La Evolución de la Gestión de Identidad (IAM) en la Seguridad de la Información

The Evolution of Identity Management (IAM) in Information Security

Andres Benjamin Rojas Alza, Bryan Anthony Sauñe Huaman

Universidad Nacional de Trujillo, Trujillo, Perú.

Resumen

El artículo presentado a continuación es una revisión sistemática de la evolución de la Gestión de identidades y accesos (IAM) en el ámbito de la Seguridad de la Información. La investigación realizada proporciona una visión integral de cómo la IAM ha evolucionado a lo largo de las décadas, adaptándose constantemente a los cambios en el panorama tecnológico y a las amenazas en constante evolución. Se ha organizado la información en secciones que abordan cada etapa importante en la evolución de la IAM, destacando hitos significativos, avances tecnológicos y desafíos superados. Además, se identifican tendencias emergentes y se ofrece una síntesis de las tendencias actuales y futuras en la Gestión de Identidades y Accesos. También se implementó conceptos de tecnologías de seguridad de la información tales como los distintos tipos de autenticaciones incluyendo el multifactor (MFA), gestión de privilegios, single sign-on (SSO) y el uso biometría y la inteligencia artificial. Todo esto para realizar un análisis cualitativo en la UX (User experience) y las implementaciones finales en diversos sistemas especializados

Palabras Claves: Gestión de identidades y accesos, gestión de identidades, seguridad de la información, autenticación.

Abstract

The article presented below is a systematic review of the evolution of Identity and Access Management (IAM) in the field of Information Security. The research conducted provides a comprehensive view of how IAM has evolved over the decades, constantly adapting to changes in the technological landscape and evolving threats. The information has been organized into sections that address each major stage in the evolution of IAM, highlighting significant milestones, technological advances and challenges overcome. In addition, emerging trends are identified and a synthesis of current and future trends in Identity and Access Management is provided. It also implemented information security technology concepts such as different types of authentications including multi-factor authentication (MFA), privilege management, single sign-on (SSO) and the use of biometrics and artificial intelligence. All this to perform a qualitative analysis on the UX (User experience) and final implementations in various specialized systems.

Keywords: Identity and access management, identity management, information security, authentication.

INTRODUCCIÓN

En un mundo cada vez más interconectado y digitalizado, la seguridad de la información se ha convertido en un componente crítico para salvaguardar los activos empresariales y proteger la privacidad de los individuos. La Gestión de Identidades y Accesos (IAM) emerge como un pilar fundamental en la estrategia de seguridad de las organizaciones, proporcionando un marco integral para administrar y controlar el acceso a los recursos digitales.

La IAM ha experimentado una notable evolución a lo largo de las décadas, adaptándose constantemente a los cambios en el panorama tecnológico y a las amenazas en constante evolución. Este artículo de revisión sistemática se propone explorar y analizar esta evolución, trazando un recorrido desde los primeros sistemas de autenticación hasta las soluciones de IAM más avanzadas de la actualidad.

La historia de la IAM está marcada por una transición desde soluciones de autenticación rudimentarias, como contraseñas y tokens físicos, hacia enfoques más sofisticados, que incluyen autenticación multifactor (MFA), gestión de privilegios, single sign-on (SSO) y el uso de tecnologías emergentes como la biometría y la inteligencia artificial. Además, la IAM se ha expandido más allá de las fronteras de las organizaciones, abarcando aplicaciones en la nube, dispositivos móviles y entornos de Internet de las cosas (IoT).

Este artículo también examinará los desafíos que han surgido a medida que la IAM se ha vuelto más compleja y se ha expandido a través de diversas plataformas y sistemas. La gestión de identidades y accesos no solo es esencial para garantizar la seguridad, sino que también juega un papel fundamental en la usabilidad y la experiencia del usuario. Por lo tanto, abordaremos cómo se equilibra la seguridad con la comodidad y la eficiencia en la IAM moderna.

A lo largo de esta revisión sistemática, se analizarán estudios y desarrollos clave en la evolución de la IAM, se identificarán tendencias emergentes y se ofrecerá una visión integral de cómo la IAM continúa desempeñando un papel crucial en la protección de la información en la era digital.

