(19) Deutsches Patent- und Markenamt

(10) **DE 20 2025 101 951 U1** 2025.05.28

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2025 101 951.5**
(22) Anmeldetag: **09.04.2025**
(47) Eintragungstag: **17.04.2025**
(45) Bekanntmachungstag im Patentblatt: **28.05.2025**

(51) Int Cl.: ***G06F 21/31*** (2013.01)

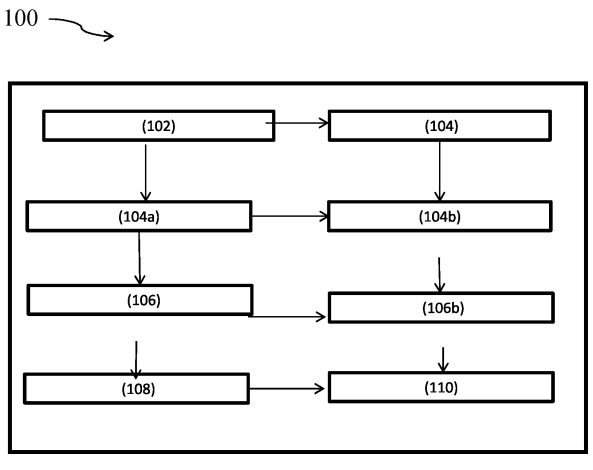
(73) Name und Wohnsitz des Inhabers:
Jasuja, Nimisha, Champaign, IL, US; Thadari, Vishal, Champaign, IL, US

(74) Name und Wohnsitz des Vertreters:
LIPPERT STACHOW Patentanwälte Rechtsanwälte Partnerschaft mbB, 46117 Oberhausen, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **System zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags in Identitätsmanagement-Netzwerken**

(57) Hauptanspruch: Ein System zur adaptiven Multi-Faktor-Authentifizierung unter Verwendung von NFC-Tags in Identitätsmanagementnetzwerken, bestehend aus:
ein NFC-fähiges Authentifizierungsgerät, das als passives Etikett konfiguriert ist, das in eine Smartcard, ein tragbares Gerät oder ein physisches Token eingebettet ist, wobei das Gerät ein sicheres Element zur Speicherung eines kryptografischen Schlüsselpaars und einer eindeutigen Gerätekennung enthält;
ein Endgerät, das ein NFC-Lesemodul, einen kryptografischen Coprozessor, eine biometrische Erfassungsschnittstelle und einen lokalen Steuerprozessor umfasst, der so konfiguriert ist, dass er bei einer Annäherungserkennung innerhalb von 10 Zentimetern ein kryptografisches Challenge-Response-Authentifizierungsprotokoll mit dem NFC-fähigen Authentifizierungsgerät initiiert;
einen Backend-Identitätsverwaltungsserver, der über ein sicheres Kommunikationsnetzwerk mit dem Endgerät verbunden ist, wobei der Server eine kontextbezogene Richtlinien-Engine, ein auf maschinellem Lernen basierendes Risikobewertungsmodul und eine Identitätsföderationsschnittstelle umfasst, wobei das Endgerät beim Empfang einer Antwort auf eine kryptografische Herausforderung, die mit dem im NFC-Gerät eingebetteten privaten Schlüssel signiert ist, diese signierte Antwort, biometrische Daten und kontextbezogene Metadaten einschließlich Zeitstempel, Geolokalisierung des Endgeräts und Gerätevertrauensstufe an den Backend-Identitätsverwaltungsserver überträgt, und wobei der Backend-Identitätsverwaltungsserver eine dynamisch generierte Risikobewertung basierend auf Echtzeit-Verhaltensanalyse, Authentifizierungsverlauf und Kontextdaten auswertet und eine adaptive Authentifizierungsrichtlinie anwendet, die den Zugriff bedingt erlaubt, verweigert oder auf zusätzliche Authentifizierungsfaktoren eskaliert.



Beschreibung

Technisches Gebiet:

[0001] Die vorliegende Offenlegung betrifft den Bereich sicherer Identitätsverwaltungs- und Authentifizierungssysteme und insbesondere ein adaptives Multi-Faktor-Authentifizierungssystem (MFA), das Near-Field-Communication-Tags (NFC) in Verbindung mit kontextsensitiven Richtlinien-Engines in Identitätsverwaltungsnetzwerken nutzt, um Benutzerauthentifizierungsprotokolle in physischen und digitalen Domänen zu verbessern.

Hintergrund:

[0002] Herkömmliche Authentifizierungsmechanismen, die auf statischen Anmeldeinformationen wie Passwörtern basieren, sind anfällig für eine Reihe von Sicherheitslücken, darunter Phishing, Credential Stuffing und Social Engineering. Zwei-Faktor-Authentifizierungssysteme (2FA) bieten zwar zusätzliche Schutzebenen, basieren aber häufig auf SMS- oder softwarebasierten Token, die abgefangen oder gefälscht werden können. Zudem fehlt aktuellen Authentifizierungssystemen die dynamische Anpassung an Kontext und Nutzerverhalten. Es besteht Bedarf an einem sicheren, hardwarebasierten und kontextsensitiven Multi-Faktor-Authentifizierungssystem, das sich nahtlos in bestehende Identitätsmanagement-Frameworks integriert und gleichzeitig reibungslose Benutzerfreundlichkeit und hohe Sicherheit sowohl online als auch offline bietet.

[0003] Die zunehmende Nutzung digitaler Dienste und die Verbreitung vernetzter Geräte haben robuste, sichere und benutzerfreundliche Authentifizierungsmechanismen immer wichtiger gemacht. Identitätsmanagementsysteme bilden das Herzstück dieses Paradigmas und sollen sicherstellen, dass der Zugriff auf digitale und physische Ressourcen nur autorisierten Nutzern gewährt wird. Traditionell ist die gängigste Methode zur Benutzerauthentifizierung die Verwendung von Passwörtern, die als wissensbasierte Anmeldeinformationen dienen. Passwörter weisen jedoch mehrere inhärente Schwächen auf: Sie werden oft dienstübergreifend wiederverwendet, sind leicht zu erraten, anfällig für Brute-Force-Angriffe und Social-Engineering-Taktiken wie Phishing. Dies hat zur Entstehung von Multi-Faktor-Authentifizierungssystemen (MFA) geführt, bei denen Nutzer zwei oder mehr Nachweise vorlegen müssen, um ihre Identität zu bestätigen. Diese Faktoren lassen sich typischerweise in drei Kategorien einteilen: etwas, das der Nutzer weiß (z. B. Passwort oder PIN), etwas, das der Nutzer besitzt (z. B. Token oder Smartphone) und etwas, das der Nutzer ist (z. B. biometrische Kennung).

