Año 17 / Núm. 42 / - julio – diciembre 2024
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

REVISTA DE
INVESTIGACIÓN ACADÉMICA SIN FRONTERA

BLOCKCHAIN Y ENCRIPTACIÓN: LA NUEVA FRONTERA DE LA SEGURIDAD DIGITAL

BLOCKCHAIN AND ENCRYPTION: THE NEW FRONTIER OF DIGITAL SECURITY

Mtro. Francisco Alan Espinoza Zallas[1], Mtro. Miguel Ángel Romero Ochoa[2], Mtro. Efren Samano Hermosillo[3]

[1]Profesor de tiempo completo, Universidad Estatal de Sonora, https://orcid.org/0000-0002-1177-2028. alan.espinoza@ues.mx.

[2]Profesor de tiempo completo, Universidad Estatal de Sonora, https://orcid.org/0000-0003-4617-9950. miguel.romero@ues.mx.

[3]Profesor de tiempo completo, Universidad Estatal de Sonora, efren.samano@ues.mx.

DOI: https://doi.org/10.46589/riasf.v1i42.740

Recibido: 14 de julio de 2024.
Aceptado: 20 de noviembre de 2024.
Publicado: 20 de diciembre 2024.

Cómo citar

Espinoza Zallas, F., Romero Ochoa, M., & Samano Hermosillo, E. (2024). Blockchain y encriptación: la nueva frontera de la seguridad digital. Revista De Investigación Académica Sin Frontera: Facultad Interdisciplinaria De Ciencias Económicas Administrativas - Departamento De Ciencias Económico Administrativas-Campus Navojoa, 1(42). https://doi.org/10.46589/riasf.v1i42.740

Resumen

El vertiginoso avance de las tecnologías emergentes, en particular el Internet de las Cosas (IoT), ha traído consigo desafíos críticos en la seguridad de la información. Con la creciente adopción de dispositivos conectados, se ha evidenciado una brecha significativa en la seguridad que necesita ser abordada, ya que estos dispositivos transmiten datos sensibles que pueden comprometer la privacidad y la integridad de la información si caen en manos equivocadas. Esta investigación se enfoca en el desarrollo de una plataforma de pruebas de seguridad diseñada específicamente para el IoT, utilizando los protocolos MQTT, la tecnología blockchain y la librería ReactJS. La plataforma busca abordar los desafíos de seguridad que enfrentan los dispositivos y las comunicaciones en un entorno IoT.

El análisis de la documentación existente sobre seguridad en redes informáticas revela diversas técnicas, protocolos y algoritmos para garantizar la integridad de la información transmitida. A pesar de la existencia de métodos como HTTPS, se ha detectado su vulnerabilidad en el contexto del IoT. Para abordar esta vulnerabilidad y mejorar la seguridad de los dispositivos IoT, esta investigación examina protocolos existentes y considera la creación de algoritmos de encriptación y la implementación de la tecnología blockchain, basándose en algoritmos de curva elíptica y contratos inteligentes.

La blockchain y los contratos inteligentes emergen como oportunidades prometedoras para establecer una metodología que garantice la privacidad y seguridad de la información en el IoT. Además, la información almacenada en la cadena de bloques permanece inalterable, asegurando la integridad de los datos. Este proceso se lleva a cabo en tiempos competitivos en comparación con otros mecanismos, lo que constituye el objetivo central de esta investigación.

Palabras clave: Internet de las Cosas (IoT), seguridad, blockchain, encriptación, MQTT, ReactJS, privacidad, contratos inteligentes.

Abstract

The rapid advancement of emerging technologies, particularly the Internet of Things (IoT), has brought critical challenges in information security. With the increasing adoption of connected devices, a significant security gap has become evident that needs to be addressed, as these devices transmit sensitive data that can compromise privacy and data integrity if they fall into the wrong hands. This research focuses on developing a security testing platform specifically designed for IoT, utilizing MQTT protocols, blockchain technology, and the ReactJS library. The platform aims to address the security challenges faced by devices and communications in an IoT environment.

The analysis of existing literature on network security reveals various techniques, protocols, and algorithms to ensure the integrity of transmitted information. Despite the existence of methods like HTTPS, their vulnerability has been detected in the IoT context. To address this vulnerability and enhance the security of IoT devices, this research examines existing protocols and considers creating encryption algorithms and implementing blockchain technology, based on elliptic curve algorithms and smart contracts.

