anderer Zugriffskontrolllisten oder anderer Mittel einschließt. Beispielsweise kann ein Bild eines Verzeichnisses Rechte erben. Auch ist es denkbar, dass Hierarchien von Business Objekten, wie zum Beispiel Stammdaten oder Stammdatengruppen oder Belege oder/und andere Objekte in betriebswirtschaftlichen Systemen, wie z.B. in Erp Systemen oder Data Warehouses vorkommen und dadurch Rechte vererbt werden.

Diese Beziehungen können zum Beispiel über die Angabe des Elternobjektes, zum Beispiel über deren Typ oder/und Identität definiert werden. Zum Beispiel über Klasse und ObjektID der Elternobjekte oder über die Identität der Eltern Entscheidermittel 113. Dies kann zum Beispiel in den Ressourcen 111 selbst oder auch in Entscheidermitteln 113 geschehen. Auch eine Kombination der Möglichkeit könnte in einer Variante der Erfindung 100 unterstützt werden. Aufgrund dessen, dass Entscheidermittel 113 mit Ressourcen 111 verknüpft sind, wird in dieser Offenbarung oftmals nur

von der Erbschaft der Ressourcen 111 geschrieben, was jedoch auch immer die Erbschaft von Entscheidermitteln 113 einschließt und umgekehrt.

Man beachte hierbei, dass diese Erbschafts- und andere Beziehungen auch zwischen Objektinstanzen bei der Programmierung sein können und nicht nur zwischen Klassen selbst oder Klassen und Objektinstanzen. Vielmehr ist es möglich, das jede Ressource 111 von jeder anderen Ressource 111 Rechte erbt, was die Erfindung 100 sehr flexibel und anpassungsfähig sein lässt.

Eine besonders bevorzugte Variante von Zugriffskontrolllisten unterstützt es, Verweigerungen und Erlaubnisse für Benutzer oder Benutzergruppen auf Daten und Funktionen zu definieren. Dabei können beispielsweise durch Verweigerungen Benutzer aus Gruppen ausgeschlossen werden.

Ferner können solche Zugriffskontrolllisten Regeln oder Programme enthalten, oder auf Regeln oder Programme verweisen, wie deren Auswertung bei zumindest einer Zugriffsentscheidung genutzt wird. Dabei können solche Regeln oder Programme auch weitere Ressourcen 111 mit einbeziehen, die bei der Zugriffsentscheidung beachtet werden sollen. Die Erfindung 100 kann dabei über zusätzlich spezialisierte Mittel verfügen, die es ermöglichen, Aggregate für Regeln oder Programme zu berechnen. Dies kann z.B. dazu genutzt werden, die Auswertungsgeschwindigkeit für Zugriffskontrolllisten zu erhöhen, oder Systemen, die selbst nicht die Möglichkeit unterstützen, Regeln in Kombination mit Zugriffskontrolllisten zu nutzen, das Zusammenspiel mit anderen Systemen 110 oder mit Regeln oder Programmen zu ermöglichen.

Zugriffskontrolllisten können des Weiteren auch nur Regeln oder Programme sein, wie eine andere Ressource 111 als Zugriffskontrolliste zu nutzen oder zu transformieren ist.

Dadurch ist es möglich, dass zum Beispiel Freundeslisten in Social Networks zur Auswertung einer Erlaubnis eines Zugriffs genutzt werden können. Im Gegensatz zu heute eingesetzten manuellen Abfragen, die solche Fälle abprüfen, ist es somit möglich, diese Fälle über ein Sicherheitssystem abzuhandeln und somit sozusagen „virtuelle“ Zugriffskontrolllisten nutzen. Dies ermöglicht es, die Sicherheitsfunktion für solche Fälle aus dem eigentlichen Quelltext zu entfernen und dadurch übersichtlicheren Quelltext schreiben, bzw. erzeugen zu können. Dadurch sind zusätzlich weitere Probleme, die sich aus der Limitation zuvor ergaben, gelöst. Beispielsweise kann somit von einer „Freundesliste als Zugriffskontrollliste“ in anderen Zugriffskontrolllisten problemlos geerbt werden.

Beispiele für solche Regeln können auch Überprüfungen sein, welche Rechte ein Benutzer bei einem Zugriff verändern darf. Oder es können komplexe Überprüfungen vorgenommen werden, welche verschiedenen Rechte ein Benutzer besitzen muss. Auch können solche Regeln oder Programme dazu dienen, weitere Informationen wie die reinen Zugriffskontrolllisten bei der Zugriffsprüfung zu beachten.

Oftmals besitzen Zugriffskontrolllisten auch verschiedene Formate. Beispielsweise werden in einer Zugriffskontrollliste die Rechte für einen Klienten 130 aufgrund einer Bitmaske definiert. An anderer Stelle werden nur reine Listen definiert. Oder, anstatt den Klienten 130 oder die Gruppe direkt in der Zugriffskontrollliste zu definieren, wird eine Stellvertreteridentifikation hinterlegt. Andere erlauben es LDAP oder OpenID Verweise zu hinterlegen. Aus diesem Grund kann die Erfindung 100 für solche oder ähnliche Fälle über hierfür spezialisierte Mittel verfügen, um mit den verschiedensten Zugriffskontrolllisten arbeiten zu können. Dabei können auch weitere Apparate oder Verfahren eingesetzt werden, die dann Teil der Erfindung 100 sind. Beispielsweise um auf OpenID Provider zugreifen oder auch um die Zugriffskontrolllisten aus den verschiedenen Formaten zusammen aggregieren und in andere Formate transformieren zu können.

Besonders bevorzugt bietet die Erfindung 100 auch Mittel, denen es möglich ist, die Zugriffskontrolllisten einfach zu verwalten, zum Beispiel durch zumindest ein Modell einer Zugriffskontrollliste 500, um die heterogenen Zugriffskontrolllisten aus verschiedenen Systemen 110 einheitlich

bearbeiten zu können. Wobei mit verwalten hierbei beispielsweise eine Schnittstelle zur einfachen Bearbeitung oder den einheitlichen Zugriff oder ähnliches gemeint ist. Als Beispiel kann hierbei Fig. 1c herangezogen werden. Dabei könnten in den verschiedenen Systemen 110 verschiedene Arten von Zugriffskontrolllisten zu finden sein, auf diese homogenisiert durch die Erfindung 100 zugegriffen wird.

Eine Ausführung des Modells 500 oder auch von Zugriffskontrolllisten, die zusammen mit der Erfindung 100 eingesetzt werden können verfügt dabei auch über Rechte, die als nicht vererbbar markiert werden können. Bevorzugt ist des Weiteren auch eine Zugriffskontrollliste des Modells 500 danach aufgebaut, dass zu einer Gruppe oder einem Klienten 130 Rechte oder Rollen erlaubt und verweigert werden.

Eine besonders bevorzugte weitere Fähigkeit ist es, nicht nur Rechte in Zugriffskontrolllisten spezifizieren zu können, sondern darin auch Rollen definieren zu können. Dadurch lassen sich Rollen ressourcenspezifisch oder auch in einer Ressourcenhierarchie definieren. Somit wird „Role based Access Control" auch auf Objektebene und nicht nur auf Klassenebene bei der Programmierung möglich, wie zum Beispiel bei Spring Security.

Ferner könnten auch Hierarchien von Rechten oder Rollen in Zugriffskontrolllisten definiert werden. Diese können dann bei Zugriffsentscheidungen oder der Aggregation genutzt werden. Der große Vorteil ist dabei, dass somit die Komplexität bei der Vergabe von Rechten abnimmt.

Bevorzugt verfügt die Erfindung 100 auch über die Fähigkeit, dass Informationen in einem oder mehreren Ausführungen der Erfindung 100 gespeichert werden können. Beispielsweise, wenn sich Informationen, zum Beispiel Erbinformationen, nicht in Sicherheitssystemen 110 speichern lassen. Zum Beispiel die Information, welche Ressource 111 von welchen Ressourcen 111 erbt. Aber es sind auch andere Fähigkeiten denkbar, über die z.B. das Modell 500 einer Zugriffskontrollliste verfügen kann. Solche Informationen können dann in der Erfindung 100 selbst gespeichert werden, oder diese verfügt zum Beispiel über Mittel die benötigten Informationen über Umwege im betreffenden System zu speichern. Beispielsweise könnte ein Aggregat berechnet werden, und die Zusatzinformationen könnten in den Kommentaren einer Zugriffskontrollliste gespeichert werden.

Fig. 1b zeigt die Erfindung 100 in einem größeren Umfeld. Hierbei ist zu sehen, dass die Erfindung 100 selbst ein Sicherheitssystem 110 beinhalten oder mit diesem direkt verbunden sein kann. Des Weiteren ist zu sehen, dass sie auch mit einer weiteren Instanz oder Variante der Erfindung 100 direkt verbunden sein kann. Beispielsweise kann durch diese Möglichkeiten eine höhere Skalierbarkeit ermöglicht werden.

Im Weiteren ist zu sehen, dass die Erfindung 100 mit weiteren Systemen 110 und Instanzen oder Varianten der Erfindung 100 über zumindest ein Computernetzwerk 50, wie zum Beispiel das Internet, verbunden sein kann. Dabei kann eine solche Verbindung eine statuslose oder auch statusbehaftete Verbindung sein.

Auch zeigt Fig. 1b, dass sämtliche Kommunikation der Erfindung 100 über zumindest ein Computernetzwerk 50 stattfinden kann. Es ist dabei aber auch möglich, dass eine Vielzahl vom Computernetzwerken 50 benutzt wird. Beispielsweise kann ein Klient 130 oder andere Teile auch über ein Drahtlosnetzwerk, wie Wlan oder Mobilfunknetzte mit der Erfindung 100 kommunizieren.

Durch die Verteilung über ein Computernetzwerk 50 ist es auch möglich, dass die Erfindung 100 selbst oder Teile von ihr über ein Computernetzwerk 50 verbunden und verteilt sind. Beispielsweise müssen Aggregation und Integrationseinheiten nicht zwangsläufig in einem System realisiert werden.

Die verschiedenen Systeme 110 in Fig. 1b zeigen weiterhin, dass eine Vielzahl von verschiedenen Verfahren und Systemen 110 mit einer Vielzahl von Instanzen der Erfindung 100 oder einer Viel-

zahl derer Komponenten zusammenspielen kann. Dies ermöglicht eine besonders gute Verteilbarkeit der Erfindung, z.B. in großen Clusterumgebungen.

Der Klient, der auch an das Computernetzwerk 50 angeschlossen ist, zeigt dabei, dass dieser direkt über das Netzwerk auf die Systeme 110, wie auch auf die Erfindung 100 zugreifen kann. Dabei ist dieser Klient aber als Stellvertreter für eine Vielzahl von Klienten 130 zu sehen.

Man beachte, dass die Erfindung 100 nicht zwangsläufig in einem Computernetzwerk 50 eingesetzt werden muss. Vielmehr kann diese auch in einer Vielzahl von Computernetzwerken eingesetzt werden. Beispielsweise auch in Peer-to-Peer-Netzwerken. Oder es ist möglich, dass der Klient über ein Mobilfunknetz mit dem Internet verbunden ist.