[0004] Die heute am weitesten verbreiteten MFA-Lösungen umfassen zeitbasierte Einmalkennwörter (TOTP), die über mobile Apps wie Google Authenticator generiert werden, SMS-basierte Verifizierungscodes und Hardware-Token wie RSA SecurID. Diese Ansätze bieten zwar zusätzliche Sicherheit gegenüber einer einfachen passwortbasierten Authentifizierung, sind aber nicht ohne Einschränkungen. SMS-basierte Codes sind beispielsweise anfällig für Man-in-the-Middle-Angriffe, SIM-Swapping und das Abfangen durch bösartige Apps. TOTP-Systeme sind zwar sicherer, hängen aber von der Verfügbarkeit und Integrität des Mobilgeräts ab, was einen Single Point of Failure darstellt. Zudem erfordern beide Methoden, dass Nutzer zum Zeitpunkt der Authentifizierung mit einem Netzwerk verbunden sind oder ein geladenes, betriebsbereites Smartphone besitzen - Einschränkungen, die in Umgebungen mit hohen Sicherheitsanforderungen oder eingeschränkten Ressourcen möglicherweise nicht geeignet sind.

[0005] In jüngerer Zeit haben biometrische Authentifizierungsmethoden - wie Fingerabdruckscan, Gesichtserkennung und Iriserkennung - aufgrund ihrer Benutzerfreundlichkeit und einzigartigen Identifizierungsmöglichkeiten an Bedeutung gewonnen. Biometrische Verfahren bergen jedoch auch Herausforderungen in Bezug auf Datenschutz, Spoofing und Unumkehrbarkeit. Einmal kompromittiert, lässt sich ein biometrischer Identifikator nicht wie ein Passwort ändern. Darüber hinaus können biometrische Systeme aufgrund von Umgebungsbedingungen, Sensorverschleiß oder physiologischen Veränderungen des Benutzers falsch positive oder negative Ergebnisse liefern. Diese Faktoren beeinträchtigen die Zuverlässigkeit, insbesondere in Anwendungsfällen, die eine gleichbleibend hohe Sicherheit erfordern. Zudem kann die zentrale Speicherung biometrischer Daten ein lukratives Ziel für Angreifer werden, was Bedenken hinsichtlich Datenschutzverletzungen und Missbrauch personenbezogener Daten aufkommen lässt.

[0006] Smartcards auf Basis von Public-Key-Infrastrukturen (PKI) sind eine weitere gängige Lösung, insbesondere im Regierungs- und Verteidigungssektor. Diese Karten speichern kryptografische Schlüssel und Benutzerzertifikate, die für sichere Anmeldungen und digitale Signaturen genutzt werden können. Bei ordnungsgemäßem Einsatz bieten sie zwar hohe Sicherheit, ihre Nutzbarkeit ist jedoch durch die Notwendigkeit kompatibler Kartenleser und die Komplexität des Zertifikatslebenszyklusmanagements eingeschränkt. Darüber hinaus können Smartcards verloren gehen, gestohlen oder physisch beschädigt werden, und ihre Akzeptanz im Verbrauchermarkt ist aufgrund ihrer Kosten und der mangelnden Geräte- und Plattformübergreifenden Verwendbarkeit nach wie vor gering.

[0007] Die Near Field Communication (NFC)-Technologie hat sich als vielversprechende Alternative zur Identitätsprüfung etabliert, insbesondere im Zusammenhang mit kontaktlosem Bezahlen und der Interaktion mit mobilen Geräten. NFC-fähige Geräte wie Smartphones und Schlüsselanhänger können über kurze Distanzen mit Lesegeräten kommunizieren und so einen schnellen und sicheren Datenaustausch ermöglichen. Diese Technologie bietet Vorteile wie die Einhaltung der physischen Nähe, die das Risiko von Remote-Angriffen reduziert, die einfache Integration in physische Zugangssysteme und einen minimalen Energiebedarf, insbesondere bei passiven NFC-Tags. In den meisten bestehenden Implementierungen wird NFC jedoch lediglich als einstufiger „Proximity-Token“ verwendet und ist nur unzureichend oder gar nicht in dynamische, kontextsensitive Identitätsmanagement-Frameworks integriert. Diesen NFC-Lösungen fehlt in der Regel die Intelligenz, sich an das Risikoprofil eines Zugriffsversuchs, das Nutzerverhalten oder die Betriebsumgebung anzupassen.

[0008] Herkömmliche Zutrittskontrollsysteme arbeiten zudem mit statischen Richtlinien, deren Authentifizierungsanforderungen vordefiniert sind und sich nicht in Echtzeit anpassen. Beispielsweise kann ein Benutzer beim Betreten einer sicheren Einrichtung einen Ausweis und einen Fingerabdruck vorzeigen müssen, unabhängig von kontextuellen Faktoren wie Zutrittszeitpunkt, bisherigem Vertrauensniveau oder aktuellen Bedrohungsinformationen. Dieses Einheitsmodell führt zu Ineffizienzen: Es kann in Szenarien mit geringem Risiko zu übermäßigem Aufwand führen oder unter Hochrisikobedingungen die Sicherheitsmaßnahmen nicht ausreichend verstärken. Darüber hinaus sind viele Systeme nicht miteinander kompatibel oder nicht erweiterbar, um neue Authentifizierungsmodalitäten oder die Integration mit Risiko-Engines und Identitätsanbietern von Drittanbietern zu unterstützen.

[0009] Es wurden Anstrengungen unternommen, MFA-Systeme durch die Integration risikobasierter Authentifizierungsrahmen (RBA) zu verbessern. Diese Systeme weisen Anmeldeversuchen Risikobewertungen zu, die auf Faktoren wie IP-Adresse, Gerätefingerabdruck, Geolokalisierung und Tageszeitmustern basieren. Basierend auf dem berechneten Risiko gewährt das System den Zugriff, verweigert ihn oder fordert zusätzliche Authentifizierungsschritte an. Dieser adaptive Ansatz stellt zwar einen Fortschritt dar, seine Wirksamkeit wird jedoch häufig durch das Fehlen hochsicherer physischer Token und die Schwierigkeit, Sicherheit und Benutzerfreundlichkeit in Einklang zu bringen, beeinträchtigt. Viele RBA-Systeme arbeiten isoliert und sind schwer zu kalibrieren oder zu prüfen. Zudem hängen sie oft stark vom Browserverhalten der Nutzer oder der Telemetrie mobiler Apps ab, die gefälscht oder manipuliert werden können.

[0010] Angesichts dieser Einschränkungen besteht eine wachsende Nachfrage nach einem System, das die physische Präsenzsicherung durch NFC-Tags mit der Anpassungsfähigkeit risikobewusster Richtlinien-Engines kombiniert. Ein solches System bietet die Vorteile der kontaktlosen Authentifizierung mit passiven NFC-Geräten und passt den Authentifizierungspfad dynamisch an den Umgebungskontext, Verhaltensanalysen und organisatorische Risikoschwellenwerte an. Darüber hinaus sollte es die Integration mit biometrischer Authentifizierung, kryptografischen Protokollen und bestehender Identitätsmanagement-Infrastruktur unterstützen. Idealerweise funktioniert ein solches System sowohl in vernetzten als auch in Offline-Szenarien zuverlässig und bietet Fallback-Mechanismen sowie manipulationssicheren Schutz, der Sicherheit und Ausfallsicherheit gewährleistet.