Blockchain and smart contracts emerge as promising opportunities to establish a methodology that ensures the privacy and security of information in the IoT. Furthermore, information stored on the blockchain remains unalterable, ensuring data integrity. This process is carried out in competitive times compared to other mechanisms, which constitutes the central objective of this research.

Keywords: Internet of Things (IoT), security, blockchain, encryption, MQTT, ReactJS, privacy, smart contracts.

Introducción

El último siglo ha sido testigo de un avance sin precedentes en las telecomunicaciones, la expansión global de Internet y el desarrollo de microcontroladores y sensores, lo que ha conducido a una sociedad cada vez más interconectada. Esta interconexión se extiende más allá de los individuos, abarcando electrodomésticos y dispositivos cotidianos, conformando el concepto del Internet de las Cosas (IoT). Sin embargo, este crecimiento vertiginoso plantea desafíos críticos relacionados con la privacidad y la seguridad de la información.

La revisión sistemática de la literatura realizada por Caron, Bosua, Maynard y Ahmad (2015) identifica cuatro temas clave de privacidad que representan problemas significativos en la recopilación de datos a través del IoT: vigilancia no autorizada, generación y uso de datos, autenticación inadecuada y riesgos de seguridad de la información. Los resultados de esta investigación revelan que las aplicaciones actuales no protegen de manera adecuada la privacidad de los datos recopilados a través del IoT. A pesar de la existencia de protocolos de seguridad, como el TLS (Transport Layer Security), algunos de estos han demostrado vulnerabilidades, como indican Huang, Zhang, Li y Xin (2019) en sus investigaciones. Además, la implementación de protocolos de seguridad existentes para el IoT se ha vuelto una tarea complicada, comprometiendo en gran medida la seguridad de los datos recopilados por proyectos IoT.

La última década ha sido testigo del rápido crecimiento de dispositivos conectados al IoT, pero también ha destacado la creciente amenaza de explotación por parte de personas malintencionadas. Los ataques a dispositivos IoT, incluido el histórico ataque DDoS (Distributed Denial of Service) de la botnet Mirai, subrayan la urgencia de abordar los desafíos de seguridad en este entorno, como mencionan Vignau et al. (2021) y Hamza et al. (2020) en sus investigaciones.

Ante esta problemática, se vuelve esencial desarrollar una metodología que incluya mecanismos de seguridad para preservar la integridad y confidencialidad de la

información en el IoT. El propósito de esta investigación es analizar diversos protocolos de seguridad, incluyendo la seguridad simétrica, asimétrica y mixta, junto con mecanismos utilizados en otras tecnologías, para crear una metodología innovadora que resuelva los desafíos de seguridad en el IoT. Este nuevo paradigma presenta muchos desafíos de seguridad y privacidad relacionados con la autenticación y la autorización, la confidencialidad de los datos, la información personal, la comunicación y la seguridad informática (Li, 2017). Aunado a esto, Sahmim y Gharsellaoui (2017) aportan que las intrusiones y vulnerabilidades serán cada vez más recurrentes debido a la complejidad de los sistemas y las diferentes formas para controlar cada intento de acceso. Esta investigación tiene como objetivo proporcionar una plataforma que garantice la privacidad e integridad de la información en el IoT, permitiendo que quienes la implementen confíen en que sus datos permanecerán seguros y confidenciales. El proyecto se basará en la combinación de sensores generadores de datos, un dispositivo IoT como Raspberry Pi 3, un servidor de Internet como intermediario y una aplicación desarrollada en ReactJS, siguiendo las recomendaciones de Saravanan et al. (2021).

Este estudio aborda una necesidad crítica en el campo del IoT al desarrollar una plataforma de pruebas de seguridad basada en MQTT y Blockchain. Su finalidad es proporcionar una solución robusta que garantice la seguridad de la información en un mundo cada vez más interconectado y en constante evolución.

Material y método

La metodología para el estudio de la seguridad en el Internet de las Cosas (IoT) a menudo se centra en el análisis y la integración de protocolos de comunicación como MQTT con tecnologías de seguridad avanzadas como blockchain, y su visualización a través de interfaces de usuario modernas como ReactJS.