Fig. 1c zeigt dabei, wie die Erfindung 100 als Vermittler zur Kommunikation mit einer Vielzahl von Systemen 110 eingesetzt werden kann. Dies hat den Vorteil, dass durch die Erfindung 100 homogenisiert auf die verschiedenen Systeme 110 zugegriffen werden kann. Dabei ist es auch möglich, dass auf eine Instanz der Erfindung 100 zugegriffen wird, und diese mit weiteren Instanzen kommuniziert, um es z.B. Klienten 130 zu ermöglichen, Einstellungen zentral vornehmen zu können, und diese dann verteilt werden. Dabei kann der Klient 130 auch durch die einzelnen Bestandteile der Erfindung 100 auf verschiedene Systeme 110 zugreifen oder diese können bei einem Zugriff genutzt werden. Beispielsweise können Entscheidermittel 113 durch die Erfindung, z.B. auch unter Zuhilfenahme eines Modells 500 oder/und Integratoren angesprochen und manipuliert werden.

Auch ist es möglich, dass durch das Ansprechen der einzelnen Systeme 110 in der oder den Erfindungen, Erbschaftsinformationen hinterlegt werden. Beispielsweise kann durch einen Zugriff spezifiziert werden, welche Ressourcen 111 Rechte von welchen Ressourcen 111 erben. Dabei ist es auch möglich, dass die Erbschaftsstruktur, über Zugriffe auf eine oder mehrere Erfindungen oder Systeme 110 geändert wird.

Man beachte dabei, das ein Klient 130 in Fig. 1c nicht zwingend ein Benutzer sein muss. Vielmehr kann ein solcher Klient 130, wie beschrieben, auch ein System oder eine Erfindung 100 sein, wie dies durch die verschiedenen Bezeichner 100/110/130 angedeutet ist. Fig. 1d stellt dies noch einmal deutlicher dar. Dabei wird das Ganze zweistufig dargestellt. Ein Klient 100/110/130 kommuniziert dabei mit einem System oder einer Erfindung 100/110, das oder die wiederum mit einer Erfindung 100 kommunizieren kann. Dabei kann durch eine solche Kommunikation oder eine direkte Kommunikation mit einem Klienten 130 z.B. eine Aktion 150, wie zum Beispiel ein Verfahren ausgelöst werden.

Beispielsweise kann eine solche Aktion 150 ein Verfahren der Aggregatbildung sein. Für das Auslösen von Aktionen 150 können dabei hierfür besonders spezialisierte Mittel eingesetzt werden. Beispielsweise könnten regelmäßig Entscheidermittel 113 auf Aktualisierungen überprüft werden und dadurch die entsprechende Aggregatbildung ausgelöst werden. Dies könnte zum Beispiel in einem oder mehreren Integratoren oder in hierfür speziell ausgebildeten Mittel geschehen. Es könnte auch möglich sein, dass ein Klient 130, einer Erfindung 100 oder dem System einer Erfindung 100 mitteilt, dass Entscheidermittel 113 aktualisiert werden. Beispielsweise über spezielle dafür ausgebildete Mittel für diesen Fall, wie eine Erweiterung der mit der Erfindung 100 zusammen eingesetzten Systeme.

Durch diese Fähigkeiten können somit zusammenfassend gesagt, z.B. mehrere Erfindungen hintereinander geschaltet werden. Des Weiteren wurde erläutert wie passiv, wie z.B. durch Mitteilungen und aktiv, z.B. durch regelmäßiges Prüfen von Entscheidermitteln 113, Aktualisierungen von Entscheidermitteln 113 erkannt werden können, und dies zu Aktionen 150, wie z.B. Aggregatbildungen führen kann.

Somit kann die Erfindung 100 über Mittel verfügen, dass Aktualisierungen von Entscheidermitteln 113 erkannt werden. Dies kann dazu genutzt werden, dass beispielsweise ein Prozess zur Aggregatbildung, für Objekte die Rechte erben, automatisiert durchgeführt wird.

Fig. 1e zeigt einen weiteren Systemaufbau mit Klienten 130 und Erfindungen 100 und Systemen 110. Dabei können Klienten 130 wie zuvor auch Systeme 110 oder auch Erfindungen 100 sein. Der Klient 130 kann dabei direkt auf eine Ressource 111 zugreifen, die in einer Erfindung 100 oder einem herkömmlichen Sicherheitssystem zu finden ist 110/100. Beim Zugriff werden dabei Mittel zur Zugriffsentscheidung ausgewertet und zumindest eine Zugriffsentscheidung zu fällen. Der Klient kann dabei auch über die Erfindung 100 auf die Ressource 111 zugreifen. Eine weitere Möglichkeit ist, dass der Klient Mittel zum Zugriff auf die Ressource 111 der Erfindung 100 übermittelt bekommt, durch die er Zugriff auf die Ressource 111 erlangen kann. Beispielsweise können diese Mittel zum authentifizieren sein, durch die er sich beim System 100/110, das die Ressource 111 verwaltet, authentifizieren kann, oder durch die er Zugriff erlangen kann.

Die Erfindung 100 kann des Weiteren über kryptographische Mittel verfügen. Diese können beispielsweise in solchen Szenarien eingesetzt werden. Dabei kann dem Klienten 130 beispielsweise ein Geheimnis übermittelt werden, durch das er Zugriff erlangen kann.

Auch ist es möglich, dass sich der Klient 130 bei einer oder mehreren Erfindungen authentifiziert oder autorisiert, und diese dann den einzelnen Systemen 110 oder Erfindungen mitteilen, welcher Klient auf welche Ressource 111 Zugriff hat.

Bei solchen Szenarien können des weiteren Zeitfenster gesetzt werden, wie lange ein Klient Zugriff auf eine Ressource 111 hat. Beispielsweise, indem Geheimnisse eine Gültigkeitsdauer erhalten und diese beispielsweise den einzelnen Systemen 110 oder Erfindungen mitgeteilt wird.

Somit ist es möglich, dass auf Ressourcen 111 nicht über ein zentrales Sicherheitssystem zugegriffen werden muss, sondern direkt auf Ressourcen 111 in weiteren Systemen 110 durch verschiedenste Mittel zugegriffen werden kann.

Diese Fähigkeiten ermöglichen es zum Beispiel, dass Dateiuploads nicht über einen Dateistream über einen Server/System 110 zur Sicherheitskontrolle gesendet werden müssen. Vielmehr ist es somit möglich, dass Klienten 130 direkt Zugriff auf Ressourcen 111 erlangen und somit direkt Ressourcen 111 vom Klienten 130 in ein System übertragen werden können.

Diese Fähigkeit ermöglicht es, die Erfindung 100 besonders komfortabel mit Cloud Computing Diensten, wie zum Beispiel den Amazon Webservices, der Google App Engine oder Ähnlichen und zugehörigen weiteren Diensten einzusetzen. Beispielsweise können somit durch die Mittel, Geheimnisse für Klienten 130 zeitbegrenzt für den Zugriff zu berechnen, für sie direkte Uploads angeboten werden. Desweiteren können alle weiteren Fähigkeiten der Erfindung 100 in einem solchen Cloud oder Grid Computing Umfeld genutzt werden. Dadurch können somit die Sicherheitsmechanismen, die dort schon existieren, verwendet und durch die Erfindung 100 ergänzt werden. Beispielsweise können somit Zugriffskontrolllisten durch Vererbung ergänzt werden.

Besonders vorteilhaft ist auch die Fähigkeit der Erfindung, mit Identitätsprovidern 140, zum Beispiel Ldap-Authentifizierung (beschrieben in: http://www.microsoft.com/germany/technet/itsolutions/network/grundlagen/tec_comp_2_2_3.mspx) oder ähnlichen Apparaten, Techniken, Verfahren, Protokollen oder einer Kombination derer, zusammenarbeiten zu können, wie beispielsweise OpenID (http://openid.net/), Kerberos (http://de.wikipedia.org/wiki/Kerberos_(Informatik), http://www.hznet.de/security/kerbeinf.pdf) oder andere Authentifizierungsmittel. Identitätsprovider sind somit Mittel, die zumindest einen Benutzer authentifizieren können. Insbesondere in großen verteilten Szenarien ist diese Fähigkeit vorteilhaft. Fig. 1f zeigt hierzu exemplarisch ein solches Szenario. Dabei ist zu sehen, wie ein Klient 130 mit dem Identitätsprovider 140 kommuniziert, beispielsweise zur Authentifizierung,

wobei diese auch über die Erfindung 100 oder in Kombination mit dieser und dem System 100/110 mit der Ressource 111 geschehen kann. Diese und ähnliche Vorgänge sind dabei aus dem Stand der Technik bekannt. Wesentlich für dieses Szenario ist dabei, dass die Erfindung 100 und das System 100/110 mit der Ressource 111, einen Identitätsprovider 140 nutzen kann.

Man beachte zudem, dass ein Identitätsprovider selbst wiederum ein System 110 sein kann.

Beispielsweise kann die Erfindung 100 Aggregate für das System 100/110 berechnen, in denen Verweise auf einen Identitätsprovider 140 gesetzt werden. Dies ermöglicht es zum Beispiel, dass der Klient 130 sich direkt durch den Identitätsprovider 140 authentifizieren kann, und die Erfindung 100 selbst bei dem konkreten Zugriff nicht gebraucht wird.

Eine weitere Fähigkeit über die die Erfindung 100 in einer Ausführung verfügen kann ist zudem das Integrieren von verschiedenen Identitätsprovidern 140 oder ähnlichen Authentifizierungsmitteln. Dabei kann diese über die Fähigkeit verfügen, Klienten 130 eines Identitätsproviders 140 Klienten 130 in einem anderen Identitätsprovider 140 zuzuordnen. Solche Zuordnungen können zum Beispiel durch Regeln oder einfache oder komplexe Mappings, die z.B. in einer Speichereinheit, auf die die Erfindung 100 zugreifen kann oder die in diese integriert ist, definiert werden. Dadurch können beispielsweise bei der Aggregatbildung nicht nur systemübergreifend Aggregate und Vererbungen ermöglicht werden, sondern es können dabei weitere Rahmenfaktoren beachtet werden und dass verschiedene Systeme 110 auch oftmals Klienten 130 verschieden bezeichnen können. Somit können letztendlich auch Ressourcen 111 in Systemen 110 mit verschiedenen Systemen 110 durch die Erfindung 100 Beziehungen wie z.B. Erbschaft haben.

Diese Fähigkeiten, durch die Erfindung 100 eine höhere Skalierbarkeit erreichen zu können, kann besonders bevorzugt im Bezug auf moderne Internetplattformen wie z.B. Social Networks eingesetzt werden. Beispielsweise hat http://www.studivz.net/ das http://www.wer-kennt-wen.de/ und http://www.facebook.com/ das Problem, sofern die Adresse eines Bildes im Netzwerk bekannt ist, dass jeder durch die direkte URL das Bild abrufen kann und keine Sicherheitsfunktionen mehr das Bild schützen, da nur der Zugriff durch die Plattform die Sicherheitsüberprüfung durchführt und nicht die Bild-ausliefernde Komponente. Dies wird von vielen Benutzern als Sicherheitslücke gesehen. Durch die Erfindung 100 wäre ein solches Problem lösbar. Dabei könnten direkt Entscheidermittel 113 zum Bild hinzu gespeichert werden. Zum Beispiel als Zugriffskontrolliste für den Webserver der das Bilder ausliefert.

