Análisis Comparativo de los Métodos de Evaluación de la Confianza en Redes 6G

Elmira Saeedi Taleghani, Ronald Iván Maldonado Valencia,
Jesús Ángel Alonso López, Luis Javier García Villalba
E-mail: {elmirasa, ronaldim, jesusaal, javierv}@ucm.es
Grupo de Análisis, Seguridad y Sistemas (GASS), Dpto. de Ingeniería del Software e Inteligencia Artificial
Facultad de Informática, Despacho 431, Universidad Complutense de Madrid (UCM)
Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid

***Resumen*- 6G networks are anticipated to facilitate a diverse array of technologies to deliver secure, premium services. Consequently, the pivotal role of trust in addressing the exigencies of 6G networks cannot be overstated. This article undertakes a comprehensive exploration of trust concepts, methodologies, and techniques essential for ensuring a secure and dependable 6G ecosystem. Initially, we classify trust assessment techniques according to the specific field of study to which each technique pertains. Subsequently, a detailed scrutiny of these techniques is conducted, focusing on the distinct approaches delineated within each category. Lastly, a thorough examination of the technical hurdles, as well as the merits and demerits associated with the implementation of each technique, is provided.**

Palabra clave: 6G, evaluation methods, networks, privacy, security, trust.

I. INTRODUCCIÓN

Se espera que las redes de Sexta Generación (6G) soporten un gran número de dispositivos y aplicaciones conectadas [6], tales como dispositivos de Internet de las Cosas (IoT), redes de sensores inalámbricos, aplicaciones de, inteligencia artificial, dispositivos móviles, etc. Se deben abordar los retos de seguridad, privacidad, eficiencia y la capacidad de ofrecer servicios de alta calidad. Esto hace que la gestión de la confianza desempeñe un papel fundamental ya que contribuye a abordar estos retos en las operaciones de red en el panorama dinámico de las redes 6G [5]. Con estas consideraciones, se han planteado diferentes enfoques para abordar el problema de la gestión de la confianza en redes 6G.

El primero de estos enfoques consiste en hacer uso de inteligencia artificial (IA): En [10] se emplean redes neuronales profundas (DNN) para la evaluación de la confianza resaltando la sensibilidad de los parámetros, la seguridad y la consideración de ejemplos adversarios. En [36] se hace uso de inteligencia artificial explicable con el fin de dar entendimiento al impacto de los datos maliciosos, sesgados o deficientes, también para entender las acciones en la red y sus características clave para mejorar la confianza.

Otro enfoque consiste en cuantificar y mantener los niveles de reputación y confianza de la red evaluando las políticas de uso de recursos en el sistema y considerando los comentarios de los usuarios de dichos recursos, esto basado en la tecnología blockchain [4] [11] para garantizar la integridad de los comentarios. En [25] se aborda la incertidumbre y conocimiento incompleto de un sistema haciendo uso de lógica subjetiva para evaluar la confianza global y local de un servicio.

El presente trabajo pretende dar claridad sobre las posibles ventajas e implicaciones de estas soluciones en escenarios del mundo real. El resto del artículo se estructura como sigue: En la Sección II se explican los conceptos de confianza y su definición en el contexto de las redes 6G. En la Sección III se describen las técnicas utilizadas para evaluar la confianza en diferentes aplicaciones de las redes 6G. En la Sección IV se presenta un análisis de las técnicas analizadas en función de su aplicabilidad, destacando sus ventajas y desventajas. Finalmente, las conclusiones se presentan en la Sección V.