Consideraciones de Diseño de Sistemas de Seguridad: Para garantizar la seguridad en entornos IoT, la arquitectura de los sistemas debe considerar la integración efectiva de protocolos de comunicación y tecnologías de inmutabilidad de datos. MQTT,

un protocolo ligero para la comunicación entre dispositivos y servidores, es fundamental, mientras que blockchain puede ser implementado para asegurar la integridad de los datos. Estos sistemas deben ser modulares y escalables para permitir futuras expansiones y mejoras. La selección de bibliotecas y herramientas adecuadas para MQTT y blockchain es crucial, aplicando las mejores prácticas de seguridad en su configuración. Las interfaces de usuario, a menudo desarrolladas con tecnologías como ReactJS, permiten la configuración de escenarios, la visualización de resultados y la supervisión del estado de los dispositivos IoT. Las medidas de seguridad deben ser inherentes al diseño, incluyendo controles de acceso y autenticación, para restringir el uso a usuarios autorizados. La combinación de Solidity para contratos inteligentes, Metamask para la gestión de claves y Ganache como entorno de desarrollo blockchain local, junto con ReactJS para la interfaz, es un enfoque que fortalece la capacidad de evaluar y mejorar la seguridad en aplicaciones IoT basadas en MQTT y blockchain.

Enfoques para la Evaluación y Pruebas de Seguridad: La fase de evaluación y pruebas es esencial para determinar la eficacia de los mecanismos de seguridad en un entorno IoT. Comúnmente, se utiliza un dispositivo de bajo costo y alta conectividad como Raspberry Pi 3 como nodo central de la infraestructura de pruebas. En él, se pueden configurar las bibliotecas y herramientas necesarias para interactuar con dispositivos IoT simulados y el sistema de seguridad.

Para la evaluación, se diseñan casos de prueba que simulan situaciones del mundo real, exponiendo los dispositivos IoT a amenazas de seguridad, incluyendo escenarios de ataque, vulnerabilidades conocidas y situaciones de tráfico de datos críticos. Se pueden llevar a cabo simulaciones de ataques para evaluar la respuesta del sistema, así como su capacidad para detectar y mitigar dichas amenazas.

El rendimiento del sistema se mide durante estas pruebas, considerando la velocidad de detección de amenazas, la eficacia de las contramedidas implementadas y

la escalabilidad del sistema en términos de procesamiento y manejo de datos. La recopilación de datos detallados, como registros de eventos, resultados de pruebas de seguridad y métricas de rendimiento, es fundamental. Estos datos son analizados en profundidad para evaluar la eficacia de las soluciones y determinar áreas de mejora, lo que a menudo lleva a ajustes y optimizaciones en la configuración de los protocolos y tecnologías de seguridad.

Metodología de Investigación de Software: La investigación en este campo a menudo sigue una metodología estructurada, que puede incluir los siguientes pasos:

Revisión de la Literatura: Una revisión exhaustiva de la literatura es fundamental para comprender el estado del arte en seguridad IoT, el protocolo MQTT, la tecnología blockchain y las mejores prácticas en encriptación y autenticación.

Diseño de Soluciones: Se conceptualizan y diseñan arquitecturas de seguridad que integran MQTT y blockchain como componentes clave. Estas soluciones permiten simular y evaluar amenazas de seguridad en un entorno controlado, a menudo utilizando dispositivos como Raspberry Pi 3.

Experimentación y Pruebas: Se implementan escenarios de prueba y se simulan ataques para evaluar la resistencia de los dispositivos IoT y las comunicaciones frente a amenazas comunes. Se mide el rendimiento y la eficacia en términos de detección y mitigación de amenazas.

Análisis de Resultados: Los resultados de las pruebas son analizados y comparados con otras soluciones de seguridad existentes en el ámbito del IoT, prestando especial atención a la contribución de los componentes individuales y su impacto en el rendimiento general de la seguridad.

Propuesta de Mejoras: A partir de los hallazgos de la investigación, se formulan recomendaciones y mejores prácticas específicas para fortalecer la seguridad en sistemas IoT que utilizan MQTT y blockchain.