Beispielhaft ist dies in Fig. 1g aufgezeigt. Dabei wurde ein allgemeines System 110 durch ein Social Network 160 dargestellt, um das Szenario besser zu visualisieren. Dabei wurde bewusst ein zweites System 110 hinzugefügt, das zumindest z.B. den Bildserver 110 des Social Networks darstellt und somit symbolisieren soll, dass auf diesen auch ohne das Social Network 160 zugegriffen werden kann. Die Erfindung 100 erzeugt dabei aus den Daten im Social Network 160 Entscheidermittel 113 und speichert diese in dem Bilderserver 110. Dies kann beispielsweise dadurch passieren, dass auf Datenbanken oder ähnliches des Social Networks 160 zugegriffen wird und daraus Zugriffskontrolllisten erstellt werden. Dabei können in diesen auch Benutzer/Klienten 130 spezifiziert werden, die auf verschiedene Bilder Zugriff haben. Dabei könnten zum Beispiel Verweise von Bildern zu den Benutzerdaten/Klienteninformationen/Benutzeridentitäten hinterlegt werden.

Der Klient 130 kann nun auf das Social Network 160 und den Bilderserver 110 zugreifen. Dabei kann dann der Bilderserver 110 die Zugriffskontrolle des Zugriffsentscheiders unter Nutzung der Entscheidermittel 113, die durch die Erfindung 100 erzeugt oder aktualisiert wurden, durchführen. Dabei können zuvor oder im Weiteren in diesem Dokument spezifizierte Mittel genutzt werden. Beispielsweise könnte der Klient 130 vom Social Network 160 ein Geheimnis erhalten. Oder der Klient 130 könnte sich gegenüber dem Social Network 160 authentifizieren, womit dieses die Rolle eines Identitätsproviders 140 einnimmt. Auch ist es denkbar, andere Identitätsprovider 140

zu nutzen. Zum Beispiel könnten ähnliche Verfahren oder Apparate, wie ein Apache Websever eingesetzt werden, für den Module verfügbar sind, um gegen verschiedenste Quellen Authentifizierungen durchzuführen oder auch auf verschiedenste Quellen zu verweisen.

Generell sind hierbei durch die Aggregate viele Möglichkeiten denkbar, wie dieser direkte Zugriff durchgeführt werden könnte. Im Wesentlichen besitzt die Idee, und ein somit zugehöriges Verfahren oder Apparate durch die Erfindung 100 zu nutzen und Bilder oder ähnliches von modernen Web Plattformen, insbesondere Social Networks 160 abzusichern, die folgenden Schritte. Diese oder Teile derer können natürlich mit allen weiteren Merkmalen der Erfindung kombiniert werden.

a. Zugriff auf die Daten zumindest einer Webplattform 160 und bestimmen der Daten, die für zumindest eine Zugriffsentscheidung auf zumindest eine Ressource 111 innerhalb der Webplattform 160 genutzt werden;

b. berechnen und Speichern von Mitteln 113, die zu zumindest einer Zugriffsentscheidung genutzt werden, wobei diese Zugriffsentscheidung unter der Nutzung von Mitteln 114 des ressourcenausliefernden Systems 110 stattfindet.

Somit stellt diese Ausführung der Erfindung 100 eine Möglichkeit dar die Systeme, die Ressourcen 111 wie Bilder oder ähnliches ausliefern, zusätzlich zu der Zugriffsentscheidungen zu Nutzen. Dies ermöglicht es somit, diese Ressourcen 111 besser abzusichern und stellt dabei besser dar, wobei die Erfindung 100 in einem Anwendungsfall eingesetzt werden kann.

Die Erfindung 100 kann zudem über die Eigenschaft verfügen, dass ihr zur Laufzeit neue Funktionen hinzugefügt werden. Beispielsweise durch das Nachladen von Quelltext oder kompilierten Programmen. Dies ermöglicht es, die Erfindung 100 besonders flexibel anzupassen.

In Fig. 2a ist ein Beispiel für die Erbschaft von Entscheidermitteln 113 oder auch von Ressourcen 111 aufgezeigt. Dabei kennzeichnen die Vierecke die einzelnen verschiedenen Systeme 110, benannt mit 200, 210 und 220, in denen die Ressource 111 oder auch die Entscheidermittel 113 vorkommen können. Die Kreise zeigen Anordnungen der Erbschaft zwischen Mitteln, die zur Zugriffsentscheidung genutzt werden, die zum Beispiel dadurch zu Stande kommen, dass auf eine Ressource 111 eine oder mehrere ElternRessourcen 111 verweisen oder es in den Entscheidermitteln 113 selbst definiert ist, wovon geerbt wird. Es ist dabei zu sehen, dass 211 von 201 erbt und 212 und 222 von 211. Dabei ist die Erbschaft zwischen 211 und 201 systemübergreifend zwischen 210 und 200 und die Erbschaft zwischen 222 und 211 zwischen den Systemen 110 220 und 210. Ähnlich ist der Sachverhalt zwischen 202 und 221, 223 und 224.

Fig. 2b zeigt dabei ein weiteres Beispiel für eine Erbschaft. Hierbei wird von mehreren Elternobjekten geerbt. Dabei kann eine Mehrfachvererbung beliebig viele Vorfahren besitzen, von denen Rechte ererbt werden. Dieses Beispiel der Mehrfachverberung wird in Fig. 2c in einem größeren Rahmen dargestellt. Dabei wird gezeigt, dass Mehrfachvererbung dabei auch über verschiedene Systeme 110 230, 240 und 250 hinweg geschehen kann. Dabei sind wie zuvor die Pfeilspitzen als Eltern-Kind-Zuordnung zu sehen.

Eine Variante der Erfindung 100 kann des Weiteren über Fähigkeiten verfügen, die es ermöglichen, Elemente im Erbschaftsbaum anders anzuordnen und die Vererbungsstruktur zu verändern oder auch die Vererbung für einzelne Elemente an als auch abzuschalten. An als auch abzuschalten bedeutet dabei, dass zum einen Elemente, die einen oder mehrere Vorfahren besitzen, zukünftig keine oder weniger Vorfahren besitzen und somit keine oder weniger Rechte erben oder zum anderen umgekehrt Elemente, die keine Vorfahren besitzen, einen oder mehrere Vorfahren zugeteilt bekommen. Ebenso können Elemente neue Vorfahren oder weitere Vorfahren zugeteilt bekommen. Für solche Fälle kann die Erfindung 100 zudem über weitere, besonders hierfür spezialisierte, Mittel verfügen, die zum Beispiel neue Aggregatvorgänge auslösen, die die neue Erbschaftsstruktur und die zugehörigen Mittel zur Zugriffsentscheidung 112 beachten.

Besonders bevorzugt kann die Erfindung 100 auch über einen Zykluschecker bei der Vererbung verfügen. Ein solcher kann beispielsweise Zyklen in Vererbungshierarchien aufdecken. Dieser kann bei Einfach- als auch bei Mehrfachvererbung eingesetzt werden. Ein Beispiel für einen Zyklus ist in Fig. 2c zu sehen. Dabei erbt 242 von 241 und 231 von 242. Nun könnte die Verbindung 260 durch die 241 hinzugefügt werden durch die 241 von 231 erben würde. Solche und ähnliche Fälle können von einem Zykluschecker erkannt werden.

Ein solcher Zykluschecker könnte beispielsweise dadurch realisiert werden, dass beim Hinzufügen einer neuen Erbschaftverbindung geprüft wird, ob der Erbschaftsbaum des Elementes A von dem Element B zukünftig erben soll, schon Element B an irgend einer Stelle im bisherigen Baum enthält und ob Element A und B in verschiedenen Objekten sind.

Weil in den beispielhaften Erbschaftsbäumen Aggregate durch die Erfindung 100 mit den jeweiligen Ressourcen 111 in den Systemen 110 assoziiert werden können, wird ein weiterer Vorteil der Erfindung 100 sichtbar. Es ist es somit möglich, dass an die jeweiligen Systeme 110 Anfragen gestellt werden, die schon bei der Anfrage selbst die Aggregate nutzen, um zu der Ergebnismenge gehörende Elemente zu bestimmen. Dies ermöglicht es zum Beispiel, unpassende Elemente schon in einer Abfrage auszuschließen, da alle Zugriffsinformationen durch Aggregate direkt verfügbar sind. Beispielsweise könnten Objekte einer Klasse erfragt werden, für die der Anfragende eine bestimmte Rolle besitzt. Ohne Aggregate müssten die Vorfahren ebenso befragt werden und dies wäre langsam, insbesondere bei fremden Systemen, sofern überhaupt technisch möglich. Mit Aggregaten können diese nun verwendet werden, um nur zutreffende Objekte zu bestimmen.

Um auf die verschiedenen Systeme 110 200, 210 und 220 und deren Entscheidermittel 113 zuzugreifen, kann z.B. die Integrationseinheit 101verwendet werden. Dadurch, dass die Erfindung 100 auch über die Aggregationsmittel verfügt, ist es möglich, die Erbschaft systemübergreifend zu ermöglichen. Dabei nutzt die Aggregationseinheit 102 z.B. die Integrationseinheit, um auf die verschiedenen Systeme 110 zuzugreifen. Weil diese somit die Möglichkeit hat, die Entscheidermittel 113 aus den verschiedenen Systemen 110 zu lesen, kann sie aus diesen Aggregate berechnen. Beispielsweise kann sie 201 lesen und mit dem derzeitigen Inhalt von 211 die absoluten Rechte für 211 schreiben, sodass dies wiederum bei weiteren Zugriffen als Entscheidermittel 113 verwendet werden kann. Deshalb kann danach beispielsweise 222 und 212 berechnet werden. Ebenso ist dies so ähnlich für die weiteren Rechte und für das Erben von mehreren Vorfahren umsetzbar.

Man beachte jedoch, dass die Aggregation, wie zuvor beschrieben, auch weitere Schritte, wie beispielsweise die Transformation der Mittel zur Zugriffsentscheidung in das richtige Format, enthalten kann. Dabei kann die Aggregation auch genutzt werden, um z.B. lange Zugriffskontrolllisten zu vereinfachen, indem zum Beispiel doppelte Einträge, die z.B. bei Erbschaft zustande kommen zu filtern. Solche Transformationen können in der jeweiligen Anwendung, durch speziell dafür angepasste Transformationsmittel, realisiert werden.

Die Aggregation kann des Weiteren unter der Nutzung von Mechanismen aus der funktionalen Programmierung oder/und der Nutzung der Warteschlangentheorie beschleunigt werden. Beispielsweise kann die Aggregation durch deklarative Programmierung definiert werden, um eine hohe Parallelität zu erreichen. Dabei ist es auch möglich, dass die Aggregation Techniken, wie zum Beispiel Map Reduce, zum Beispiel US7650331, Amazon Elastic MapReduce (http://aws.amazon.com/elasticmapreduce/) oder Ähnliche, die z.B. unter http://de.wikipedia.org/wiki/MapReduce zu finden sind, nutzt. Des Weiteren können Erkenntnisse aus der Warteschlangentheorie genutzt werden, um einen hohen Datendurchsatz zu erreichen.

Fig. 3a zeigt das Verfahren, nach dem Aggregate gebildet werden. Dabei werden zuerst die benötigten Mittel, die zur Aggregatbildung benötigt werden, bestimmt 301. Darauf werden dann eines

oder mehrere Aggregate gebildet 302. Solche benötigten Mittel können dabei beispielsweise die Elemente sein, von denen ein Element, für das ein Aggregat gebildet werden soll, erbt.