[0011] Die vorliegende Erfindung schließt diese Lücken durch die Einführung eines Systems zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags innerhalb eines einheitlichen Identitätsmanagement-Netzwerks. Durch die Integration von KI-gestützter Risikobewertung, kryptografischen Challenge-Response-Mechanismen und kontextsensitiven Eskalationsprotokollen reduziert die vorgeschlagene Lösung die Mängel aktueller MFA-Implementierungen und verbessert gleichzeitig das Benutzererlebnis und die Systemintegrität. Diese Innovation ermöglicht eine nahtlose Kombination aus physischer und logischer Sicherheit und ermöglicht es Unternehmen, granulare, situationsspezifische Authentifizierungsrichtlinien zu implementieren, ohne Benutzerprobleme zu verursachen oder die Sicherheit zu beeinträchtigen.

Zusammenfassung:

[0012] Die vorliegende Erfindung offenbart ein System zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags, integriert in ein Identitätsmanagement-Netzwerk, das Verhaltensanalysen, kontextsensitive Richtlinienmodule und Echtzeit-Risikobewertungsmodule umfasst. Das System umfasst ein Benutzerauthentifizierungsgerät mit eingebettetem passivem NFC-Tag, ein dediziertes Leseterminal mit integriertem kryptografischem Verarbeitungsmodul und einen adaptiven Backend-Identitätsmanagement-Server mit kontextbezogener Richtlinien-Engine. Das System passt den Authentifizierungsprozess dynamisch an Standort, Benutzerverhalten, Gerätevertrauensstufe, Zugriffszeitpunkt und Umgebungsparameter an. Es unterstützt die Integration biometrischer und gerätebasierter Authentifizierungsebenen und nutzt kryptografische Challenge-Response-Protokolle

sowie KI-basierte Anomalieerkennung für erhöhte Sicherheit.

[0013] Das Hauptziel der vorliegenden Erfindung ist die Bereitstellung eines fortschrittlichen und adaptiven Multi-Faktor-Authentifizierungssystems (MFA), das Near Field Communication (NFC) nutzt, um die Sicherheit in Identitätsmanagement-Netzwerken zu erhöhen und gleichzeitig Benutzerfreundlichkeit und Betriebseffizienz zu gewährleisten. Ziel dieser Erfindung ist es, die Einschränkungen herkömmlicher Authentifizierungsmechanismen zu überwinden, indem ein sicherer, kontextsensitiver und hardwaregestützter Ansatz eingeführt wird, der sich nahtlos in bestehende Identitätsrahmen integriert. Ein weiteres Ziel der Erfindung ist es, sicherzustellen, dass die Authentifizierung nicht nur mehrschichtig ist, sondern auch dynamisch auf Echtzeit-Risikobewertungen reagiert. Dadurch kann das System die Authentifizierungsanforderungen basierend auf Kontextparametern wie Benutzerverhalten, Zugriffszeit, Standort, Gerätereputation und Umgebungsvariablen intelligent erhöhen oder verringern.

[0014] Ein weiteres Ziel der Erfindung ist die Bereitstellung eines manipulationssicheren, NFC-fähigen physischen Authentifizierungstokens, beispielsweise eines passiven Tags, eingebettet in einen sicheren Personalausweis, ein tragbares Gerät oder einen Schlüsselanhänger. Dieser benötigt keine interne Stromquelle und unterstützt kryptografische Challenge-Response-Protokolle. Das System bietet robusten Schutz vor Klonen, Replay-Angriffen und unbefugtem Zugriff durch die Implementierung von Public-Key-Kryptografie, sicheren Elementen und temporären Sitzungsschlüsseln während des Authentifizierungsaustauschs. Ein weiteres Ziel ist die nahtlose Integration mit biometrischen und gerätebasierten Authentifizierungsmechanismen, wodurch ein mehrschichtiges Authentifizierungsmodell ermöglicht wird, das „etwas, das der Benutzer hat“, „etwas, das der Benutzer weiß“ und „etwas, das der Benutzer ist“ kombiniert.

[0015] Darüber hinaus zielt die Erfindung darauf ab, ein lesegerätintegriertes Terminal oder eine Maschinenstruktur bereitzustellen, die mit NFC-Tags interagieren, biometrische Daten erfassen, lokale kryptografische Operationen durchführen und mit einem zentralen oder verteilten Identitätsserver kommunizieren kann. Diese Terminalstruktur soll sowohl in vernetzten als auch in Offline-Szenarien funktionieren und nutzt Trust Caches, verschlüsselte Gutscheine und Synchronisierungsprotokolle, um die Authentifizierungskontinuität auch in Umgebungen mit Netzwerkstörungen zu gewährleisten. Ein Ziel der Erfindung ist es außerdem, Organisationen die Implementierung anpassbarer, rollen- und attributbasierter Zugriffskontrollrichtlinien zu ermöglichen, die in Echtzeit aktualisiert und dynamisch über die Backend-Richtlinien-Engine durchgesetzt werden können.

[0016] Darüber hinaus zielt die Erfindung darauf ab, föderierte Identitätsarchitekturen zu unterstützen, indem sie sicheren Token-Austausch und Identitätsnachweis mithilfe von Standardprotokollen wie SAML, OAuth2 und OpenID Connect ermöglicht, ohne Kompromisse bei der lokalen Kontexterkennung und Endpunktverifizierung einzugehen. Ein weiteres Ziel ist die Gewährleistung der Interoperabilität über heterogene Plattformen hinweg, sodass das System reibungslos in Unternehmens-IT-Umgebungen, physischen Zugangskontrollsystemen, mobilen Geräten und Cloud-basierten Servicearchitekturen eingesetzt werden kann. Schließlich zielt die Erfindung darauf ab, die Grundsätze des Datenschutzes, der Überprüfbarkeit und der Einhaltung gesetzlicher Vorschriften durch die Integration von Anonymisierungstechniken, sicheren Protokollierungsmechanismen und End-to-End-Verschlüsselung in die Authentifizierungspipeline zu wahren.

KURZBESCHREIBUNG DER FIGUR

[0017] Diese und andere Merkmale, Aspekte und Vorteile der vorliegenden Erfindung werden besser verständlich, wenn man die folgende detaillierte Beschreibung im Zusammenhang mit der beigefügten Zeichnung liest, in der gleiche Zeichen durchgängig gleiche Teile darstellen. Dabei gilt:

> **Fig.** 1 zeigt ein Blockdiagramm eines Systems zur adaptiven Multi-Faktor-Authentifizierung unter Verwendung von NFC-Tags in Identitätsmanagementnetzwerken.