II. CONCEPTO DE CONFIANZA

La confianza implica depositar la Fe en una fuente fiable, y cuando esta fuente falla, la integridad y la seguridad del sistema se ven comprometidas. Según [1] se define la confianza como, "la creencia firme en la capacidad de una entidad para actuar de forma segura y fiable dentro de un contexto específico". La confianza que se tiene sobre una entidad puede ser directa o indirecta. Cuando un usuario se comunica con el sistema, establece una confianza directa, mientras que la confianza indirecta se produce cuando otro usuario comparte su experiencia acerca de esta entidad, lo que también se conoce como confianza recomendada [2]. Al ser un elemento crucial para la colaboración segura entre nodos la evaluación de la confianza suele considerarse un componente cuantificable, cuya naturaleza se ejemplifica en la relación entre el fideicomitente (*trustor*) y el fiduciario (*trustee*) [32].

Otro concepto importante es la gestión de confianza, el cual consiste en un conjunto de pasos en donde una entidad intenta asignar un nivel de confianza a otra [33]. En este modelo de gestión de confianza el primer paso es establecer una relación entre un fideicomitente y un fiduciario. La segunda etapa es la recopilación de datos útiles para la confianza, estos datos pueden ser las pruebas recogidas mediante la monitorización de los fiduciarios, la recopilación del historial de relaciones y comportamientos del fideicomitente, la solicitud de recomendaciones a los nodos vecinos del fiduciario (en ausencia de comunicación directa), o la retroalimentación de otros sistemas de monitorización. La tercera etapa es la evaluación de la confianza, que puede ser diferente según el tipo de servicio. La última etapa consiste en la toma de decisiones, control y mantenimiento de la confianza esto debido a que las relaciones de confianza cambian dinámicamente. El modelo de confianza se muestra en la Figura 1.

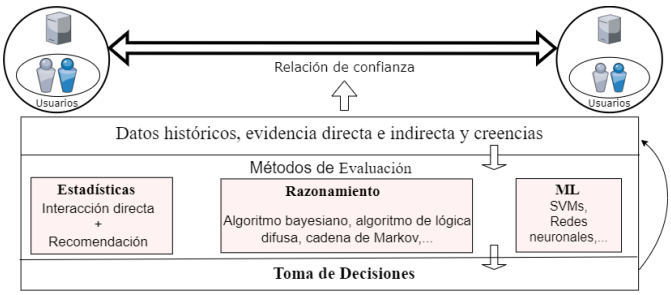

Fig. 1. Modelo de gestión de confianza

III. Evaluación de la Confianza en Redes 6G

Existen distintos tipos de modelos de confianza utilizados para determinar el grado de fiabilidad de las redes 6G. Hay cuatro categorías: modelos estadísticos, modelos de aprendizaje automático, modelos descentralizados y modelos de razonamiento. Cada categoría ofrece ventajas y consideraciones distintas, lo que permite a las partes interesadas elegir el enfoque más adecuado en función de los recursos disponibles, los datos y los requisitos específicos del proceso de evaluación de la confianza. A continuación, se presentan las investigaciones en cada una de estas categorías.

A. Enfoque Estadístico

Los métodos de suma ponderada son cruciales para evaluar el nivel de confianza en las redes 6G, ya que ofrecen varias ventajas en la evaluación de la confianza. Estos métodos agregan diversos parámetros de confianza, como la fiabilidad, la honestidad y el conocimiento del contexto, lo que permite un proceso de evaluación de la confianza más adaptable y específico del contexto [29]. También permiten incorporar opiniones subjetivas e incertidumbre, mejorando la flexibilidad y solidez de la evaluación de la confianza en entornos de redes 6G dinámicas [30]. Sin embargo, los métodos de suma ponderada también presentan desventajas, como la dificultad para determinar las ponderaciones adecuadas para los parámetros de confianza, lo que puede introducir sesgos e incoherencias. Además, la interpretabilidad del enfoque de la suma ponderada puede ser limitada, ya que la lógica que subyace a las ponderaciones asignadas puede no ser transparente, lo que podría dificultar el establecimiento de la confianza [31].