Dabei kann das Bestimmen der benötigten Mittel auch das Laden der benötigten Mittel einschließen. Nach der Bildung der Aggregate kann zudem noch ein Schreibvorgang erfolgen, der neue Entscheidermittel 113 erzeugt, löscht oder aktualisiert. Das Bestimmen oder Laden der nötigen Mittel kann auch durch die Integrationseinheit, ebenso wie das Schreiben durchgeführt werden. Auch ist es möglich, dass diese dabei über zumindest ein Computernetzwerk 50 übertragen werden. Zudem ist es möglich, dass die Aggregationseinheit(en) und die Integrationseinheit(en) als gemeinsame Einheit erstellt werden. Somit kann eine Aggregationseinheit 102 über sämtliche Merkmale der Integrationseinheit 101 verfügen und umgekehrt.

Fig. 3b zeigt, dass Aggregatbildungen auch wieder neue Aggregatbildungen auslösen können 303. Beispielsweise könnte wie in Fig. 3c eine Vererbungshierarchie existieren. Dadurch, dass ein Aggregat von o1 gebildet wird oder die zugehörigen Mittel, die zur Zugriffskontrolle genutzt werden, erzeugt oder aktualisiert werden, könnte dies durch die Erfindung 100 erkannt werden und Aggregate für o2 und o3 könnten berechnet werden. Ebenso für o4,o5 und o6. In Fig. 3d ist dies dargestellt. Dabei können Aggregate, die auf der gleichen Hierarchiestufe sind, z.B. auch parallel berechnet werden.

Die Erfindung 100 kann für solche Fälle über spezialisierte Mittel verfügen, die es z.B. ermöglichen, Aggregate parallel zu erzeugen. Beispielsweise können bei jeder neuen Hierarchiestufe neue Prozesse für jedes Element erzeugt werden.

Das eigentliche Bilden der Aggregate kann über Regeln oder Computerprogramme spezifiziert sein. Dabei könnten auch Regeln oder Computerprogramme dynamisch zur Laufzeit geladen werden. Solche Regeln oder Computerprogramme können dabei speziell für die verschiedenen Mittel, die zur Zugriffsentscheidung genutzt werden, optimiert sein.

Optimaler weise kann des Weiteren das Erzeugen eines Ablaufplans zur Aggregatbildung Teil der Erfindung 100 und des Aggregaterstellungsverfahrens sein. Ein solcher Ablaufplan kann dazu dienen, wie und/oder in welcher Reihenfolge Aggregate für verschiedene Mittel zur Zugriffsentscheidung bestimmt werden sollen. Dabei kann dieses Erzeugen eines Ablaufplans, aufgrund der Ressource, für die ein Aggregat die Mittel zur Zugriffsentscheidung nutzt, geschehen. Es ist auch möglich, dass dabei die Mittel oder mehrere Mittel selbst genutzt werden, um zu bestimmen, wie das Aggregat gebildet werden soll. Zudem ist es auch möglich, dass weitere Mittel der Erfindung 100 benutzt werden, um einen solchen Ablaufplan zu erzeugen.

Beispielsweise kann die Erfindung 100 auch über einen oder mehrere Erbschaftsbäume verfügen, z.B. in mehreren Varianten oder Instanzen, in denen Informationen hinterlegt sind, welche Vererbungen zwischen Ressourcen 111 oder deren Mittel zur Zugriffsentscheidung existieren. Dabei könnte als Datenstruktur z.B. ein speziell angepasster Patricia Trie, HAT Trie oder Brust Trie oder eine ähnliche Datenstruktur (vgl. „HAT-trie: A Cache-conscious Trie-based Data Structure for Strings", http://crpit.com/confpapers/CRPITV62Askitis.pdf) dienen. Diese könnten dann bei der Aggregatbildung genutzt werden und einen Ablaufplan dafür bilden, damit z.B. Aggregate in der Hierarchie von oben nach unten berechnet werden.

Fig. 4 zeigt eine Integrationseinheit 101 der vorliegenden Erfindung 100. Diese verfügt über einen Zugriffsausführer 401, der den Zugriff auf verschiedene Systeme 110, über zumindest einen Integrator 402, durchführt. Die Integratoren 402 enthalten dabei Mittel, um auf verschiedene Systeme 110 zugreifen zu können. Solche Integratoren 402 können dabei zum Beispiel programmatisch als eine Sammlung von Funktionen oder auch Klassen erstellt werden. Durch diese Integratoren 402 ist es der Integrationseinheit 101 durch den Zugriffsausführer möglich, z.B. die verschiedenen in diesem Dokument beschriebenen Operationen, auf die Mittel, die zur Zugriffskontrolle genutzt werden, durchzuführen. Im Zugriffsausführer 401 oder auch in einem oder mehreren Integratoren

402 oder an anderer Stelle in der Integrationseinheit 101, können dabei zuvor besprochene Mittel zur Transformation eingesetzt werden.

In den Integratoren 402 im Zugriffsausführer 401 oder an anderer Stelle der Erfindung 100 kann zudem ein Modell 500 von Mitteln zur Zugriffskontrolle 112, das zuvor besprochen wurde, verfügbar sein. Dieses kann zum Beispiel als Transformationsmodell 500 oder zum Zugriff von Klienten 130 dienen, wie in Fig. 5 dargestellt. Dabei werden die Mittel, die zur Zugriffsentscheidung, die dem Modell von System A 501 folgen, zuerst in das Modell der Erfindung 500 transformiert und von diesem in das Modell des Systems B 504 oder auch C 503 oder D 502. Dies ermöglicht beispielsweise, dass nicht alle verschiedenen Transformationsarten von verschiedenen Systemen 110 zueinander beschrieben werden müssen.

Die Erfindung 100 kann, wie erwähnt, auch über eine Speichereinheit verfügen. Auf diese kann zum Beispiel auch von den Bestandteilen der Erfindung, wie zum Beispiel der Integrationseinheit 101 oder Aggregationseinheit 102 oder deren Bestandteile zugegriffen werden. In dieser können zum Beispiel die Daten über Erbschaftsbeziehungen oder andere Daten gespeichert werden. Zum Beispiel könnte ein System es nicht unterstützen, Aggregat-Entscheidermittel und Original-Entscheidermittel zu speichern. Somit könnte das Original-Entscheidermittel vor dem Aggregatsvorgang in der Erfindung 100 verbleiben und nur das Aggregat-Entscheidermittel in das System 110 geschrieben werden. Sofern das Original-Entscheidermittel über die Erfindung 100 geändert würde, würde dies ein neues Aggregat-Entscheidermittel erzeugen. Oder es wäre möglich, dass falls das Aggregat-Entscheidermittel im System 110 geändert wurde, im Vergleich mit dem Original-Entscheidermittel, in der Erfindung 100 die Veränderung zu erkennen und das Original-Entscheidermittel dementsprechend anzupassen.

Wie zu sehen ist, kann die Integrationseinheit 101 auch über einen Zwischenspeicher/Cache 404 verfügen. Dies soll vor allem der Beschleunigung dienen. Dies kann die Geschwindigkeit von Verarbeitungen erhöhen, wie zum Beispiel bei Aggregatbildungen oder auch beim Nutzen der Erfindung 100 zur Zugriffskontrolle. Dabei kann der Cache 404 an verschiedenen Stellen in der Erfindung 100 eingesetzt werden. Es ist dabei auch denkbar, Caches 404 an mehreren Stellen einzusetzen.

In Fig. 4 ist aufgezeigt, dass ein Cache 404 von den Integratoren 402 und vom Zugriffsausführer benutzt werden kann. Beispielsweise können geladene Entscheidermittel 113 im Cache 404 von Integratoren 402 oder vom Zugriffsausführer 401 abgelegt werden. Dieser oder die Integratoren 402 könnten vor Zugriffen zuerst den Cache 404 auf den Inhalt der benötigten Mittel prüfen, um langwierige, erneute Zugriffe durch Netzwerklatenz zu vermeiden.

Ferner kann die Erfindung 100 über ein Systemverzeichnis 403 verfügen. In diesem kann beispielsweise hinterlegt werden, zu welchen Ressourcen 111 welche Entscheidermittel 113 und/oder Systeme 110 gehören. Dabei kann hinterlegt sein, in welchen Systemen 110 diese Mittel abgerufen werden können, oder/und durch welche Integratoren 402 diese aufzufinden sind.

Diese Informationen können beispielsweise über einfache Mappings oder auch über Regeln hinterlegt sein. Solche Regeln können zum Beispiel auch spezifizieren, wie aufgrund zumindest eines Identifikationsmerkmals einer Ressource 111, zumindest ein oder auch mehrere zugehörige Integratoren 402 bestimmt werden können. Dabei kann z.B. eine Anfrage an das Systemverzeichnis 403 über eine Ressource 111 gestellt werden, die dann mit zumindest einem zugehörigen Integrator 402 oder einem Verweis aus diesem beantwortet werden kann.

Somit stellt das Systemverzeichnis 403 Mittel bereit, die es ermöglichen, durch die Integratoren 402 und weitere zugehörige Informationen, verwaltet werden zu können.

Dabei kann der Zugriffsausführer 401 bei einem Zugriff, z.B. aufgrund einer Ressource 111 oder eines ihrer Identifikationsmerkmale, zumindest einen zugehörigen Integrator 402 bestimmen und

somit auf deren System und somit auf deren Mittel, die zur Zugriffsentscheidung 112 genutzt werden zugreifen.

Eine, besonders bevorzugt im dynamischen Internetumfeld, wie Web.2.0, eingesetzte Variante der Erfindung 100 besitzt die Fähigkeit, dass dynamisch Integrationsmittel eingebunden oder entfernt werden können. Solche Integrationsmittel können zum Beispiel Integratoren oder Gruppen von Integratoren 402 sein. Dabei können solche Integratoren 402 zum Beispiel beim dynamischen Hinzufügen dem Systemverzeichnis 403 hinzugefügt werden. Dabei könnte z.B. im Integrator 402 selbst oder durch Zusatzinformation, wie zum Beispiel die zuvor erwähnten Regeln, Mappings oder Computerprogramme, definiert sein, wie die zugehörigen Ressourcen 111 zu erkennen sind. Dies könnte dann ebenfalls in das Systemverzeichnis 403 aufgenommen werden. Dadurch ist es zur Laufzeit möglich, auch aufgrund von Ressourcen 111 oder derer Identifikationsmerkmale, den neuen Integrator 402 als zugehörig zu bestimmen und diesen somit nahtlos in die bisherige Funktionalität eines Systems einzuweben. Ebenfalls ähnlich wie das Hinzufügen könnte das Entfernen realisiert werden. Dabei würde die Information des Erkennens der zugehörigen Ressourcen 111 aus dem Systemverzeichnis 403, mitsamt dem Integrator 402, entfernt werden.

Eine weitere Variante der Erfindung 100 kann Mittel zum dynamischen Hinzufügen von Komponenten benutzen. Zum Beispiel OSGI auf der Java Plattform. Beispielsweise könnte damit das dynamische Hinzufügen/Registrieren und Entfernen von Integratoren 402 realisiert werden.

Die hier Vorgestellte Erfindung 100, Verfahren, Anordnung und Apparat kann besonders bevorzugt auch dazu eingesetzt werden, um für Videoplattformen genutzt zu werden. Insbesondere, um diese mit Social Networks zu verbinden.

Ein besonders bevorzugter Anwendungsfall dieses Sicherheitssystems ist die Kombination mit einer Videoplattform oder einer Livestreaming-Videoplattform, wie z. B. das „Newreporter System, Anordnungen und Verfahren für Videoplattformen“ das vom Erfinder am 4.4.2010 zur Anmeldung beim DPMA eingereicht wurde und somit dem Stand der Technik entspricht (DPMA Amtliches Aktenzeichen: 10 2010 016 323.6). Dieses Newreporter System kann durch die Kombination mit der Erfindung beispielsweise mit weiteren Systemen 110 interagieren und Rechte erben, und es können Sicherheitsfunktionen, aufgrund von Klienteninformation, realisiert werden, zum Beispiel ortsabhängige Sicherheitsfunktionen.