[0018] Fachleute werden außerdem erkennen, dass die Elemente in der Zeichnung der Einfachheit halber dargestellt und nicht unbedingt maßstabsgetreu sind. Beispielsweise veranschaulichen die Flussdiagramme das Verfahren anhand der wichtigsten Schritte, um das Verständnis der Aspekte der vorliegenden Offenbarung zu verbessern. Hinsichtlich der Konstruktion des Geräts können außerdem einzelne oder mehrere Komponenten des Geräts in der Zeichnung durch herkömmliche Symbole dargestellt sein. Die Zeichnung zeigt möglicherweise nur die spezifischen Details, die für das Verständnis der Ausführungsformen der vorliegenden Offenbarung relevant sind, um die Zeichnung nicht durch Details zu überladen, die für Fachleute auf diesem Gebiet nach der vorliegenden Beschreibung ohne weiteres ersichtlich sind.

Detaillierte Beschreibung der Erfindung

[0019] Um das Verständnis der Erfindungsprinzipien zu fördern, wird nun auf die in der Zeichnung dargestellte Ausführungsform Bezug genommen und diese verständlich beschrieben. Der Umfang der

Erfindung wird dadurch jedoch nicht eingeschränkt. Änderungen und weitere Modifikationen des dargestellten Systems sowie weitere Anwendungen der Erfindungsprinzipien sind möglich, wie sie einem Fachmann auf dem Gebiet der Erfindung normalerweise einfallen.

[0020] Für den Fachmann ist klar, dass die vorangegangene allgemeine Beschreibung und die folgende ausführliche Beschreibung beispielhaft und erläuternd für die Erfindung sind und diese nicht einschränken sollen.

[0021] Verweise in dieser Spezifikation auf „einen Aspekt“, „einen anderen Aspekt“ oder ähnliche Formulierungen bedeuten, dass ein bestimmtes Merkmal, eine bestimmte Struktur oder eine bestimmte Eigenschaft, die im Zusammenhang mit der Ausführungsform beschrieben wird, in mindestens einer Ausführungsform der vorliegenden Offenbarung enthalten ist. Daher können sich die Formulierungen „in einer Ausführungsform“, „in einer anderen Ausführungsform“ und ähnliche Formulierungen in dieser Spezifikation auf dieselbe Ausführungsform beziehen, müssen dies aber nicht.

[0022] Die Begriffe „umfasst“, „umfassend“ oder andere Variationen davon sollen eine nicht ausschließliche Einbeziehung abdecken, so dass ein Prozess oder eine Methode, die eine Liste von Schritten umfasst, nicht nur diese Schritte, sondern auch weitere Schritte enthalten kann, die nicht ausdrücklich aufgeführt sind oder diesem Prozess oder dieser Methode innewohnen. Ebenso schließt die Angabe „umfasst ... ein“ für ein oder mehrere Geräte, Subsysteme, Elemente, Strukturen oder Komponenten nicht ohne weitere Einschränkungen die Existenz anderer Geräte, Subsysteme, Elemente, Strukturen, Komponenten oder zusätzlicher Geräte, Subsysteme, Elemente, Strukturen oder Komponenten aus.

[0023] Sofern nicht anders definiert, haben alle hier verwendeten technischen und wissenschaftlichen Begriffe die gleiche Bedeutung, wie sie von einem Fachmann auf dem Gebiet der Erfindung verstanden werden. Die hierin bereitgestellten Systeme, Methoden und Beispiele dienen lediglich der Veranschaulichung und sind nicht als einschränkend zu verstehen.

[0024] Ausführungsformen der vorliegenden Offenbarung werden nachfolgend unter Bezugnahme auf die beigefügte Zeichnung ausführlich beschrieben.

[0025] In **Fig.** 1 ist ein Blockdiagramm eines Systems zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags in Identitätsmanagementnetzwerken dargestellt. Das System 100 umfasst: ein NFC-fähiges Authentifizierungsgerät (102), das als passives Tag konfiguriert und in eine Chipkarte, ein tragbares Gerät oder ein physisches Token eingebettet ist. Das Gerät enthält ein sicheres Element zur Speicherung eines kryptografischen Schlüsselpaars und einer eindeutigen Gerätekennung; ein Endgerät (104), das ein NFC-Lesemodul, einen kryptografischen Coprozessor (104a), eine biometrische Erfassungsschnittstelle (104b) und einen lokalen Steuerprozessor umfasst, der so konfiguriert ist, dass er bei einer Annäherungserkennung innerhalb von 10 Zentimetern ein kryptografisches Challenge-Response-Authentifizierungsprotokoll mit dem NFC-fähigen Authentifizierungsgerät initiiert; einen Backend-Identitätsverwaltungsserver (106), der über ein sicheres Kommunikationsnetzwerk mit dem Endgerät verbunden ist, wobei der Server eine kontextbezogene Richtlinien-Engine (106a), ein auf maschinellem Lernen basierendes Risikobewertungsmodul (106b) und eine Identitätsföderationsschnittstelle umfasst, wobei das Endgerät (108) beim Empfang einer Antwort auf eine kryptografische Herausforderung, die mit dem im NFC-Gerät eingebetteten privaten Schlüssel signiert ist, diese signierte Antwort, biometrische Daten und kontextbezogene Metadaten einschließlich Zeitstempel, Geolokalisierung des Endgeräts und Gerätevertrauensstufe an den Backend-Identitätsverwaltungsserver überträgt, und wobei der Backend-Identitätsverwaltungsserver (110) eine dynamisch generierte Risikobewertung basierend auf Echtzeit-Verhaltensanalyse, Authentifizierungsverlauf und Kontextdaten auswertet und eine adaptive Authentifizierungsrichtlinie anwendet, die den Zugriff bedingt erlaubt, verweigert oder auf zusätzliche Authentifizierungsfaktoren eskaliert.

[0026] In einer Ausführungsform Das kryptografische Challenge-Response-Protokoll (104a), das zwischen dem NFC-fähigen Authentifizierungsgerät und dem Endgerät ausgeführt wird, verwendet die Elliptic Curve Digital Signature Technique (ECDSA) mit Schlüsseln von mindestens 256 Bit Länge und beinhaltet eine auf Nonce basierende zeitliche Randomisierung, um Replay-Angriffe und Session-Fixation zu verhindern.

[0027] In einer Ausführungsform umfasst die Schnittstelle zur biometrischen Erfassung (104b) einen Fingerabdruckscanner mit einer Auflösung von mindestens 500 dpi und einen Mechanismus zur Erkennung lebender Finger unter Verwendung einer kapazitiven Ridge-Pore-Mustererkennung, und wobei die erfasste biometrische Vorlage vor der Übertragung an den Backend-Server unter Verwendung sicherer Schutztechniken für biometrische Vorlagen in einen irreversiblen Hash-Vektor umgewandelt wird.

[0028] In einer Ausführungsform umfasst die kontextbezogene Richtlinien-Engine (106a) des Backend-Servers einen Richtlinienentscheidungspunkt (PDP) und einen Richtliniendurchsetzungs-

punkt (PEP), die so konfiguriert sind, dass sie Regeln für die attributbasierte Zugriffskontrolle (ABAC) in Echtzeit auswerten, wobei die Regeln durch adaptives Lernen aus aktuellen Authentifizierungsmustern über verteilte Terminals hinweg kontinuierlich aktualisiert werden.