Este artículo se organizará en secciones que abordarán cada etapa importante en la evolución de la IAM, destacando hitos significativos, avances tecnológicos y desafíos superados. Al finalizar, se presentará una síntesis de las tendencias actuales y futuras en la Gestión de Identidades y Accesos, proporcionando una visión completa de su importancia continua en la seguridad de la información.

MATERIAL Y MÉTODOS

En orden de llevar a cabo esta revisión bibliográfica, se realizó una exhaustiva búsqueda de literatura científica y técnica relacionada con la evolución de la Gestión de Identidades y Accesos (IAM) en el ámbito de la Seguridad de la Información. Se aplicaron Se utilizaron bases de datos académicas de renombre, como IEEE Xplore, Elsevier, Science Direct, ResearchGate, Scielo y Repositorios de Investigación de diversas instituciones académicas para recopilar los artículos relevantes. Se establecieron los siguientes criterios de inclusión para la selección de fuentes:

1. **Relevancia Temática:** Los artículos seleccionados debían abordar aspectos relacionados con la IAM, incluyendo autenticación, autorización, gestión de accesos, control de privilegios y seguridad de la información.

2. **Fecha de Publicación:** Se consideraron en su mayoría, artículos publicados en los últimos 5 años, desde el año 2018 hasta la fecha actual. Sin embargo, con el objetivo de abarcar el marco completo de la evolución de la IAM se tomó en cuenta investigaciones de fechas anteriores.

3. **Calidad de la Fuente:** Se dieron preferencia a artículos revisados por pares, libros académicos y documentos técnicos de organizaciones reconocidas en tópicos de tecnologías.

Bases de datos	N° de artículos
IEE Xplore	8
Elsevier	15
Science Direct	16
ResearchGate	9
Scielo	5
Repositorios de investigación	12
TOTAL	**65**

Tabla 1. Números de artículos encontrados en bases de datos

Búsqueda y recopilación de datos:

Al realizar las búsquedas con operadores booleanos estandarizados tales como “AND”, “OR”, “NOT”, “-”. Se aplico filtros de búsqueda en el área de Ciencias de la Computación para obtener un total de 2532 investigaciones científicas en la base de datos académica interdependiente Scopus para así someter los resultados a un análisis bibliométrico utilizando el software VOSViewer en su última versión de v.1.6.19. Obteniendo así una visualización de calor basada en la densidad del número de artículos obtenidos agrupados por palabras claves con iteraciones superiores a las 5 veces, dicha vista se presenta de la siguiente manera:

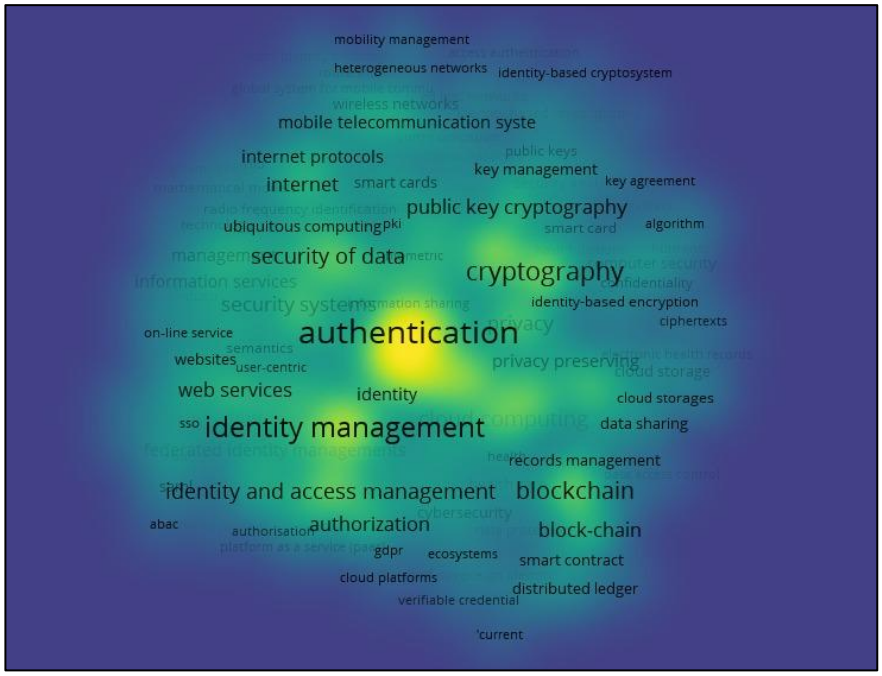

Figura 1. Diagrama de calor por densidad de palabras claves

De igual manera, se genera un mapa de redes bibliométricas para evaluar las relaciones y contenido de información altamente registrado en las bases de datos. El cual se presenta a continuación:

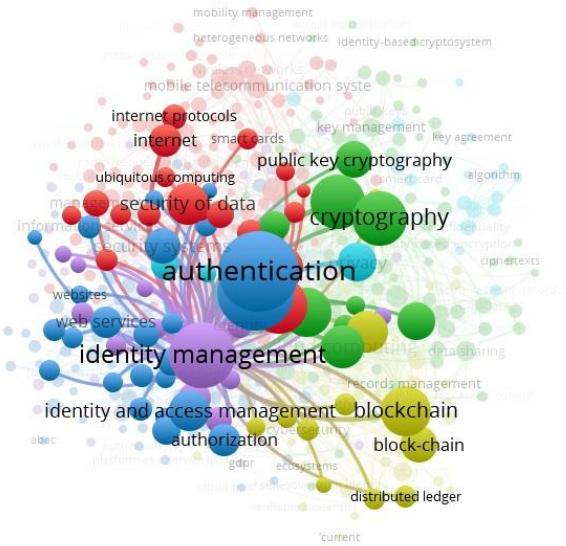

Figura 2. Mapa de redes bibliométricas

Concluyendo así en el uso de palabras claves principales tales como: Autenticación, gestión de identidades, gestión de identidades y accesos, autorización y seguridad de datos. Las cuáles serán tomadas en cuenta para el proceso de selección de artículos y su análisis respectivo en posteriores marcos de referencias.

Proceso de Selección y Análisis:

Los artículos inicialmente identificados a través de las bases de datos se sometieron a un proceso de selección en dos etapas. En la primera etapa, se revisaron los títulos y resúmenes de los artículos para determinar su relevancia con respecto a la temática de IAM y su evolución. Aquellos artículos que no cumplían con los criterios de inclusión fueron excluidos.

En la segunda etapa, se realizó una revisión más detallada de los artículos seleccionados en la etapa anterior. Se evaluaron los contenidos completos de estos 65 artículos para recopilar información detallada sobre el marco de referencias de la Seguridad en la información y su avance de la calidad en diferentes ámbitos empresariales, aplicaciones e implementaciones en sistemas de información y estudios de focalización a lo largo del tiempo, destacando los hitos clave, avances tecnológicos y desafíos superados en cada etapa

Limitaciones:

Es importante mencionar que esta revisión sistemática se basa en la disponibilidad de literatura académica y técnica. Puede haber desarrollos y tendencias adicionales en la IAM que no estén representados en esta revisión debido a limitaciones de acceso a fuentes de información específicas.

1 Resultados y discusión

La gestión de identidades y accesos (IAM) comprende los procesos organizativos y técnicos que involucran el registro y la autorización de derechos de acceso durante la fase de configuración, seguidos por la fase de operación que se centra en identificar, autenticar y controlar a individuos o grupos para acceder a aplicaciones, sistemas o redes, basándose en los derechos de acceso previamente autorizados. Este proceso abarca la información sobre usuarios en computadoras, incluyendo datos de autenticación e información que describe las acciones y datos a los que están autorizados. La gestión de identidades también implica el manejo de información descriptiva sobre el usuario y las restricciones sobre cómo y por quién puede accederse y modificarse esa información. Además de usuarios, las entidades gestionadas suelen incluir recursos de hardware, redes e incluso aplicaciones. La relación entre las fases de configuración y operación en IAM, así como la distinción entre la gestión de identidades y la gestión de acceso, se ilustra en el diagrama adjunto Josang (2017):