Ein weiterer, besonders bevorzugter, Anwendungsfall ist die Kombination der Erfindung 100 mit einem Hyperadapter (EP09180953) . Hierbei kann die Erfindung, insbesondere die Yourweb Variante, absichern.

Ein weiterer, besonders bevorzugter, Anwendungsfall ist die Kombination der Erfindung 100 mit einem So-ad-tec System (EP10001967). Hierbei kann zum Beispiel das Nexusnodes System damit abgesichert werden. Dabei ist es auch möglich, ein So-ad-tec System selbst damit abzusichern. Des Weiteren kann die dargestellte Erfindung 100 auch über ein dort beschriebenes SCAPTCHA System oder dessen Funktionen verfügen oder mit einem solchen zusammenarbeiten. Dies macht es zum Beispiel möglich, ein solches SCAPTCHA System als Infrastrukturdienst, zusammen mit den anderen beschrieben Funktionen, in einer Cloud Computing Infrastruktur anzubieten.

Ein weiterer Anwendungsfall ist das Absichern von betriebswirtschaftlichen Systemen. Z. B. ERP-Systemen, CRM-Systemen, Portale u.v.A.

Man beachte, dass diese Erfindung, bzw. Gruppe von Erfindungen als computerimplementierte Systeme, beziehungsweise als Computerprogramme realisierbar sind. Aufgrund der Natur dieser Erfindung 100 lassen sich sämtliche dargestellten Sachverhalte in verschiedenen Programmiersprachen auf verschiedenen Plattformen realisieren. Zudem lassen sich sämtliche Verfahren in deklarativen Programmen und somit in deklarativen Sachverhalten darstellen und umgekehrt. Ebenso lassen sich die Verfahren als Apparate oder Anordnungen umwandeln und umgekehrt.

Zudem lassen sich, aufgrund der flexiblen Natur der Erfindung, viele einzelne besprochene Teile der Erfindung 100 kombinieren oder anders anordnen, um Lösungen mit höherer Geschwindigkeit oder in anderer Form bessere Lösungen zu ermöglichen. Daher ist die Beschreibung der Erfindung 100 eher als exemplarische Ausführung zu verstehen, derer Merkmale auch in anderen Anordnungen vorkommen können.

Ansprüche

1. Eine Erfindung (100) als System oder Anordnungen, für das Absichern von Zugriffen auf Ressourcen (111), insbesondere für Zugriffe über ein Computernetzwerk (50), wobei das System oder eine Anordnung folgendes aufweisen:

   a. Zumindest ein Mittel zur Integration, das es ermöglicht, auf zumindest ein oder mehrere Mittel zuzugreifen, die genutzt werden, um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource (111) zu beeinflussen;

   b. Zumindest ein Mittel zur Aggregation, das es ermöglicht, aggregierte Zugriffsrechte zu berechnen, wobei bei der Berechnung, zumindest ein Mittel zur Zugriffsentscheidung (112) verwendet wird.

2. Ein System oder eine Anordnung nach Anspruch 1, wobei die Erfindung (100), zumindest ein berechnetes Recht, zumindest eines Aggregates, als Mittel, das zu zumindest einer weiteren Zugriffsentscheidung genutzt wird, gespeichert wird.

3. Ein System oder eine Anordnung nach Anspruch 1 oder 2, wobei die Erfindung (100) über zumindest ein Mittel verfügt, dass es ermöglicht, dass zumindest ein Recht über zumindest zwei verschiedene Systeme (110) vererbt werden kann.

4. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei auf zumindest ein Mittel zur Zugriffsentscheidung (112) beim Berechnen zumindest eines Aggregates über zumindest ein Computernetzwerk (50) zugegriffen wird.

5. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei die Erfindung (100) über zumindest einen Erbschaftsbaum verfügt, der zumindest eine Erbschaftsbeziehung aufzeigt, die das Erben von Rechten zwischen zumindest zwei oder mehr Ressourcen (111) definiert.

6. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei bei zumindest einer Zugriffsentscheidung im Quelltext eines Programmes spezifizierte Mittel berücksichtigt werden.

7. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei das Einbinden oder Entfernen von Mitteln zur Integration zur Laufzeit geschehen kann.

8. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei der Zugriff von zumindest einem Klienten (130), auf zumindest eine Ressource (111), direkt durch das Auswerten von zumindest einem von der Erfindung (100) erstellten oder aktualisierten Mittel zur Zugriffsentscheidung (112), geschieht.

9. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei die Erfindung (100) über kryptographische Mittel verfügt oder/und mit solchen Mitteln eines weiteren Systems oder Plattform zusammenwirken kann.

10. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei die Erfindung (100) mit einer Cloud Computing Plattform zusammen genutzt oder als Infrastrukturdienst eingesetzt wird.

11. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei zumindest eine Klienteninformation bei zumindest einer Zugriffsentscheidung, direkt oder indirekt durch Aggregate, beachtet wird.

12. Ein System oder Anordnungen nach einem der vorhergehenden Ansprüche, wobei bei zumindest einer Zugriffsentscheidung, direkt oder indirekt durch Aggregate, zumindest eine Hierarchie, aus Rollen und/oder Rechten, die mit zumindest einer Ressource (111) assoziiert ist, beachtet wird.

13. Ein Verfahren zum Absichern von Zugriffen auf Ressourcen (111), insbesondere für Zugriffe über ein Computernetzwerk (50), wobei das Verfahren die folgenden Schritte aufweist:

    a. Zugriff auf ein oder mehrere Mittel (112), die genutzt werden, um Zugriffsentscheidungen über den Zugriff auf zumindest eine Ressource (111) zu beeinflussen;

    b. Berechnung zumindest eines Aggregates, wobei bei der Berechnung zumindest ein Mittel zur Zugriffsentscheidung (112) verwendet wird

14. Das Verfahren nach Anspruch 13, ferner aufweisend den Schritt der Zugriffsentscheidung, wobei diese Zugriffsentscheidung unter der Nutzung von Mitteln (112) des ressourcenausliefernden Systems (110) stattfindet und dabei zumindest ein Mittel, das bei der Berechnung des Aggregates genutzt wurde, zu einer Webplattform (160) zugehörig ist.

15. Ein Computerprogramm, das Instruktionen aufweist, um ein Verfahren nach einem der vorhergehenden Ansprüche 13 – 14 auszuführen.

Fig. 1a

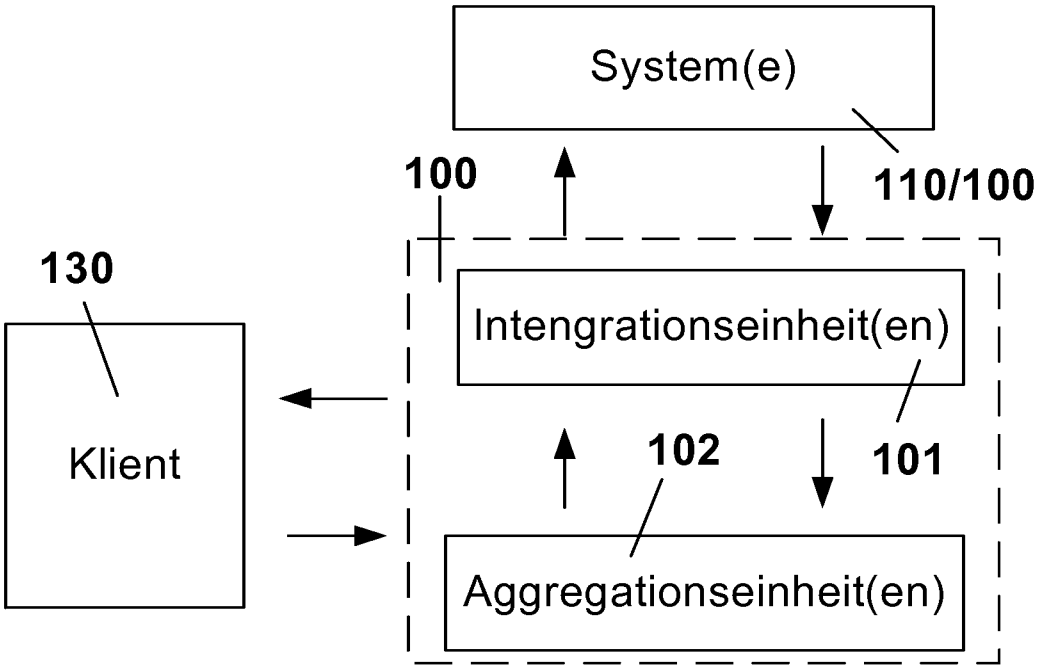

System(e)
100
110/100
130
Intengrationseinheit(en)
Klient
102
101
Aggregationseinheit(en)