Instrumentos de Investigación y Análisis de Datos: Para la recolección de datos en estudios de seguridad IoT, se pueden utilizar diversos instrumentos. Las entrevistas

a expertos en criptografía, desarrolladores de aplicaciones IoT o usuarios finales son valiosas para recopilar información cualitativa sobre experiencias, necesidades y perspectivas relacionadas con la privacidad y seguridad de la información. Adicionalmente, el análisis de registros o datos recopilados de aplicaciones IoT o simulaciones permite realizar evaluaciones de seguridad, análisis de riesgos o mediciones del rendimiento de los algoritmos criptográficos implementados. Esto incluye el análisis de datos encriptados y desencriptados, pruebas de vulnerabilidades y comparaciones de rendimiento. Estos instrumentos están diseñados para evaluar la efectividad de las medidas de seguridad, la percepción de los usuarios sobre la privacidad y seguridad de la información, y para identificar posibles mejoras o recomendaciones. El análisis de datos cualitativos se realiza mediante la transcripción y codificación de las entrevistas, identificando temas y patrones relevantes para organizar y analizar los datos de manera sistemática. Para el análisis de los registros de datos, la seguridad se evalúa mediante pruebas de vulnerabilidades o comparando el rendimiento de diferentes algoritmos criptográficos, utilizando métricas relevantes, gráficos comparativos, pruebas de hipótesis o técnicas de modelado. Finalmente, la interpretación y síntesis de los resultados implican buscar patrones, tendencias o relaciones significativas entre los datos y su conexión con las preguntas de investigación y objetivos, destacando los hallazgos más importantes y ofreciendo recomendaciones o sugerencias basadas en los datos analizados.

Resultados

La investigación en el campo de la seguridad IoT, especialmente aquella que explora la integración de protocolos de comunicación y tecnologías distribuidas, ha arrojado y continúa arrojando resultados clave que informan sobre las mejores prácticas y el potencial de estas soluciones.

1. Identificación de protocolos y algoritmos criptográficos óptimos: Los estudios en este ámbito consistentemente identifican los protocolos y algoritmos criptográficos

más adecuados para garantizar la privacidad y seguridad en las aplicaciones del IoT. Esto implica una evaluación continua de diferentes opciones y la selección de aquellas que demuestran ser más efectivas en términos de protección de la información, considerando factores como la eficiencia computacional y la resistencia a ataques conocidos.

2. Impacto de la integración tecnológica en la protección de la información: Se ha determinado que la integración de enfoques avanzados de criptografía, como el uso de blockchain, impacta positivamente en la protección de la información en el contexto del IoT. Esta integración mejora la seguridad y privacidad de la información, reduciendo los riesgos de vulnerabilidades y manipulación, y fortaleciendo la confianza en los sistemas.
3. Evaluación de la percepción del usuario: Las investigaciones también evalúan la percepción, actitudes y prácticas de seguridad y privacidad por parte de los usuarios finales de aplicaciones del IoT. Estos análisis revelan información valiosa sobre la aceptación y comprensión de las medidas de seguridad implementadas, así como posibles áreas de mejora o preocupaciones específicas de los usuarios.
4. Análisis del rendimiento de blockchain en la transmisión de información: En términos de velocidad de transmisión de la información es un área clave de estudio. Los análisis permiten evaluar si los algoritmos seleccionados introducen alguna degradación significativa en la velocidad de transmisión y, en caso afirmativo, determinar si es aceptable en comparación con los beneficios de seguridad obtenidos. Los resultados suelen mostrar un equilibrio entre seguridad robusta y eficiencia operativa.
5. Generación de recomendaciones y mejores prácticas: La culminación de estas investigaciones a menudo incluye la generación de recomendaciones y mejores prácticas para el uso de la criptografía en aplicaciones del IoT. Estos resultados suelen ofrecer directrices sobre la selección de protocolos y algoritmos criptográficos, consideraciones de rendimiento y la promoción de la conciencia y educación en seguridad y privacidad entre los usuarios finales y desarrolladores.

Discusión

La rápida expansión del Internet de las Cosas (IoT) ha transformado la forma en que interactuamos con nuestro entorno, pero también ha expuesto un sinfín de vulnerabilidades y desafíos de seguridad. Como se ha evidenciado, la naturaleza de la mayoría de los dispositivos IoT dificulta la implementación de soluciones de seguridad convencionales. La presente investigación busca abordar estas problemáticas mediante la integración de protocolos robustos como MQTT y la tecnología blockchain, complementados con una interfaz ReactJS.

Las vulnerabilidades lógicas o de software, resultado de errores de programación, diseño inseguro o falta de pruebas adecuadas, son una preocupación constante en el desarrollo de aplicaciones (Quiroz, 2017). Avenía (2017) menciona que son "debilidades en el código de un programa informático que pueden ser explotadas por atacantes para acceder a sistemas o datos de forma no autorizada o causar daño". En el contexto del IoT, donde los dispositivos se comunican sin intervención humana (Fadele Ayotunde et al., 2017), estos problemas se magnifican, generando desafíos en la autenticación, autorización, confidencialidad de datos y seguridad informática (Li, 2017). La recurrencia de intrusiones y vulnerabilidades aumentará con la complejidad de los sistemas IoT (Sahmim & Gharsellaoui, 2017).