[0029] In einer Ausführungsform wird das auf maschinellem Lernen basierende Risikobewertungsmodul (106b) unter Verwendung von föderiertem Lernen von mehreren Endknoten trainiert, und das Modul enthält Ensemblemodelle, die aus einem Random-Forest-Klassifikator und einem rekurrierenden neuronalen Netzwerk (RNN) bestehen, um anomales Verhalten sowohl in zeitlichen als auch in kategorischen Dimensionen der Benutzerinteraktion zu erkennen.

[0030] In einer Ausführungsform umfasst das Endgerät (104) außerdem ein Trusted Platform Module (TPM) und einen sicheren Bootloader, der so konfiguriert ist, dass er die kryptografische Integrität der Firmware des Endgeräts überprüft, bevor er authentifizierungsbezogene Vorgänge zulässt, und der außerdem ein in das PCB-Layout eingebettetes Manipulationsschutznetz umfasst, um bei mechanischer Beeinträchtigung die Sperrung des Endgeräts auszulösen.

[0031] In einer Ausführungsform ist das Endgerät im Falle eines Offline-Betriebs oder eines Verlusts der Netzwerkkonnektivität so konfiguriert, dass es einen lokalen Vertrauenscache verwendet, der zeitlich begrenzte, vom Identitätsverwaltungsserver signierte Authentifizierungsgutscheine enthält, wobei die Gutscheine über eingebettete öffentliche Schlüssel validiert werden und nach einem vordefinierten Zeitfenster oder einer vordefinierten Anzahl von Verwendungen ablaufen.

[0032] In einer Ausführungsform unterstützt der Backend-Identitätsverwaltungsserver (110) eine föderierte Authentifizierung unter Verwendung der Protokolle Security Assertion Markup Language (SAML) und OpenID Connect, wobei Authentifizierungsbehauptungen eine kryptografische Bindung an Sitzungskontextparameter wie Geräteidentitäts-Hash, TLS-Sitzungsschlüssel-Fingerabdruck und biometrischen Übereinstimmungswert umfassen.

[0033] In einer Ausführungsform protokolliert der Backend-Server alle Authentifizierungsversuche mithilfe eines Blockchain-basierten, unveränderlichen Prüfpfads, wobei jeder Protokolleintrag einen SHA-3-512-Hash der Authentifizierungsmetadaten, eine Merkle-Baumwurzel des Benutzerinteraktionsverlaufs und einen Zeitstempel enthält, der mit einer dezentralen Zeitstempelbehörde signiert wurde.

[0034] Das oben beschriebene System zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags in Identitätsmanagement-Netzwerken basiert auf einer eng integrierten Hardware-Software-Architektur, die von einer dynamischen, kontextsensitiven Entscheidungsfindungstechnik gesteuert wird. Der Authentifizierungs-Workflow beginnt im Kern damit, dass ein Benutzer ein NFC-fähiges passives Authentifizierungsgerät - beispielsweise eine Smartcard oder ein sicheres Wearable - mit einem integrierten kryptografischen Sicherheitselement vorlegt. Dieses Sicherheitselement speichert eine eindeutige Gerätekennung und ein elliptisches Kurvenkryptografie-Schlüsselpaar (ECC). Dieses Schlüsselpaar führt bei Annäherungserkennung durch ein Lesegerät ein Challenge-Response-Protokoll aus. Der NFC-Tag arbeitet gemäß ISO/IEC 14443 Typ A mit 13.56 MHz und unterstützt die Kommunikation in einem Radius von 10 cm, um die Exposition zu begrenzen und die Sicherheit zu erhöhen. Sobald der Tag durch das Lesefeld des Terminals aktiviert wird, initiiert er einen sicheren Handshake und empfängt eine einmalige kryptografische Challenge, die mithilfe einer 256-Bit-Elliptic-Curve-Digital-Signature-Technik (ECDSA) und einer im Millisekundenbereich randomisierten Nonce generiert wird. Das sichere Element im Tag signiert die Challenge mit seinem gespeicherten privaten Schlüssel und sendet die signierte Antwort zurück an das Terminal.

[0035] Gleichzeitig validiert das Terminal - ausgestattet mit einem kryptografischen Coprozessor und einem sicheren Bootloader - seine Firmware mithilfe eines Trusted Platform Module (TPM) und stellt die Integrität seiner lokalen Umgebung sicher, bevor es mit der weiteren Verarbeitung fortfährt. Das Terminal verfügt außerdem über eine Schnittstelle zur biometrischen Erfassung, beispielsweise einen kapazitiven Fingerabdruckscanner mit einer Auflösung von 500 dpi, der Live-Finger erkennt und so Spoofing verhindert. Nach erfolgreicher Fingerabdruckerfassung wird das Bild mithilfe eines Einweg-Feature-Extraktors in eine Vorlage umgewandelt und mithilfe einer sicheren biometrischen Vorlagenschutztechnik, wie beispielsweise Fuzzy Vault oder Bloom-Filter-Kodierung, gehasht, um sicherzustellen, dass biometrische Daten nicht rekonstruiert oder missbraucht werden können.

[0036] Das Terminal aggregiert mehrere Eingaben - signierte NFC-Challenge-Response, gehashte biometrische Vorlage und kontextbezogene Metadaten wie Gerätestandort (per GPS oder WLAN-Triangulation), Zeitstempel, Terminalkennung und Gerätezustandsmetriken - und überträgt diese sicher an den Backend-Identitätsmanagementserver. Alle übertragenen Daten werden mit AES-256 im Galois/Counter-Modus (GCM) verschlüsselt, wobei flüchtige Sitzungsschlüssel über Elliptic Curve Diffie-Hellman (ECDH) ausgetauscht werden. Die digitale Signatur

mit HMAC-SHA256 gewährleistet Vertraulichkeit und Integrität.

[0037] Nach Erhalt des Authentifizierungspakets initiiert der Backend-Identitätsmanagementserver seine adaptive Risikobewertung und Richtlinienauswertung. Dieser Server enthält drei Hauptmodule: eine kontextbezogene Richtlinien-Engine, ein maschinenlernbasiertes Risikoanalysemodul und einen föderierten Identitätsbroker. Die Richtlinien-Engine wertet die Zugriffsanforderung anhand eines Regelsatzes aus, der mithilfe eines attributbasierten Zugriffskontrollmodells (ABAC) definiert wurde. Attribute wie Benutzerrolle, Zugriffszeitpunkt, Ressourcensensitivität und aktuelle Bedrohungsstufe werden mit vordefinierten Richtlinien und logischen Ausdrücken in XACML (eXtensible Access Control Markup Language) abgeglichen. Parallel berechnet das Risikoanalysemodul einen Risikowert mithilfe eines mehrschichtigen maschinellen Lernmodells, das mithilfe von föderiertem Lernen über verteilte Terminalknoten trainiert wurde. Dieses Modell ist ein Ensemble aus einem Random-Forest-Klassifikator, der kategorische Attribute wie Zugriffshäufigkeit und Gerätevertrauensstatus verarbeitet, und einem rekurrenten neuronalen Netzwerk (RNN), das zeitliche Korrelationen und Anomalien im Benutzerverhalten erfasst.