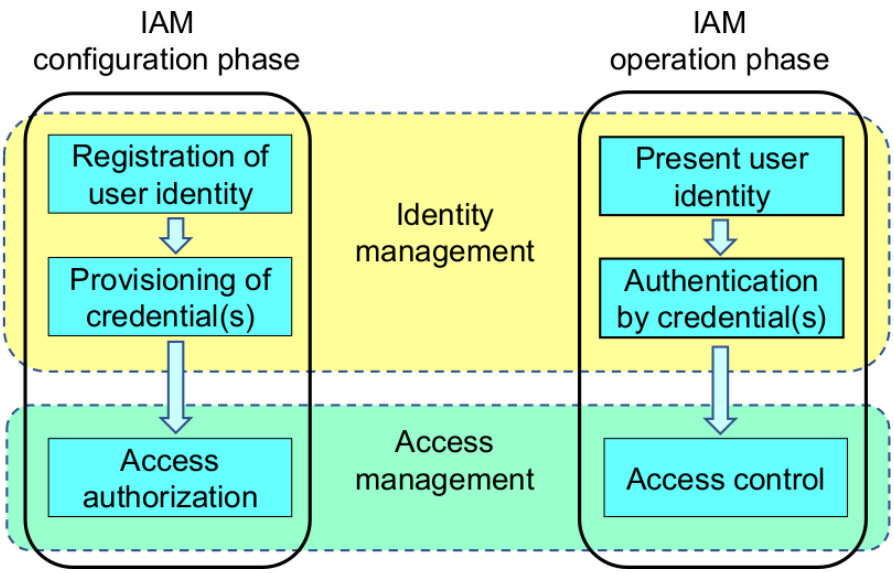

Figura 3. Fases de la Gestión de identidades y accesos. Fuente: Josang (2017)

Se presenta según las principales concesiones en la investigación que, en el contexto real de la Ingeniería, la gestión de identidades puede implicar cinco funciones básicas:

1. La función de identidad pura: Creación, gestión y supresión de identidades sin tener en cuenta el acceso o los derechos.
2. La función de acceso del usuario (log-on): Por ejemplo: una tarjeta inteligente y sus datos asociados utilizados por un cliente para iniciar sesión en un servicio o servicios (una visión tradicional).
3. La función de servicio: Un sistema que ofrece servicios personalizados, basados en roles, en línea, bajo demanda, multimedia (contenido) y basados en la presencia a los usuarios y sus dispositivos.
4. Federación de identidades: Un sistema que se basa en la identidad federada para autenticar a un usuario sin conocer su contraseña.
5. Función de auditoría: Supervisa los cuellos de botella, los fallos de funcionamiento y los comportamientos sospechosos.

Historia de la IAM:

En sus inicios, el Protocolo Ligero de Acceso a Directorios (LDAP) estableció un estándar abierto para el acceso a datos en servidores, dando origen a la administración de identidad corporativa con la introducción de Active Directory en Windows 2000 Server en 1999.

Active Directory Federation Services, lanzado en 2003, permitió el inicio de sesión único a través de Active Directory, marcando el inicio de la década de 2000 como una era donde las contraseñas eran la principal forma de autenticación.

A principios de la década de 2010, surgieron nuevas tecnologías como SAML 2.0 y OpenID Connect, facilitando el inicio de sesión único. Empresas como Okta y Ping Identity innovaron

para asegurar aplicaciones en la nube, y la Alianza FIDO (2013) promovió estándares de autenticación para reducir la dependencia de contraseñas.

Aunque MFA (autenticación multifactor) aumentó su uso, persistió la debilidad en la autenticación. A finales de la década, se diversificaron los tipos de factores, desde OTP hasta biometría. Aunque algunas aplicaciones adoptaron MFA, su uso generalizado aún era limitado.

En su estudio, Frederiksen et al. (2020) analizaron una variedad de estrategias de Gestión de Identidad y Acceso (IAM), que abarcan desde certificados X.509 hasta proveedores de identidad en línea, pasando por el inicio de sesión único (SSO), credenciales basadas en atributos para mejorar la privacidad (P-ABCs) y la gestión de identidad federada (FIM). Cada una de estas estrategias presenta sus propias ventajas y desventajas, y la elección de una estrategia de IAM depende en última instancia de los requisitos específicos de seguridad y privacidad de la organización.