B. Enfoques Descentralizados

La tecnología *blockchain* es una forma de libro de contabilidad distribuido, en donde la información se almacena en diferentes nodos y cada nodo tiene una copia idéntica del libro de contabilidad. Esto permite que la información sea segura, trazable, esté descentralizada y sea inmutable [21]. Dadas las propiedades descritas, la tecnología *blockchain* puede garantizar que los datos relacionados con la confianza sean legítimos y en consecuencia hacer que el entorno de red sea más fiable. En [8] se propone un *framework* llamado B-RAN, el cual está basado en *blockchain,* para establecer relaciones de confianza en redes inalámbricas. Se usa un mecanismo de consenso basado en identidad, luego para la toma de acciones sobre el *blockchain* se hace uso de un despliegue rápido de contratos inteligentes. En este sistema cada dispositivo deberá resolver un acertijo *hash* para evitar el uso excesivo de recursos, problemas de latencia y el acceso de dispositivos no confiables a la red, con este esquema de acceso *hash* se garantiza que los dispositivos sigan unas reglas y así lograr establecer confianza entre los clientes y los recursos. En [37] se propone un mecanismo de evaluación de confianza para el acceso dinámico al espectro para sistemas IoT. Este aspecto dinámico hace que diferentes servicios no relacionados compartan información, con lo cual el método propuesto en [37] pretende garantizar la privacidad, la transparencia de la información, el acceso descentralizado al espectro, la gestión automática del espectro y la flexibilidad mediante la parametrización de los contratos inteligentes. En este mecanismo la información relacionada con la confianza es almacenada en la *blockchain*, donde el valor de confianza varía en función de la consistencia de las mediciones cooperativas realizadas en las redes IoT.

C. Enfoque basado en el Razonamiento

Los algoritmos bayesianos pueden ser usados para evaluar el nivel de confianza en las redes 6G. En [12] se hace uso de Redes Bayesianas (Bnets) para modelar la integración de comunicaciones, navegación, sensores y servicios en las Redes CONASENSE (CNSS). La CNSS puede ser representada matemática y gráficamente mediante redes bayesianas lo que permite reflejar las relaciones entre entidades. Esta metodología bayesiana es adecuada para evaluar la confianza en redes 6G complejas, ya que ayuda a mitigar comportamientos maliciosos, mejorar las medidas de seguridad y establecer canales de comunicación fiables. El cálculo indirecto de la confianza se invoca condicionalmente en función de la incertidumbre de la confianza directa, excluyendo la retroalimentación maliciosa [34] [35].

La lógica subjetiva es un marco matemático que puede utilizarse para evaluar la confianza en las redes 6G. Permite modelar y fusionar opiniones inciertas y subjetivas, posibilitando una evaluación más matizada y consciente del contexto [22]. Al incorporar evaluaciones subjetivas de diversas fuentes, como nodos de red, dispositivos y usuarios, las redes 6G pueden obtener una evaluación completa y contextualmente relevante de los niveles de confianza dentro de la red [24]. Este enfoque tiene en cuenta factores cualitativos e inciertos que influyen en la confianza, como las experiencias de los usuarios, las condiciones ambientales y los comportamientos dinámicos de la red. La lógica subjetiva también facilita la adaptación y el aprendizaje de las evaluaciones de confianza a lo largo del tiempo, permitiendo a la red ajustar los niveles de confianza basándose en la evolución dinámica de las evaluaciones subjetivas [23].

Sin embargo, las desventajas potenciales asociadas con el uso de la lógica subjetiva incluyen desafíos relacionados con la interpretación y el procesamiento de las evaluaciones subjetivas, la necesidad de establecer marcos estandarizados para capturar e integrar las opiniones subjetivas, y la naturaleza dinámica y evolutiva de las evaluaciones subjetivas. Por lo tanto, es esencial considerar cuidadosamente su implementación, interpretación y procesamiento para aprovechar todo su potencial en la mejora de la confianza y la seguridad en los sistemas de comunicación 6G [25].