[0038] Der föderierte Lernansatz stellt sicher, dass terminalspezifische Modelle regelmäßig synchronisiert und zu einem globalen Modell auf dem Server aggregiert werden, ohne dass Rohdaten der Benutzer übertragen werden. Dadurch wird die Privatsphäre gewahrt. Der vom Modell erstellte Risikowert dient dann als Entscheidungsfaktor innerhalb der kontextbezogenen Richtlinien-Engine. Überschreitet der Risikowert einen vordefinierten Schwellenwert - ein Hinweis auf anomales Verhalten oder ungewöhnliche Zugriffsmuster -, erhöht die Richtlinien-Engine die Authentifizierungsanforderung dynamisch. Diese Erhöhung kann die Hinzuziehung zusätzlicher biometrischer Faktoren wie Gesichtserkennung oder die Aufforderung an den Benutzer umfassen, ein sekundäres NFC-Token vorzulegen, das mit einer anderen Schlüsselhierarchie verknüpft ist. Die Gesichtserkennung wird bei Bedarf mithilfe eines Convolutional Neural Network (CNN) verarbeitet, das Gesichtseinbettungen aus einem Live-Video-Feed extrahiert und sie mit verschlüsselten Vorlagen vergleicht, die mithilfe homomorpher Verschlüsselung gespeichert wurden. So ist ein Vergleich ohne Entschlüsselung möglich.

[0039] Für Szenarien mit Netzwerkstörungen oder Offline-Zugriff ist das Terminal mit einem lokalen Trust Cache ausgestattet, der vorab ausgestellte, zeitlich begrenzte Authentifizierungsgutscheine enthält. Diese Gutscheine werden vom Backend-Server mittels ECDSA kryptografisch signiert und lokal mit dem im TPM gespeicherten öffentlichen Schlüssel des Servers verifiziert. Jeder Gutschein enthält einen Nutzungszähler und einen Ablaufzeitstempel, wodurch sichergestellt wird, dass die Offline-Authentifizierung begrenzt und an Richtlinien gebunden ist. Nach Wiederherstellung der Netzwerkverbindung werden alle offline authentifizierten Sitzungen mit dem Backend synchronisiert und die entsprechenden Prüfprotokolle validiert.

[0040] Der gesamte Authentifizierungsprozess wird in einem unveränderlichen Prüfpfad auf Basis eines privaten Blockchain-Frameworks protokolliert. Jedes Authentifizierungsereignis wird mit SHA-3-512 gehasht, und über einen Stapel solcher Ereignisse wird eine Merkle-Root berechnet. Diese Roots werden anschließend verkettet und von einer dezentralen Zeitstempelstelle signiert, sodass zukünftige Audits sowohl die chronologische Reihenfolge als auch die Integrität verifizieren können. Darüber hinaus unterstützt das Backend die Integration föderierter Identitäten über Security Assertion Markup Language (SAML) und OpenID Connect (OIDC) und stellt digital signierte Assertions mit Sitzungsmetadaten, Kontextkennungen, biometrischen Übereinstimmungsvertrauenswerten und Geräte-Fingerabdruck-Hashes aus. Diese Assertions werden mithilfe von HMACs kryptografisch an die authentifizierte Sitzung gebunden und von den Vertrauensparteien, die die Identitäts-Assertions nutzen, validiert.

[0041] Die Systemtechnik ist grundsätzlich rekursiv und Feedback-basiert. Richtlinienaktualisierungen können durch kumulative Risikobewertungen, Geräteleistungsstatistiken oder vom Administrator definierte globale Ereignisse wie geopolitische Risikowarnungen ausgelöst werden. Sobald neue Verhaltensmuster erkannt werden - ob gutartig oder bösartig -, passt sich das Risikomodell kontinuierlich an, indem es die Merkmalsgewichtung anpasst und Entscheidungsschwellen in Echtzeit aktualisiert. In sensiblen Umgebungen, wie z. B. im Militär oder in hochsicheren Unternehmensumgebungen, ist eine administrative Übersteuerung nur über eine Zwei-Faktor-Aktivierung möglich. Dafür sind sowohl ein physischer Schlüsselschalter als auch ein administrativer NFC-Token mit einer eindeutigen Schlüsselhierarchie und Berechtigungsstufe erforderlich. Übersteuerungsversuche werden als Hochrisikoereignisse behandelt und generieren priorisierte Warnungen im Sicherheits-Dashboard des Servers.

[0042] Die Kombination aus kryptografischer Echtzeitüberprüfung, Verhaltensanalyse, biometrischer Validierung, kontextbezogener Eskalation und föderierter Authentifizierungsorchestrierung - unterstützt durch betriebliche Ausfallsicherheit sowohl online als auch offline - führt zu einem robusten, modularen und adaptiven Authentifizierungssystem, das

moderne Identitätsnetzwerke sowohl im digitalen als auch im physischen Bereich sichern kann.

[0043] Das System besteht aus drei Kernkomponenten: (1) einem NFC-fähigen Authentifizierungsgerät, (2) einer maschinenintegrierten Lesestruktur, die als physischer Zugang oder digitales Gateway-Terminal fungiert, und (3) einem Backend-Identitätsorchestrierungsserver, der mit einer adaptiven Richtliniendurchsetzung auf Basis maschinellen Lernens ausgestattet ist.

[0044] Das NFC-fähige Authentifizierungsgerät ist ein passiver Tag, der in eine Smart-ID-Karte, ein tragbares Gerät oder einen sicheren Schlüsselanhänger eingebettet ist. Dieser Tag speichert eine eindeutige Kennung und ein hardwaregestütztes kryptografisches Schlüsselpaar, das durch ein manipulationssicheres Hardware-Sicherheitselement geschützt ist. Der Tag arbeitet mit einer Frequenz von 13.56 MHz und unterstützt den Kommunikationsstandards ISO/-IEC 14443. Der eingebettete Tag kann nur von autorisierten Terminals im Umkreis von 10 cm gelesen werden und gewährleistet so einen sicheren Punkt-zu-Punkt-Austausch.

[0045] Die leserintegrierte Maschinenstruktur besteht aus einer robusten Terminaleinheit mit einem NFC-Lesemodul, einem kryptografischen Coprozessor, biometrischen Eingabemodulen (z. B. Fingerabdruckscanner oder Gesichtserkennungskamera) und einem lokalen Steuerprozessor. Das Terminal ist mit eingebetteter Firmware ausgestattet, die Challenge-Response-Authentifizierungsprotokolle über die NFC-Schnittstelle ausführen kann. Nach Erhalt der UID und des öffentlichen Schlüssels eines NFC-Tags initiiert das Lesegerät eine kryptografische Abfrage, die mit dem im sicheren Element des NFC-Tags gespeicherten privaten Schlüssel signiert ist. Das Terminal erfasst außerdem biometrische Eingaben und überträgt sowohl die signierte Antwort als auch die biometrische Vorlage zur Multi-Faktor-Verifizierung an den Backend-Server.