Además, Frederiksen et al. (2020) identificaron un desafío fundamental en la mayoría de estas estrategias de IAM: la necesidad de confiar en terceras entidades. Este elemento puede introducir un riesgo significativo para la seguridad si alguna de estas entidades resulta comprometida. Además, se destaca la cuestión de la gestión de múltiples credenciales por parte de los usuarios como una posible carga adicional. Por ejemplo, los Certificados X.509 proporcionan una sólida capacidad de firma digital, aunque su uso puede ser complicado, mientras que los Proveedores de Identidad en Línea (IdPs) son convenientes, pero requieren una confianza absoluta en su integridad. El Inicio de Sesión Único (SSO) resuelve problemas de seguridad relacionados con contraseñas, pero sigue dependiendo de un IdP de confianza, y las Credenciales Basadas en Atributos (P-ABCs) brindan un alto nivel de privacidad, aunque requieren que terceros emitan las credenciales. La Gestión de Identidad Federada (FIM) simplifica el intercambio de información de identidad entre organizaciones, pero también plantea desafíos relacionados con la confianza y la complejidad que pueden dar lugar a vulnerabilidades de seguridad.

El trabajo de Alsirhani et al. (2021) resulta esencial. Ofrecen una revisión minuciosa sobre los servicios y amenazas en la seguridad de IAM en la nube, proponiendo marcos avanzados que brindan sólidos mecanismos de autenticación en entornos de nube pública y privada. Además,

presentan un algoritmo de autenticación basado en Identity-as-a-Service (IdaaS) y un modelo de amenazas que evalúa la eficacia de estos marcos.

Completando el trabajo propuesto en las amenazas mencionados Hovav, A., & Berger, R. (2009) distinguieron esas amenazas para comprobar el trabajo previo adaptado de Whitman y Mattord en 2005, donde revela el tiempo promedio en decodificar contraseñas en las credenciales de los accesos en los sistemas de gestión de identidades.

Número de caracteres en la contraseña	**Tiempo estimado en decodificar – caracteres en minúsculas**	**Tiempo estimado en decodificar – caracteres en minúsculas y mayúsculas**
4	2.7 segundos	9.5 segundos
5	3 minutos y 2 segundos	15 minutos y 17 segundos
6	3 horas y 26 minutos	23 horas, 57 minutos y 14 segundos
7	9 días, 17 horas y 26 minutos	3 meses, 3 días y 19 horas
8	1 año, 10 meses y 1 día	24 años y 6 meses

Tabla 2. Tiempo estimado en decodificar contraseñas. Fuente: Hovav y Berger (2009).

La literatura sobre IAM en la nube resalta la vital importancia de la autenticación y autorización para proteger los datos de los usuarios. Alsirhani et al. (2021) proponen un algoritmo de autenticación IdaaS basado en técnicas avanzadas de criptografía, fortaleciendo la seguridad en la nube. Además, sugieren medidas para abordar los retos de seguridad en IAM, como proveedores de identidad resistentes a intrusiones y la centralización de la gestión de identidad y acceso. Sin embargo, persisten desafíos, como las amenazas a la privacidad y el robo de datos.

Carnley y Kettani (2019) exploran cómo la tecnología blockchain puede fortalecer la Gestión de Identidad y Acceso (IAM) en el contexto de dispositivos IoT. Esto incluye una base de datos

segura, la capacidad de compartir datos y transacciones seguras. La tecnología blockchain también mejora la transparencia y la confiabilidad en IAM, crucial en el entorno en crecimiento de IoT.

En este contexto, es crucial comprender conceptos como autenticación, autorización y PKI, así como la influencia de la computación en la nube en la gestión de datos. Además, la criptografía, la comunicación cercana y la tecnología blockchain pueden mejorar la seguridad de la Gestión de Identidad y Acceso (IAM) en IoT. Estos avances son esenciales para abordar los retos emergentes en IAM y proteger los datos en el creciente mundo de IoT.