D. Enfoques basados en el Aprendizaje Automático

Existen diferentes técnicas de aprendizaje automático para evaluar la confianza, una de ellas son las cadenas de Markov. Estos métodos incluyen Markov chain Monte Carlo (MCMC) para la inferencia de confianza en redes *peer-to-peer,* esquemas de gestión de confianza basados en cadenas de Markov para redes de sensores inalámbricas, y modelos

futuristas de evaluación de la cooperación para evaluar la fiabilidad de los nodos y la estabilidad de los enlaces en redes ad hoc móviles [13] [14]. Estos métodos aprovechan las capacidades de las cadenas de Markov, como el muestreo a partir de secuencias de grafos especificadas, el análisis de grafos de influencia y la predicción de rutas de coste mínimo en redes de sensores inalámbricas móviles [15]. También se han aplicado a algoritmos de redes sociales para identificar usuarios con gran influencia en la red [16]. En general, las cadenas de Markov son herramientas versátiles para garantizar la fiabilidad y la seguridad de las redes 6G.

Las máquinas de soporte vectorial (SVM) han sido ampliamente utilizadas para evaluar la confianza en redes 6G, demostrando su eficacia en problemas de clasificación y en diversas aplicaciones [3] [17]. En el contexto de las redes 6G, las SVM se han utilizado en diversas aplicaciones como el aprendizaje federado, la evaluación de la confianza en redes móviles ad-hoc y los retos de seguridad en las tecnologías 6G [18, 7]. Han demostrado una mayor precisión de aprendizaje, una convergencia más rápida y un menor consumo de energía, lo que las hace adecuadas para escenarios de redes 6G [18]. Las SVM también se han utilizado en marcos de evaluación de la confianza para redes sociales en línea, redes vehiculares y algoritmos de aprendizaje de máquinas cuánticas [19]. Su versatilidad en la evaluación de la confianza en diferentes contextos de red se alinea con la tendencia de aprovechar los métodos de aprendizaje automático para mejorar la confianza, la seguridad y la privacidad en las redes inalámbricas [8] [20]. Las SVM también se han integrado en arquitecturas de confianza cero para redes 6G, lo que demuestra su importancia para establecer regímenes de seguridad sólidos [9]. En resumen, las SVM han demostrado ser una valiosa herramienta para la evaluación de la confianza en las redes 6G, demostrando su aplicabilidad en diversos ámbitos y ajustándose a la evolución de sus requisitos.

Las Redes Neuronales Artificiales (RNA) son usadas cada vez más para evaluar la confianza en las redes 6G por su capacidad para procesar relaciones complejas y no lineales y aprender de grandes conjuntos de datos. Las RNA pueden captar patrones y relaciones intrincados en los datos relacionados con la confianza, proporcionando evaluaciones de confianza precisas y adaptables. Pueden manejar datos de gran dimensión y ruido, lo que las hace adecuadas para modelar la naturaleza dinámica de la confianza en las redes 6G [26]. Las RNA pueden desplegarse en diferentes capas de la red, como dispositivos de computación en el borde y en la nube, para la evaluación distribuida de la confianza, mejorando la escalabilidad y la eficiencia [26]. Sin embargo, éstas también presentan retos difíciles de entender, como la interpretabilidad, y las exigencias computacionales, que pueden plantear problemas en entornos con recursos limitados [27] [28].