[0046] Der Backend-Identitätsverwaltungsserver enthält einen föderierten Authentifizierungsbroker, eine kontextbezogene Richtlinien-Engine und ein maschinenlernbasiertes Risikoanalysemodul. Dieser Server verwaltet eine Datenbank mit registrierten Benutzern, zugehörigen biometrischen Vorlagen, Gerätefingerabdrücken und historischen Verhaltensprofilen. Er bewertet Authentifizierungsversuche dynamisch anhand von Faktoren wie Standort, Zugriffszeitpunkt, früheren Zugriffsmustern und der Vertrauenswürdigkeit des Geräts. Greift ein Benutzer beispielsweise zu einem ungewöhnlichen Zeitpunkt von einem nicht vertrauenswürdigen Gerät auf das System zu, erhöht das System die Authentifizierung, indem es einen zusätzlichen biometrischen Abgleich oder ein dynamisches Einmalkennwort (OTP) anfordert. Die adaptive Richtlinien-Engine generiert in Echtzeit einen Risiko-Score und ruft bedingte Logik auf, um den geeigneten Authentifizierungspfad zu bestimmen - von passiver Authentifizierung bis hin zur vollständigen Multi-Faktor-Eskalation.

[0047] Die NFC-basierte Tag-Terminal-Interaktion nutzt ein Elliptic-Curve-Cryptography-Protokoll (ECC) für den Challenge-Response-Austausch, wobei die Schlüssel regelmäßig über temporäre Sitzungstoken rotiert werden. Alle Datenübertragungen werden mit AES-256 verschlüsselt und mit HMAC-SHA256 signiert, um Datenintegrität und Vertraulichkeit zu gewährleisten. Im Offline-Betrieb verfügt das Terminal über einen begrenzten Trust Cache, der eine bedingte lokale Validierung mithilfe zeitlich begrenzter kryptografischer Gutscheine ermöglicht. Diese Gutscheine werden später mit dem Server synchronisiert, sobald die Verbindung wiederhergestellt ist.

[0048] Darüber hinaus unterstützt das System die rollenbasierte Zugriffskontrolle (RBAC). und attributbasierte Zugriffskontrollmodelle (ABAC) durch die Integration mit Enterprise Identity Management-Frameworks wie LDAP, SAML oder OAuth2-basierten Plattformen. Benutzer können dynamisch bereitgestellt oder entzogen werden, und Authentifizierungsrichtlinien können zentral aktualisiert und an alle Terminals im Netzwerk gesendet werden.

[0049] Das System verfügt außerdem über Manipulationsschutzmechanismen, darunter Hardware-Sicherheitsmodule (HSMs) in Endgeräten, Firmware-Integritätsprüfungen über TPM (Trusted Platform Module) und NFC-Tag-Abschirmung, um unbefugte Scans zu verhindern. Das Endgerätegehäuse ist mit sicheren Gehäusedichtungen und Mesh-Schaltungen ausgestattet, die im Falle einer physischen Manipulation eine Selbstzerstörungslogik auslösen.

[0050] Die Erfindung betrifft sichere Identitäts- und Zugriffsmanagementsysteme und insbesondere adaptive Multi-Faktor-Authentifizierungstechnologien mit NFC (Near Field Communication) zur Benutzerverifizierung im physischen und logischen Zugriffskontext. Sie umfasst die Integration von hardwaregestützter kryptografischer Authentifizierung, biometrischer Erkennung, kontextsensitiven Entscheidungssystemen und Echtzeit-Risikoanalyse in ein einheitliches Framework, das die Zuverlässigkeit, Skalierbarkeit und Intelligenz von Authentifizierungsprozessen verbessert. Die Erfindung ist insbesondere in Bereichen anwendbar, die eine hochsichere Authentifizierung erfordern, wie z. B. Unternehmensinfrastruktur, Behörden, sichere Rechenzentren und föderierte digitale Ökosysteme.

[0051] Die Zeichnung und die vorstehende Beschreibung zeigen Beispiele für Ausführungsformen. Fachleute werden erkennen, dass ein oder mehrere der beschriebenen Elemente durchaus zu einem einzigen Funktionselement kombiniert werden können. Alternativ können bestimmte Elemente in mehrere Funktionselemente aufgeteilt werden. Elemente einer Ausführungsform können einer anderen Ausführungsform hinzugefügt werden. Beispielsweise kann die Reihenfolge der hier beschriebenen Prozesse geändert werden und ist nicht auf die hier beschriebene Weise beschränkt. Darüber hinaus müssen die Aktionen eines Flussdiagramms nicht in der gezeigten Reihenfolge ausgeführt werden; auch müssen nicht alle Aktionen zwingend ausgeführt werden. Auch können Aktionen, die nicht von anderen Aktionen abhängig sind, parallel zu den anderen Aktionen ausgeführt werden. Der Umfang der Ausführungsformen wird durch diese spezifischen Beispiele keineswegs eingeschränkt. Zahlreiche Variationen, ob explizit in der Spezifikation angegeben oder nicht, wie z. B. Unterschiede in Struktur, Abmessungen und Materialverwendung, sind möglich. Der Umfang der Ausführungsformen ist mindestens so breit wie in den folgenden Ansprüchen angegeben.

[0052] Vorteile, weitere Vorzüge und Problemlösungen wurden oben anhand spezifischer Ausführungsformen beschrieben. Die Vorteile, Vorzüge, Problemlösungen und alle Komponenten, die dazu führen können, dass ein Vorteil, Vorteil oder eine Lösung eintritt oder verstärkt wird, sind jedoch nicht als kritische, erforderliche oder wesentliche Merkmale oder Komponenten einzelner oder aller Ansprüche zu verstehen.

REFERENZEN

100	Ein System zur adaptiven Multi-Faktor-Authentifizierung mit NFC-Tags in Identitätsmanagement-Netzwerken.
102	NFC-Fähiges Authentifizierungsgerät
104	Endgeräte
104a	Backend-Identitätsverwaltungsserver
104b	Schnittstelle Zur Biometrischen Erfassung
106	Backend-Identitätsverwaltungsserver
106b	Modul Zur Risikobewertung Auf Basis Maschinellen Lernens
108	Endgeräte
110	Der Backend-Identitätsverwaltungsserver