Keskar y Faldu (2022) proponen un marco de gestión de identidad y acceso basado en redes neuronales para abordar los desafíos de seguridad en la nube. Utiliza aprendizaje automático para predecir el acceso a archivos y autenticar usuarios mediante una nube de palabras. Resultados experimentales muestran su eficacia, aunque se necesita más investigación.

En la actualidad, la autenticación sin contraseña, especialmente con tecnologías como WebAuthn, está revolucionando el concepto general de gestión de identidades (IAM). Apple lidera con 'Passkeys', generando claves accesibles mediante FaceID o TouchID. La autenticación adaptativa, que busca equilibrar seguridad y experiencia de usuario, está emergiendo como una tendencia futura.

Comprendiendo el pasado y las tendencias venideras, las organizaciones pueden mantenerse a la vanguardia en sus respectivos sistemas de gestión de identidades (IdMS) y garantizar la seguridad de sus activos.

Principios de Sistemas de Gestión de identidades:

A fin de lograr resolver y superar las limitaciones de los Sistemas de gestión de identidades (IdMS), varios grupos de investigación, responsables políticos y líderes del sector propónen marcos para el despliegue de los mismos.

Principio	Descripción	Definiciones
Uno	Consentimiento del usuario	Se identifica y utiliza una identidad cuando el usuario da su consentimiento.

Dos	Divulgación limitada	El sistema proporciona la información de identificación mínima necesaria para la transacción.
Tres	Menos partes	Sólo las “partes” que necesitan saber reciben información de identificación.
Cuatro	Identidad direccional	Omni-direccional vs. Unidireccional
Cinco	El IdMS debe funcionar con una variedad de tecnologías	Los diseñadores no pueden asumir la viabilidad de una identidad universal o la disponibilidad de una única expresión de una identidad.
Seis	Integración humana	Altos niveles de fiabilidad entre el usuario humano y el sistema
Siete	Experiencia coherente	Similar a la apariencia de la web para la correcta experiencia de usuario (UX).

Tabla 3. Principios de Sistemas de gestión de identidades. Fuente: Cameron (2005)

Hovav y Berger (2009) en su trabajo revisa una investigación de Cameron (2005) en la cúal sugiere un conjunto de siete principios que deberían guiar el desarrollo del IdMs (Tabla 3). El núcleo de los principios es la idea de que IdMS debe ser una encapsulación o un meta-protocolo muy parecido al Protocolo de Internet (IP) o del protocolo de hipertexto (HTTP). IP, por ejemplo, no le importa qué dispositivo está conectado a la red, qué sistema operativo, la velocidad de la red o el formato del mensaje. Mientras la carga útil (datos) se empaquete en paquetes compatibles con IP, la transmisión a través de Internet es posible. Lo mismo puede decirse de HTTP. Conceptualmente, un IdMS debería comportarse de la misma manera. Es decir, independientemente del formato o contenido de la identidad digital cada dispositivo conectado a la red debe ser capaz de procesarla.

Los siete principios mencionados (también conocidos como "Las leyes de la identidad") describen un marco conceptual de un meta-IdMS. El marco también plantea algunos retos técnicos y sociales. El más notable es quién decide qué es el "mínimo requerido" y quién define la "necesidad de saber".

Normalización:

ISO (y más concretamente ISO/IEC JTC 1, SC27 IT Security techniques WG5 Identity Access Management and Privacy techniques) está llevando a cabo algunos trabajos de normalización para la gestión de identidades (ISO 2009), como la elaboración de un marco para la gestión de identidades, incluida la definición de términos relacionados con la identidad.

4. Conclusiones

Se tiene como conclusión que la IAM ha evolucionado significativamente en el ámbito de la seguridad de la información. El enfoque brindado nos dice que se ha convertido en un componente crítico para proteger los activos empresariales y la privacidad de los individuos en un mundo cada vez más interconectado y digitalizado.