IV. Análisis Comparativo de los Métodos de Evaluación de la Confianza

Para evaluar los niveles de confianza dentro de estas redes se emplean diversas metodologías, como la bayesiana, la de suma ponderada, la de lógica subjetiva, las cadenas de Markov, las máquinas de soporte vectorial, las redes neuronales y Blockchain. Cada enfoque ofrece ventajas y desventajas únicas que deben considerarse cuidadosamente. Los métodos bayesianos proporcionan un enfoque versátil y probabilístico de la evaluación de la confianza, integrando el conocimiento previo y las pruebas; sin embargo, tienen dificultades con la incertidumbre y dependen en gran medida de determinadas hipótesis. Las técnicas de suma ponderada manejan eficazmente la incertidumbre y las opiniones subjetivas, ofreciendo flexibilidad y personalización; sin embargo, se enfrentan a retos a la hora de determinar las ponderaciones adecuadas y a una interpretabilidad limitada. La lógica subjetiva destaca en el manejo de la incertidumbre y la evaluación contextualizada, pero requiere importantes recursos informáticos y tiene dificultades para definir los operadores. Los modelos de cadenas de Markov son útiles para sistemas dinámicos, pero pueden fallar en escenarios complejos. Las máquinas de soporte vectorial se aplican a datos de alta dimensión, pero requieren un ajuste exhaustivo y carecen de explicabilidad. Las redes neuronales artificiales procesan relaciones complejas, pero se enfrentan a problemas de interpretabilidad y altas exigencias computacionales. Blockchain ofrece descentralización e inmutabilidad, pero a costa de un elevado consumo de recursos y problemas de regulación. Para seleccionar el enfoque más adecuado que permita mejorar la confianza, la seguridad y la privacidad en el ecosistema de la red 6G es fundamental tener en cuenta estos puntos fuertes y limitaciones. La Tabla I ofrece una visión general de las ventajas e inconvenientes de los métodos habituales de evaluación de la confianza.

TABLA I
COMPARACIÓN DE LAS TÉCNICAS DE EVALUACIÓN DE LA CONFIANZA

Categoría	**Técnicas**	**Ventajas**	**Desventajas**
Estadística	Suma ponderada	• Tratamiento eficaz de la incertidumbre y las opiniones subjetivas • Flexibilidad, personalización y robustez	• Dificultad para determinar los pesos • Interpretabilidad limitada
Razonamiento	Bayesiano	• Ofrece un enfoque versátil y probabilístico de la evaluación de la confianza	• No puede hacer frente a la incertidumbre de la confianza • Los conocimientos previos son difíciles de obtener
	Lógica subjetiva	• Maneja eficazmente la incertidumbre y las opiniones subjetivas	• Operadores difíciles de definir • Requiere importantes recursos computacionales
Aprendizaje Automático	Cadenas de Markov	• Útil para modelar sistemas dinámicos	• Pueden tener dificultades con escenarios complejos y grandes espacios de estado
	Máquinas de soporte vectorial	• Aplicable a datos no lineales y de alta dimensionalidad • Buena capacidad de generalización	• Poca explicabilidad • Requiere un ajuste y una optimización exhaustivos
	Redes Neuronales Artificiales	• Permite procesar relaciones complejas y no lineales • Pueden desplegarse en diferentes capas de la red	• Dificultades de interpretación • Exigente computacionalmente
Descentralizado	Blockchain	• Descentralización y coherencia • Inmutabilidad y trazabilidad	• Alto consumo de recursos: para llegar a un consenso. • Baja eficiencia del consenso se traduce en una baja escalabilidad.

V. Conclusiones

Este trabajo analiza la importancia de la confianza en la creación y funcionamiento de las redes 6G. La fiabilidad es la base de la seguridad y la privacidad en las redes, especialmente a la luz de las numerosas aplicaciones y las tecnologías de comunicación en constante evolución. Se hace hincapié en el papel esencial que desempeña la confianza en la creación de un entorno seguro y cooperativo para las redes de comunicaciones inalámbricas de próxima generación, centrándose en los procesos que establecen la confianza, *frameworks* de seguridad y tecnología respetuosa con la privacidad. Esto usando técnicas de vanguardia como las DNN, la gestión de la confianza basada en *blockchain*, los algoritmos bayesianos y el razonamiento subjetivo, el estudio ayuda a crear métodos fiables para evaluar la confianza que son específicos para las necesidades de las redes 6G. De cara al futuro, la integración de estos enfoques innovadores será decisiva para abordar vulnerabilidades y retos críticos a los que se enfrentan las redes 6G, allanando en última instancia el camino hacia un ecosistema 6G seguro, resistente y confiable.