Schutzansprüche

1. Ein System zur adaptiven Multi-Faktor-Authentifizierung unter Verwendung von NFC-Tags in Identitätsmanagementnetzwerken, bestehend aus:
ein NFC-fähiges Authentifizierungsgerät, das als passives Etikett konfiguriert ist, das in eine Smartcard, ein tragbares Gerät oder ein physisches Token eingebettet ist, wobei das Gerät ein sicheres Element zur Speicherung eines kryptografischen Schlüsselpaars und einer eindeutigen Gerätekennung enthält;
ein Endgerät, das ein NFC-Lesemodul, einen kryptografischen Coprozessor, eine biometrische Erfassungsschnittstelle und einen lokalen Steuerprozessor umfasst, der so konfiguriert ist, dass er bei einer Annäherungserkennung innerhalb von 10 Zentimetern ein kryptografisches Challenge-Response-Authentifizierungsprotokoll mit dem NFC-fähigen Authentifizierungsgerät initiiert;
einen Backend-Identitätsverwaltungsserver, der über ein sicheres Kommunikationsnetzwerk mit dem Endgerät verbunden ist, wobei der Server eine kontextbezogene Richtlinien-Engine, ein auf maschinellem Lernen basierendes Risikobewertungsmodul und eine Identitätsföderationsschnittstelle umfasst, wobei das Endgerät beim Empfang einer Antwort auf eine kryptografische Herausforderung, die mit dem im NFC-Gerät eingebetteten privaten Schlüssel signiert ist, diese signierte Antwort, biometrische Daten und kontextbezogene Metadaten einschließlich Zeitstempel, Geolokalisierung des Endgeräts und Gerätevertrauensstufe an den Backend-Identitätsverwaltungsserver überträgt, und wobei der Backend-Identitätsverwaltungsserver eine dynamisch generierte Risikobewertung basierend auf Echtzeit-Verhaltensanalyse, Authentifizierungsverlauf und Kontextdaten auswertet und eine adaptive Authentifizierungsrichtlinie anwendet, die den Zugriff bedingt erlaubt, verweigert oder auf zusätzliche Authentifizierungsfaktoren eskaliert.

2. System gemäß Anspruch 1, wobei das zwischen dem NFC-fähigen Authentifizierungsgerät und dem Endgerät ausgeführte kryptografische Challenge-Response-Protokoll die Technik der digitalen Signatur mit elliptischen Kurven (ECDSA) mit Schlüsseln von mindestens 256 Bit Länge verwendet und wobei das Protokoll eine auf Nonce basierende zeitliche Randomisierung beinhaltet, um Replay-Angriffe und Sitzungsmanipulation zu verhindern.

3. System gemäß Anspruch 1, wobei die Schnittstelle zur biometrischen Erfassung einen Fingerabdruckscanner mit einer Auflösung von mindestens 500 dpi und einen Mechanismus zur Erkennung lebender Finger unter Verwendung einer kapazitiven Ridge-Pore-Mustererkennung umfasst und wobei

die erfasste biometrische Vorlage vor der Übertragung an den Backend-Server unter Verwendung sicherer Schutztechniken für biometrische Vorlagen in einen irreversiblen Hash-Vektor umgewandelt wird.

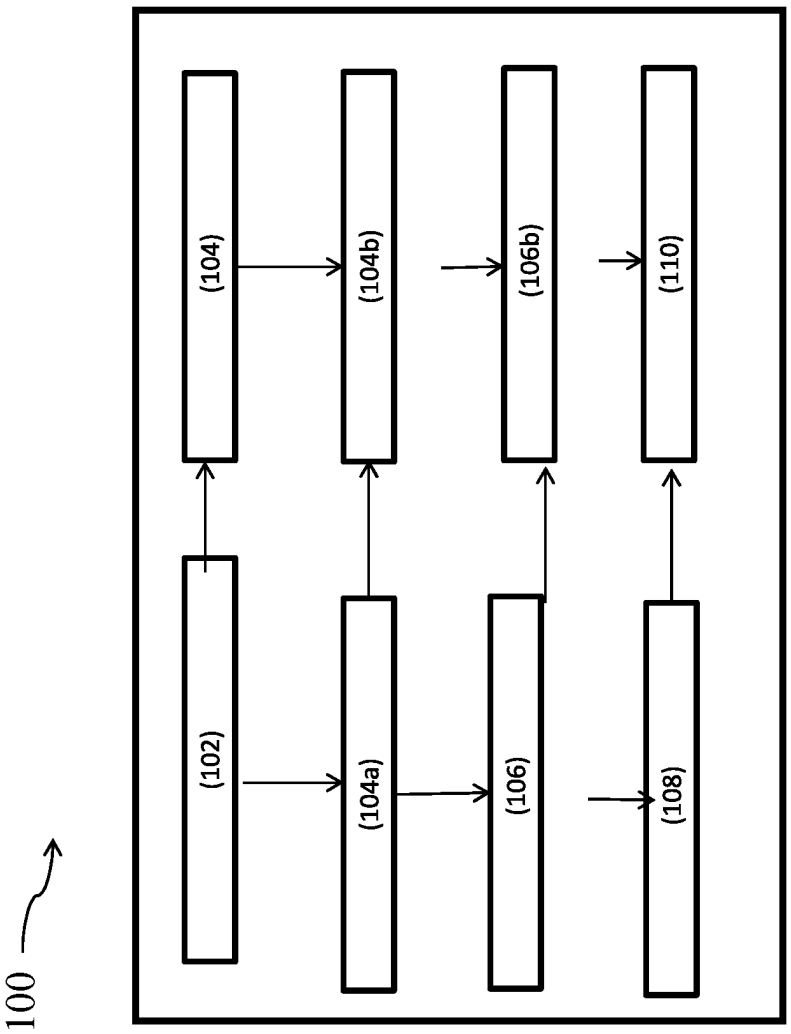
4. System gemäß Anspruch 1, wobei das auf maschinellem Lernen basierende Risikobewertungsmodul unter Verwendung von föderiertem Lernen von mehreren Endknoten trainiert wird und wobei das Modul Ensemblemodelle enthält, die aus einem Random-Forest-Klassifikator und einem rekurrierenden neuronalen Netzwerk (RNN) bestehen, um anomales Verhalten sowohl in zeitlichen als auch in kategorischen Dimensionen der Benutzerinteraktion zu erkennen.

5. System gemäß Anspruch 1, wobei das Endgerät außerdem ein Trusted Platform Module (TPM) und einen sicheren Bootloader umfasst, der so konfiguriert ist, dass er die kryptografische Integrität der Terminal-Firmware überprüft, bevor er authentifizierungsbezogene Vorgänge zulässt, und der außerdem ein in das PCB-Layout eingebettetes Manipulationsschutznetz umfasst, um bei mechanischer Beeinträchtigung die Terminalsperre auszulösen.

6. System gemäß Anspruch 1, wobei das Endgerät im Falle eines Offline-Betriebs oder eines Verlusts der Netzwerkkonnektivität so konfiguriert ist, dass es einen lokalen Vertrauenscache verwendet, der zeitlich begrenzte, vom Identitätsverwaltungsserver signierte Authentifizierungsgutscheine enthält, wobei die Gutscheine über eingebettete öffentliche Schlüssel validiert werden und nach einem vordefinierten Zeitfenster oder einer vordefinierten Anzahl von Verwendungen ablaufen.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen



Figur 1

 Das Dokument wurde durch die Firma Luminess hergestellt.