El artículo proporcionado evidencia que la gestión de identidades y accesos ha evolucionado a lo largo de las décadas, adaptándose constantemente a los cambios en el panorama tecnológico y a las amenazas en constante evolución. Se identifican tendencias emergentes y se ofrecen hitos significativos, avances tecnológicos y desafíos superados en cada etapa de la evolución de la IAM.

Para investigaciones futuras, se recomienda explorar más a fondo las tendencias actuales y futuras en la IAM, así como las limitaciones y desafíos que enfrentan las organizaciones en la implementación del tema en el ámbito de la seguridad de la información. También se sugiere investigar cómo las tecnologías informáticas de brechas en seguridad tecnológica pueden integrarse con otras tecnologías emergentes, como la Inteligencia Artificial y el aprendizaje automático, para mejorar aún más la seguridad de la información. Además, se puede investigar cómo los datos y su eficiencia en el proceso de gestiones empresarial para los usuarios cumplen un papel crucial y tecnológico que puede ayudar a prevenir ataques cibernéticos y proteger la privacidad de las partes interesadas.

REFERENCIAS BIBLIOGRÁFICAS

Framework In Cloud Environment Based On Dual-factor Authentication

Alsirhani A., Ezz M. & Mostafa A. M. (2021). Advanced Authentication Mechanisms for Identity and Access Management in Cloud Computing

Ishaq Azhar M. (2017). Systematic review of Identity Access Management in Information Security. (n.d.).

A. Sharma, S. Sharma and M. Dave, "Identity and access management- a comprehensive study," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1481-1485, doi: 10.1109/ICGCIoT.2015.7380701.

Badirova A., Dabbaghi S., Moghaddam F., Wieder P. & Yahyapour R. (2023) A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges. https://doi.org/10.1109/ACCESS.2023.3279492

Beltrán M. & Calvo M. (2023). A privacy threat model for identity verification based on facial recognition. https://doi.org/10.1016/j.cose.2023.103324

Bradford M., Earp J. & Grabski S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework Marianne. http://dx.doi.org/10.1016/j.accinf.2014.01.003

Carnley P. & Kettani H. (2019). Identity and Access Management for the Internet of Things https://doi.org/10.18178/ijfcc.2019.8.4.554

Frederiksen T. K., Hesse J., Lehmann, A. & Torres Moreno, R. (2020). Identity Management: State of the Art, Challenges and Perspectives.

Gyeongjin R., Su-hyun K. & Imyeong L. (2022). Identity Access Management via ECC Stateless Derived Key Based Hierarchical Blockchain for the Industrial Internet of Things. https://doi.org/10.1587/transinf.2022NGP0003

IEEE. (2019). A security framework for wireless sensor networks in critical infrastructures. IEEE Communications Letters, 23(7), 1234-1237. https://doi.org/10.1109/COMMNET.2019.8742375

Indu I., Rubesh Anand P.M. & Bhaskar V. (2018). Identity and access management in cloud environment: Mechanisms and challenges https://doi.org/10.1016/j.jestch.2018.05.010

Kern S., Baumer T., Groll S., Fuchs L. & Pernul G. (2022) Optimization of Access Control Policies. https://doi.org/10.1016/j.jisa.2022.103301

Keskar A. P. & Faldu P. R. (2022). NEURAL NETWORKS for Smart IAM (Identity and Access Management)

Liao C., Guan X., Cheng J., Yuan S. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. https://doi.org/10.1016/j.future.2022.05.015

Mamdouh M., Awad A. I., Khalaf A. M., Hamed H. (2021). Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. https://doi.org/10.1016/j.cose.2021.102491

Partida A., Criado R. & Romance M. (2022). Identity and Access Management Resilience against Intentional Risk for Blockchain-Based IOT Platforms https://doi.org/10.1587/transinf.2022NGP0003

Pomputius A. (2019). A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory. https://doi.org/10.1080/02763869.2018.1514912

Sabrina F., Li N. & Sohail S. (2022). A Blockchain Based Secure IoT System Using Device Identity Management. https://doi.org/10.3390/s22197535

Hovav, A., & Berger, R. (2009). Tutorial: Identity Management Systems and Secured Access Control. Communications of the Association for Information Systems, 25, pp-pp. https://doi.org/10.17705/1CAIS.02542