Agradecimientos

Los autores agradecen la financiación recibida del Programa UNICO-5G I+D del Ministerio de Asuntos Económicos y Transformación Digital y de la UE – Next Generation EU a través de los proyectos ATESTA5G (TSI-063000-2021-0049), TRAZA5G (TSI-063000-2021-0050) y Plan de Promoción y Atracción del Talento (TSI-063000-2021-0076).

Referencias

[1] M. Shafi, R. K. Jha and S. Jain, "Intelligent Trust Ranking Security Preserving Model for B5G/6G," in IEEE Transactions on Network and Service Management, vol. 20, no. 3, pp. 3549-3561, 2023.

[2] I. Ahmad, K. -L. A. Yau, M. H. Ling and S. L. Keoh, "Trust and Reputation Management for Securing Collaboration in 5G Access Networks: The Road Ahead," in IEEE Access, vol. 8, pp. 62542-62560, 2020.

[3] L. Yang, Y. Li, S. X. Yang, Y. Lu, T. Guo and K. Yu, "Generative Adversarial Learning for Intelligent Trust Management in 6G Wireless Networks," in IEEE Network, vol. 36, no. 4, pp. 134-140, 2022.

[4] G. D. Putra, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "Toward Blockchain-Based Trust and Reputation Management for Trustworthy 6G Networks," in IEEE Network, vol. 36, no. 4, pp. 112-119, 2022.

[5] Y. Wang, X. Kang, T. Li, H. Wang, C. -K. Chu and Z. Lei, "SIX-Trust for 6G: Toward a Secure and Trustworthy Future Network," in IEEE Access, vol. 11, pp. 107657-107668, 2023.

[6] H. T. Nguyen, W. Zhao and J. Yang, "A Trust and Reputation Model Based on Bayesian Network for Web Services," 2010 IEEE International Conference on Web Services, Miami, FL, USA, 2010.

[7] B. Veith, D. Krummacker and H. D. Schotten, "The Road to Trustworthy 6G: A Survey on Trust Anchor Technologies," in IEEE Open Journal of the Communications Society, vol. 4, pp. 581-595, 2023

[8] J. Wang, X. Ling, Y. Le, Y. Huang and X. You, "Blockchain-enabled wireless communications: a new paradigm towards 6G," National science review, vol 8, 2021.

[9] X. Chen, W. Feng, N. Ge and Y. Zhang, "Zero Trust Architecture for 6G Security," in IEEE Network. 2023.

[10] A. Nechi et al., "Practical Trustworthiness Model for DNN in Dedicated 6G Application," 2023 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Montreal, 2023.

[11] J. A. Alonso-Lupez et al., "Level of Trust and Privacy Management in 6G Intent-based Networks for Vertical Scenarios," 2022 1st International Conference on 6G Networking (6GNet), 2022.

[12] P. S. Rufino Henrique and R. Prasad, "Bayesian Neural Networks for 6G CONASENSE Services," 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC), Herning, Denmark, 2022.

[13] X. Li and D. Feng, "Markov chain based trust management scheme for wireless sensor networks," Journal of Networks, vol 9, no. 12, 2014.

[14] P. Theerthagiri, "FUCEM: futuristic cooperation evaluation model using Markov process for evaluating node reliability and link stability in mobile ad hoc network," Wireless Networks, vol. 26, no. 6, pp. 4173-4188, 2020.

[15] U. Dutta, B. K. Fosdick and A. Clauset, "Sampling random graphs with specified degree sequences," Arxiv, 2021.

[16] M. Richardson, R. Agrawal and P. Domingos, "Trust management for the semantic web," in International Semantic Web Conference, Berlin, Heidelberg, Oct. 2003.

[17] V. Havlíček, A. D. Córcoles, K. Temme, A. W. Harrow, A. Kandala, J. M. Chow and J. M. Gambetta, "Supervised learning with quantum-enhanced feature spaces," Nature, vol. 567, no. 7747, pp. 209-212, 2019.