Fig. 1b

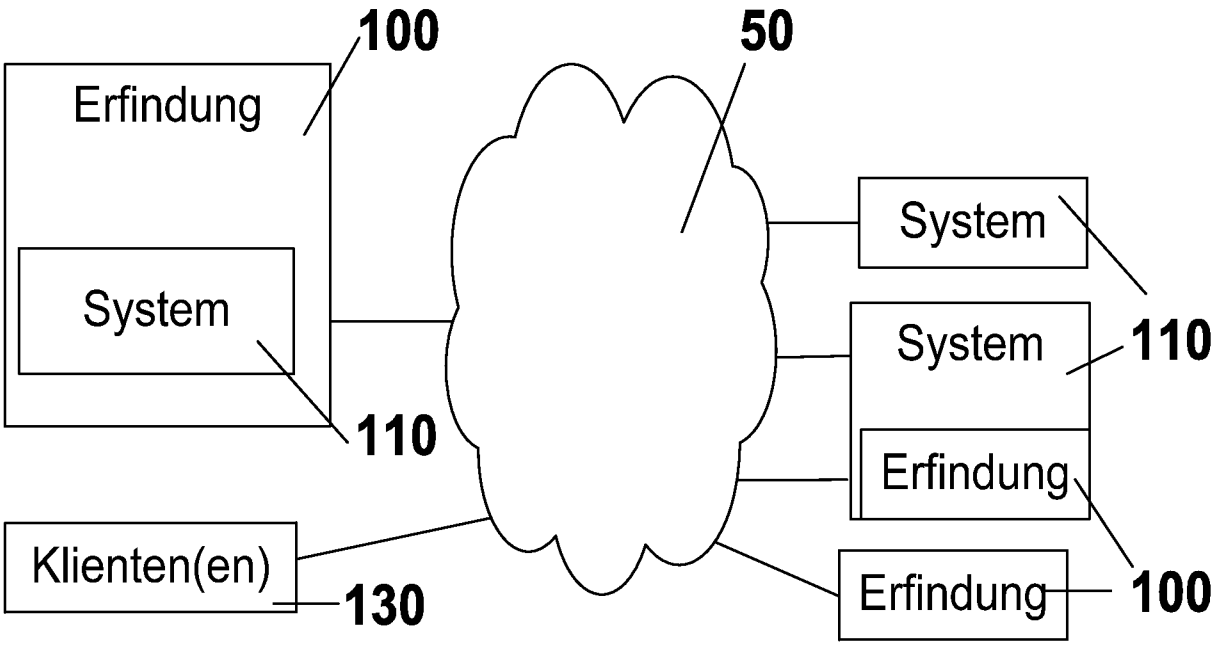

100
50
Erfindung
System
System
110
110
Erfindung
Klienten(en)
130
Erfindung
100

Fig. 1c

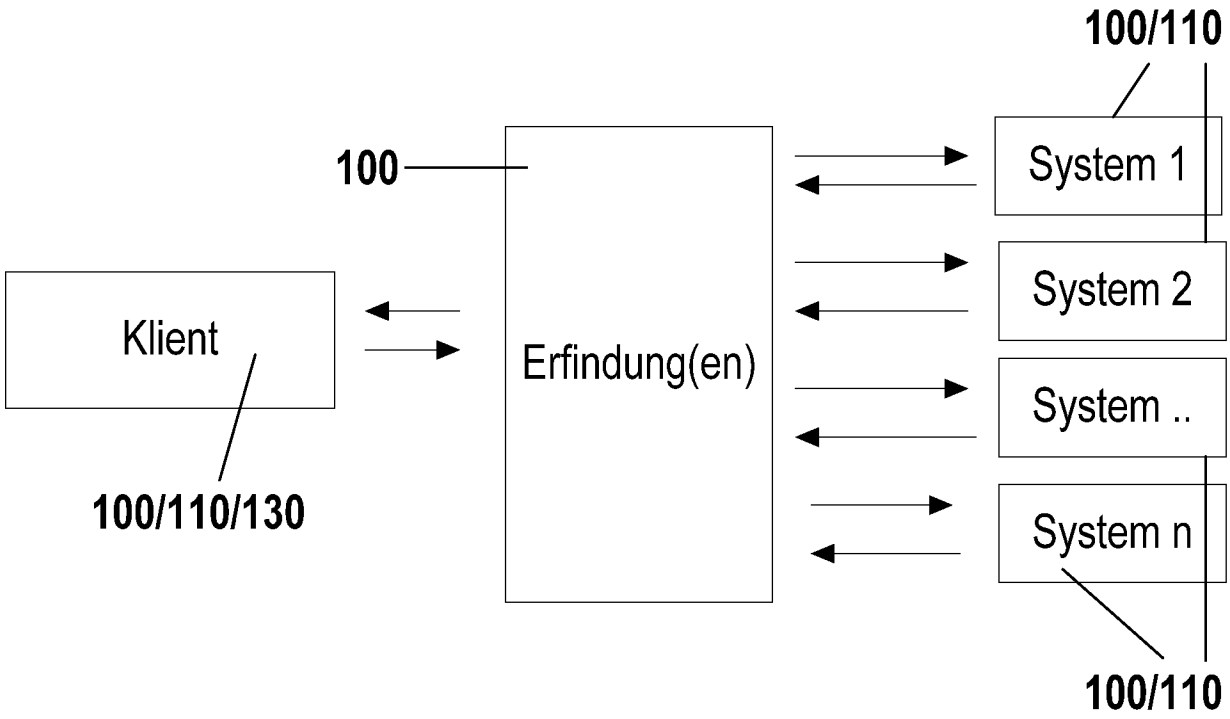

100/110
100
System 1
System 2
System ..
System n
Klient
Erfindung(en)
100/110/130
100/110