[18] X. Zhou, W. Liang, J. She, Z. Yan and K. I. -K. Wang, "Two-Layer Federated Learning with Heterogeneous Model Aggregation for 6G Supported Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 70, no. 6, pp. 5308-5317, June 2021.

[19] R. D. M. Simões, P. Huber, N. Meier, N. Smailov, R. M. Füchslin and K. Stockinger, "Experimental Evaluation of Quantum Machine Learning Algorithms," in IEEE Access, vol. 11, pp. 6197-6208, 2023.

[20] Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5098-5107, July 2021 .

[21] M. Z. Chowdhury, M. Shahjalal, S. Ahmed and Y. M. Jang, "6G Wireless Communication Systems: Applications, Requirements, Technologies, Challenges, and Research Directions," in IEEE Open Journal of the Communications Society, vol. 1, pp. 957-975, 2020.

[22] E. Alemneh, S. M. Senouci, P. Brunet and T. Tegegne, "A two-way trust management system for fog computing," Future Generation Computer Systems, vol. 106, pp. 206-220, 2020.

[23] J. Yuan, H. Zhou and H. Chen, "Subjective logic-based anomaly detection framework in wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 8, no. 1, pp. 482191, 2012.

[24] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen and R. U. Ashraf, "Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic," IET Information Security, vol. 13, no. 3, pp. 223-230, 2019.

[25] H. Kurdi, A. Alfaries, A. Al-Anazi, S. Alkharji, M. Addegaither, A. Altoaimy and S. H. Ahmed, "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments," The Journal of Supercomputing, vol. 75, pp. 3534-3554, 2019.

[26] K. Singh, A. K. Verma and P. Aggarwal, "Analysis of various trust computation methods: a step toward secure FANETs," in Computer and Cyber Security, Auerbach Publications, pp. 171-193, 2018.

[27] A. Koeppe, F. Bamer, M. Selzer, B. Nestler and B. Markert, "Explainable artificial intelligence for mechanics: physics-informing neural networks for constitutive models," arXiv, 2021.

[28] A. Apparaju and O. Arandjelović, "Towards new generation, biologically plausible deep neural network learning," Sci, vol. 4, no. 4, p. 46, 2022.

[29] S. A. Siddiqui, A. Mahmood, Q. Z. Sheng, H. Suzuki and W. Ni, "Trust in vehicles: toward context-aware trust and attack resistance for the internet of vehicles," IEEE Trans. on Intelligent Transportation Systems, 2023.

[30] X. Feng and Z. Yuan, "A novel trust evaluation mechanism for edge device access of the Internet of things," Wireless Communications and Mobile Computing, 2022.

[31] Y. Gao, X. Li, J. Li, Y. Gao and S. Y. Philip, "Info-trust: A multi-criteria and adaptive trustworthiness calculation mechanism for information sources," IEEE Access, vol. 7, pp. 13999-14012, 2019.

[32] T. D. Nguyen and Q. Bai, "A dynamic Bayesian network approach for agent group trust evaluation," Computers in Human Behavior, pp. 237-245, 2018.

[33] H. Amal, A. Samiha and C. Lamia, "A survey of trust management in the Internet of Vehicles," Computer Networks, vol. 203, p. 108558, 2022.

[34] R. Feng, X. Han, Q. Liu and N. Yu, "A credible Bayesian-based trust management scheme for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 11, no. 11, p. 678926, 2015.

[35] M. Hosseinnezhad, M. A. Azgomi and M. R. E. Dishabi, "A probabilistic trust model for cloud services using Bayesian networks," Soft Computing, vol. 28, no. 1, pp. 509-526, 2024.

[36] W. Guo, "Explainable artificial intelligence for 6G: Improving trust between human and machine," IEEE Comm. Magazine, vol. 58, no. 6, pp. 39-45, 2020.

[37] J. Ye, X. Kang, Y. C. Liang and S. Sun, "A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks," IEEE Internet of Things Journal, vol. 9, no. 15, pp. 13263-13278, 2022.