Fig. 1d

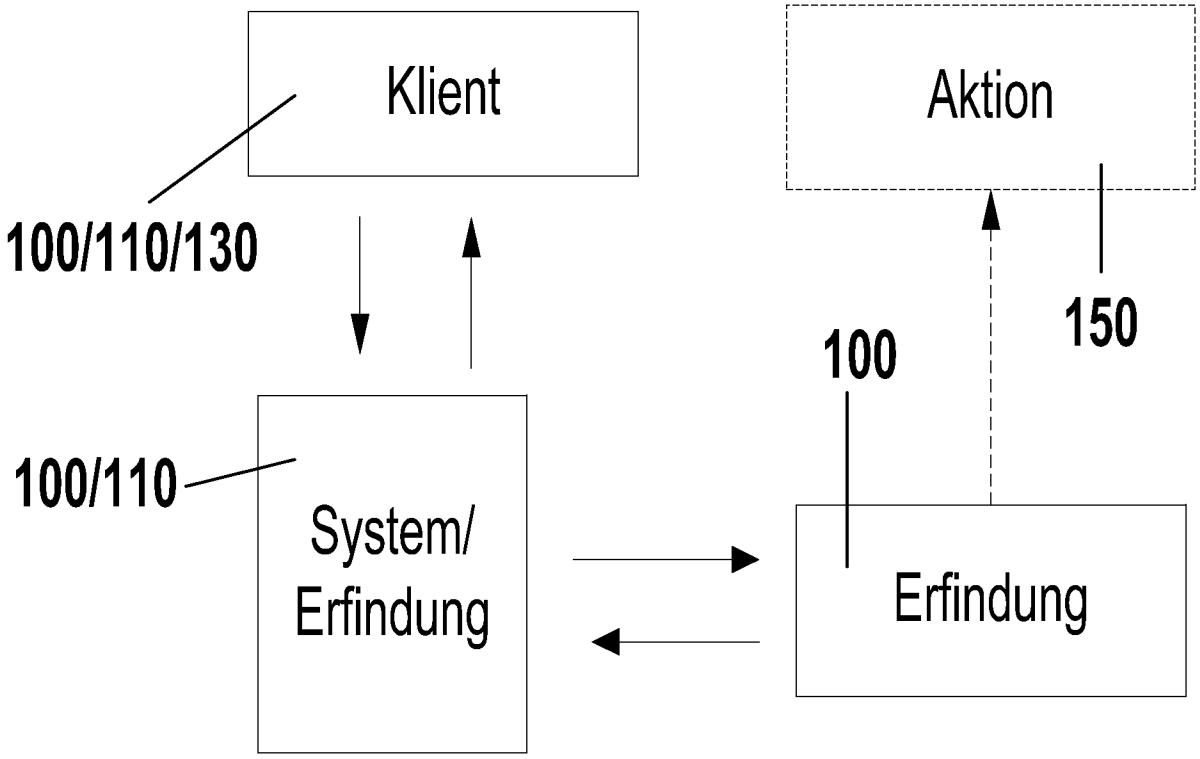

Klient
Aktion
100/110/130
150
100
100/110
System/
Erfindung
Erfindung

Fig. 1e

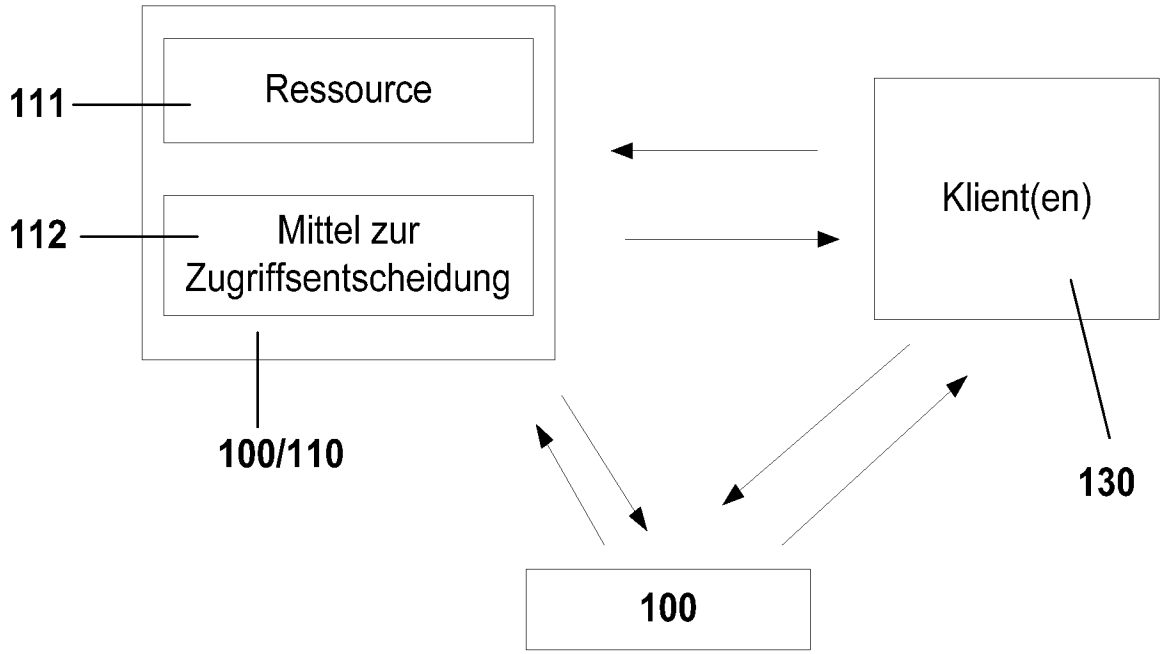

111
Ressource
112
Mittel zur Zugriffsentscheidung
100/110
Klient(en)
130
100

Fig. 1f

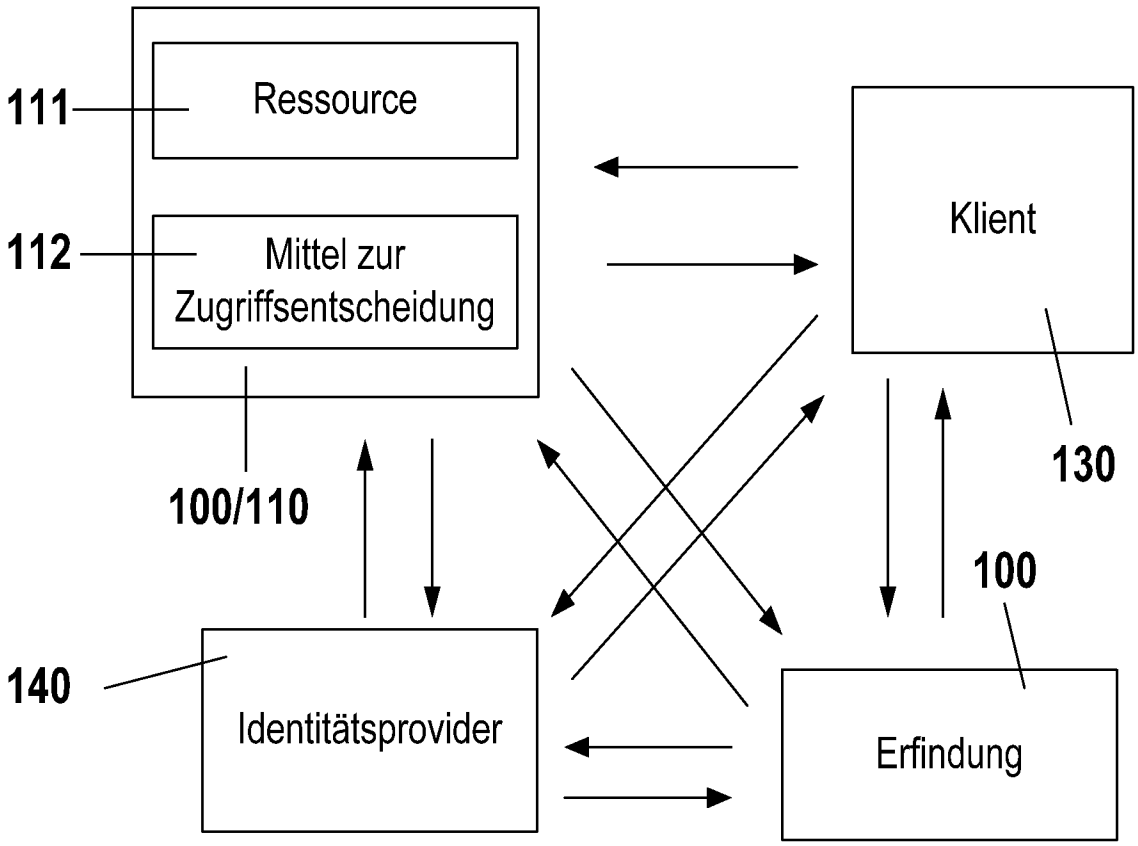

111
Ressource
112
Mittel zur Zugriffsentscheidung
100/110
Klient
130
100
140
Identitätsprovider
Erfindung

Fig. 1g

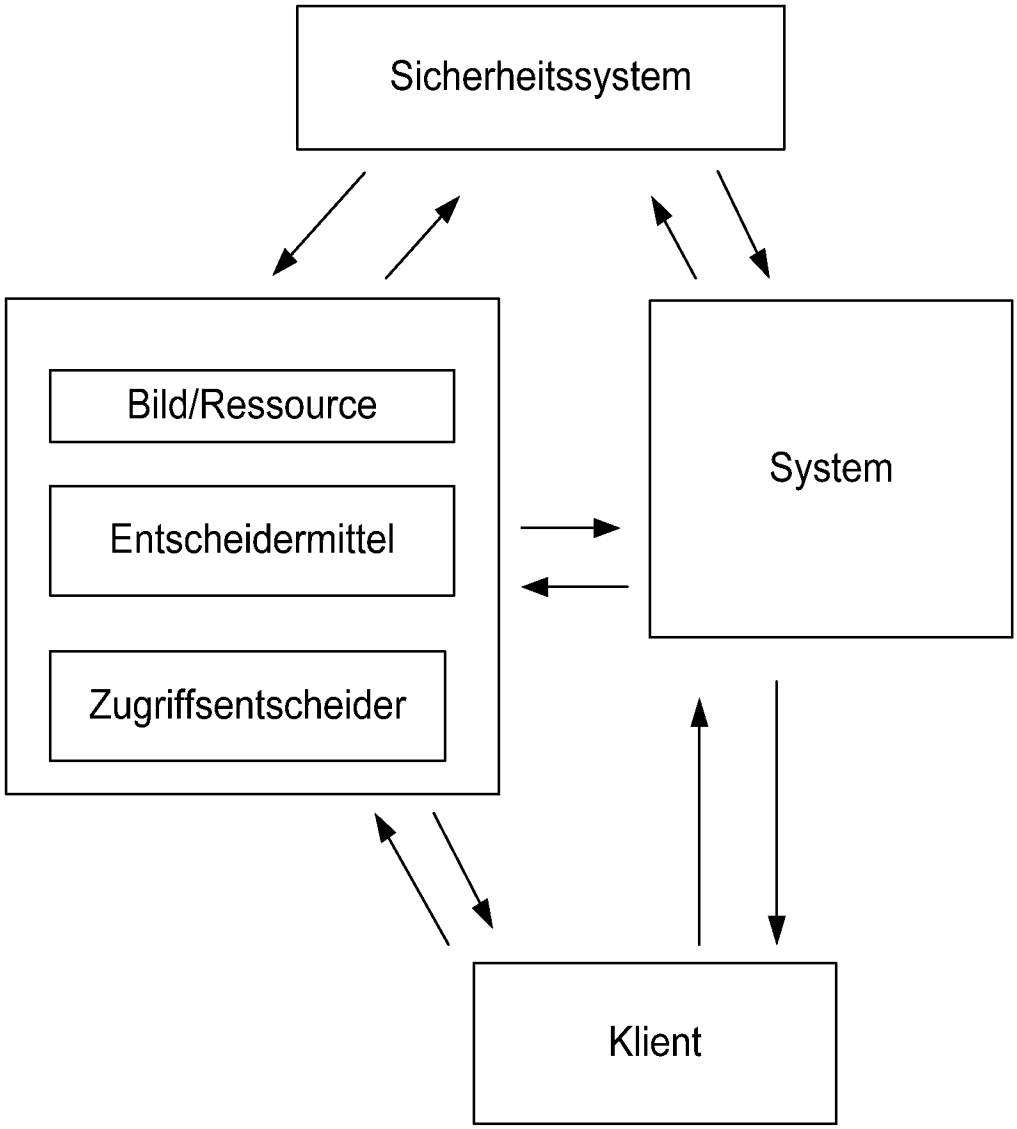

Sicherheitssystem
Bild/Ressource
Entscheidermittel
Zugriffsentscheider
System
Klient

Fig. 2a

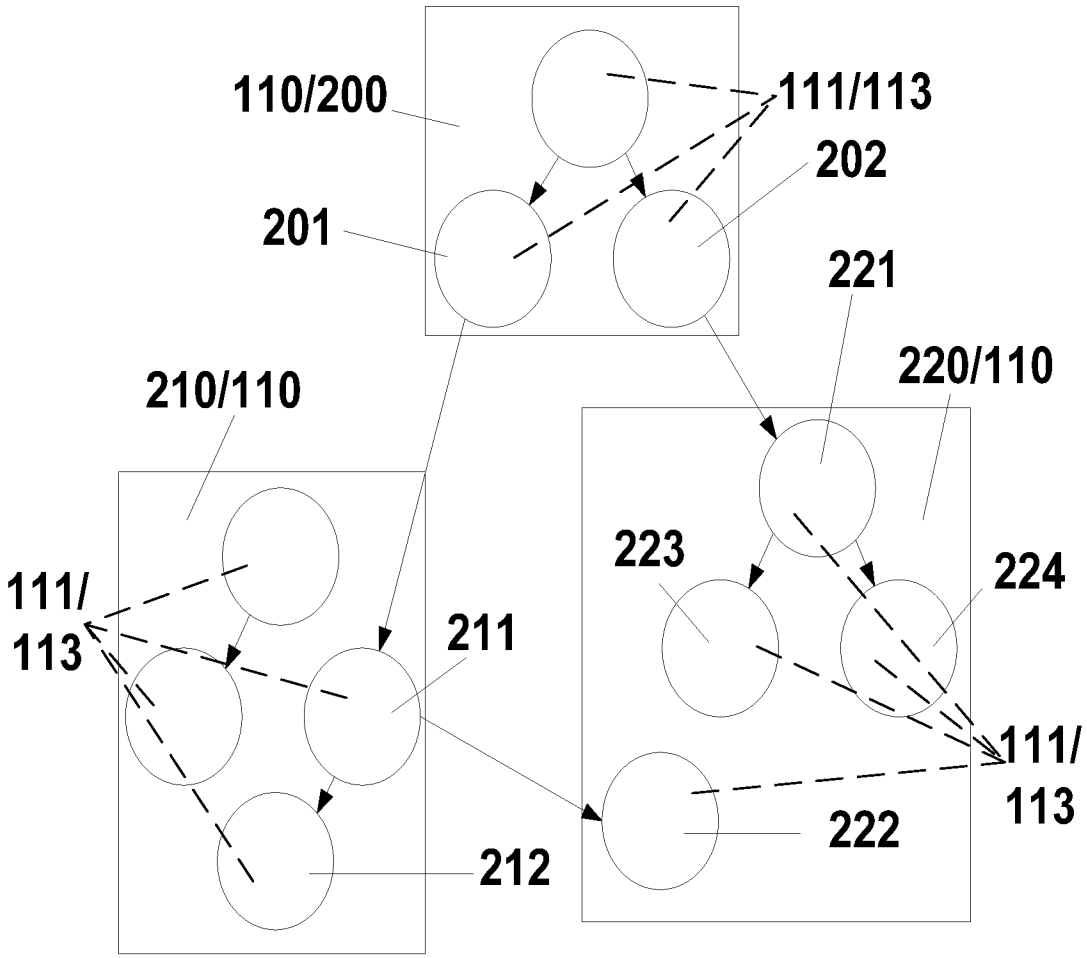

110/200
111/113
202
201
221
220/110
210/110
223
224
111/
113
211
111/
113
222
212

Fig. 2b

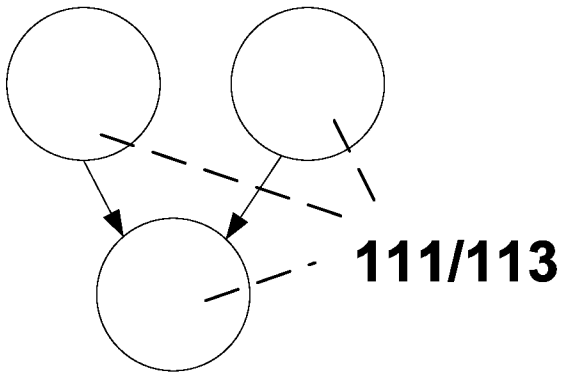

111/113

Fig. 2c

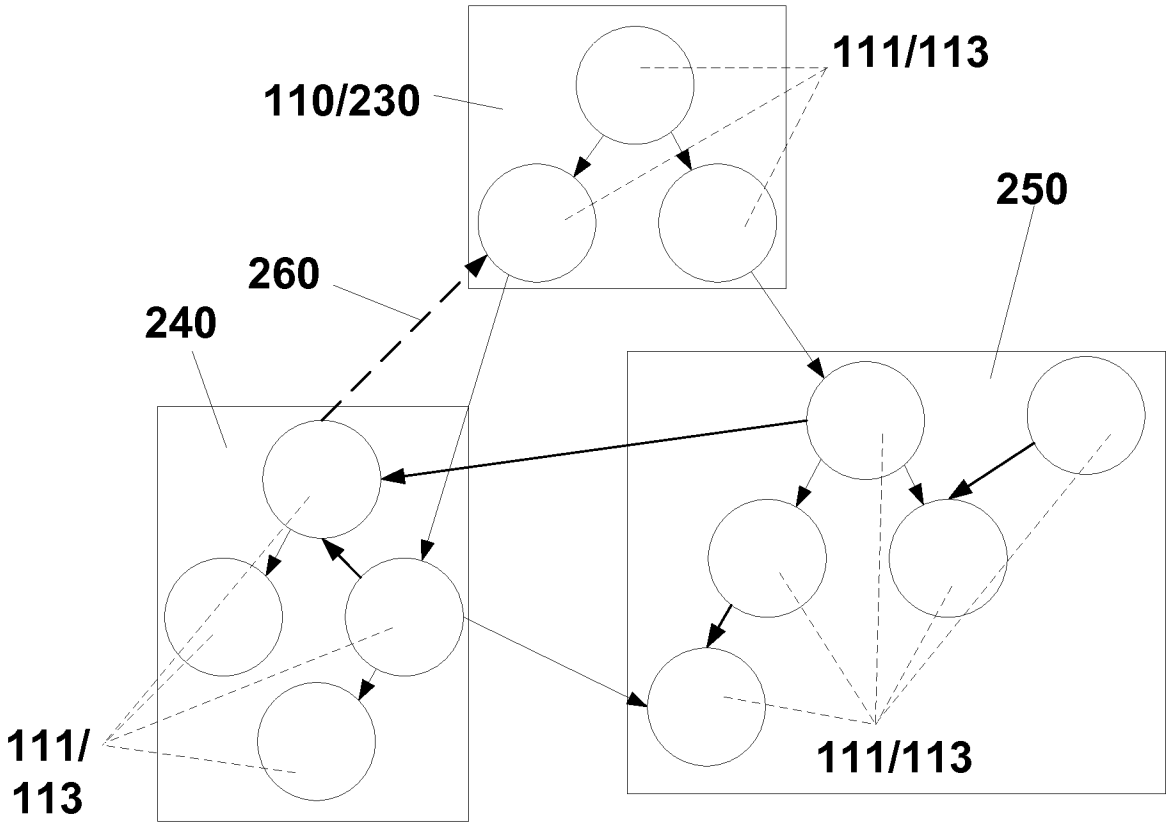


Fig. 3a

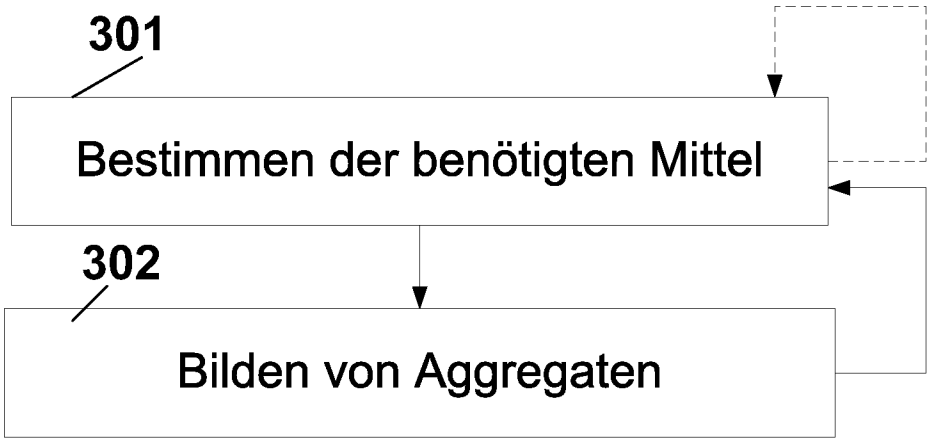


Fig. 3b

Fig. 3c

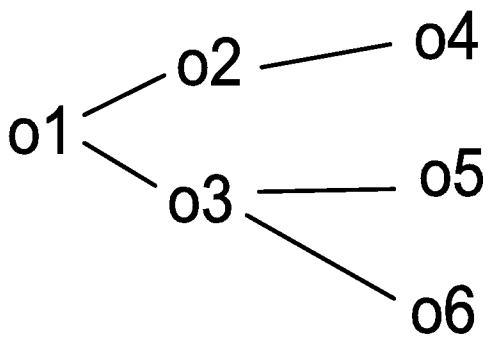

o1
o2
o3
o4
o5
o6

Fig. 3d

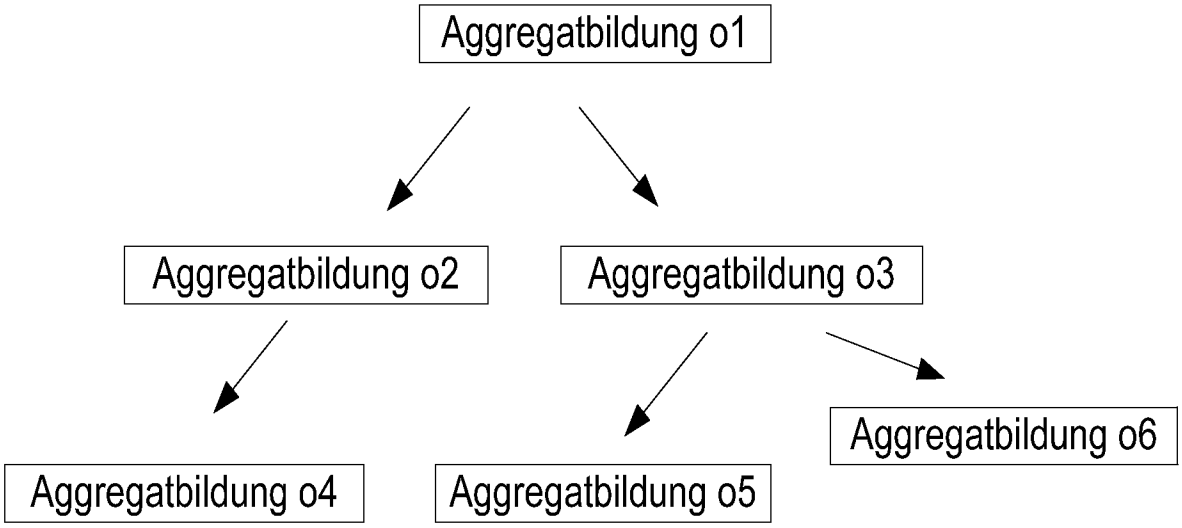

Aggregatbildung o1
Aggregatbildung o2
Aggregatbildung o3
Aggregatbildung o4
Aggregatbildung o5
Aggregatbildung o6

Fig. 4

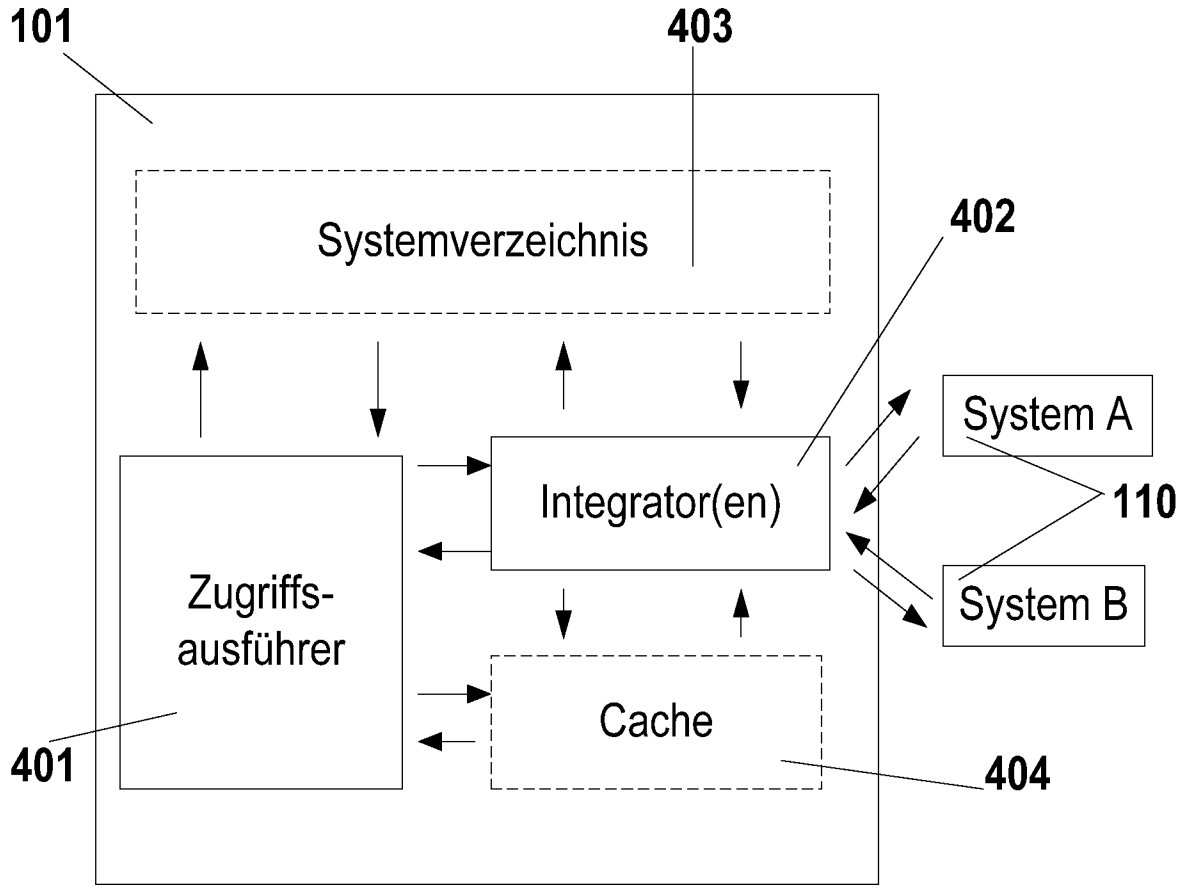
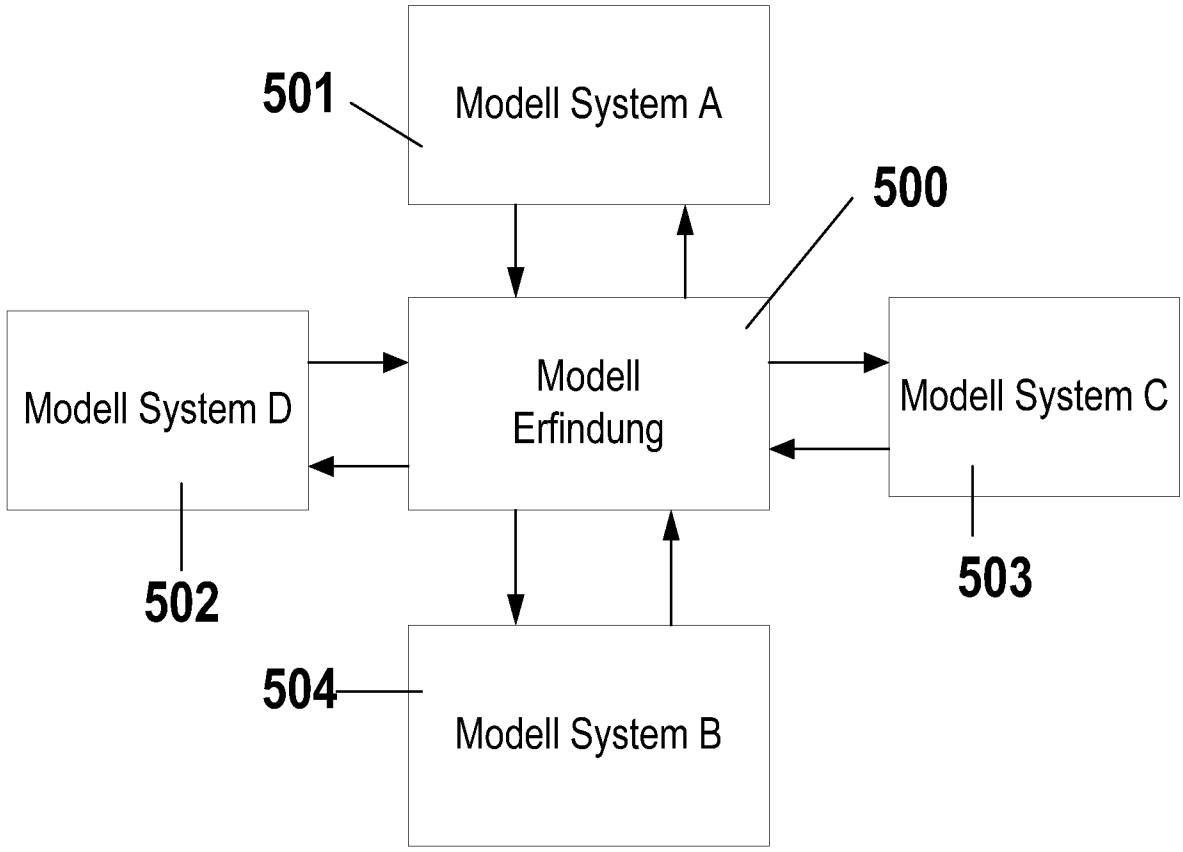

101
403
Systemverzeichnis
402
System A
Integrator(en)
110
Zugriffs-
ausführer
System B
Cache
401
404

Fig.5


501
Modell System A
500
Modell System D
Modell
Erfindung
Modell System C
502
503
504
Modell System B