A pesar de la existencia de protocolos de seguridad como TLS, su uso ha revelado vulnerabilidades, especialmente en el contexto del IoT (Huang et al., 2019). Investigaciones previas han demostrado que el protocolo MQTT, ampliamente utilizado en la capa de aplicación del IoT, es susceptible a ataques si la información no se cifra adecuadamente (Patel & Doshi, 2019; Kashyap et al., 2018). Esto subraya la necesidad crítica de métodos de seguridad innovadores y más resistentes. Incluso el popular protocolo SSL ha sido vulnerado (Kim et al., 2015).

La criptografía, definida como "la práctica y el estudio de cifrar y descifrar información mediante técnicas matemáticas" (González Díaz, 2010), es esencial para abordar las necesidades de seguridad en el IoT. Hernández (2018) menciona que existen sistemas de clave única (simétricos) y de clave pública (asimétricos). Mientras que la criptografía simétrica es eficiente y utiliza claves cortas, presenta desafíos en la gestión de claves en redes grandes y la necesidad de mantener el secreto en ambas partes (González Díaz, 2010). Por otro lado, la criptografía asimétrica, aunque más lenta, ofrece ventajas significativas al requerir que solo la clave privada se mantenga secreta y al facilitar la gestión de claves en grandes redes con la presencia de una tercera parte confiable (González Díaz, 2010). La seguridad de muchos esquemas de clave pública, como RSA, se basa en la dificultad de resolver problemas matemáticos, aunque la computación cuántica podría representar una amenaza futura (Aboud, 2009).

En este contexto, la tecnología blockchain emerge como una solución prometedora. Considerada como un libro mayor compartido e inmutable que facilita el proceso de registro de transacciones y de seguimiento de activos en una red, la blockchain garantiza que ningún participante pueda cambiar o falsificar una transacción una vez grabada. Esta inmutabilidad es clave para la integridad de los datos en el IoT. Sin embargo, la blockchain por sí sola no resuelve el problema de confianza asociado con los datos en sí mismos, lo que sugiere la necesidad de sistemas de reputación, como el propuesto TrustChain (Malik et al., 2019).

La integración de contratos inteligentes, escritos en lenguaje virtual y ejecutados de forma autónoma y automática en la blockchain, refuerza la seguridad, transparencia y confianza entre los firmantes, eliminando intermediarios y evitando malentendidos. Los contratos inteligentes se ejecutan en blockchain, lo que implica que los términos se almacenan en una base de datos distribuida y no pueden modificarse. El lenguaje Solidity, diseñado para la Máquina Virtual de Ethereum (EVM), es fundamental para el desarrollo de estos contratos.

El uso de plataformas de blockchain como servicio (BlockPaaS) se presenta como una respuesta innovadora para la implementación y prueba de soluciones blockchain en dispositivos IoT (Rajendra et al., 2023). Esto puede acelerar la investigación y el desarrollo, facilitando la experimentación y evaluación de las capacidades de blockchain en dispositivos IoT, lo que podría llevar a avances significativos en la seguridad y eficiencia de las aplicaciones IoT basadas en blockchain.

Conclusion

La investigación propuesta, centrada en el desarrollo de una plataforma de pruebas de seguridad para el Internet de las Cosas (IoT) mediante la integración de MQTT, blockchain y ReactJS, representa un paso fundamental hacia la solución de los desafíos de privacidad y seguridad que actualmente aquejan a este ecosistema interconectado. La necesidad de una metodología robusta es innegable, dada la creciente proliferación de dispositivos IoT y las vulnerabilidades inherentes a los protocolos de seguridad existentes.

Los resultados esperados de esta investigación son prometedores y directamente relevantes para fortalecer la seguridad en el IoT. La identificación de protocolos y algoritmos criptográficos óptimos, junto con la evaluación del impacto de la plataforma en la protección de la información, proporcionará directrices claras para futuros desarrollos. Además, la consideración de la percepción del usuario final es crucial para garantizar la aceptación y efectividad de las medidas de seguridad implementadas. El análisis del rendimiento de blockchain en términos de velocidad de transmisión de datos permitirá encontrar un equilibrio entre seguridad y eficiencia.

En última instancia, esta investigación contribuirá significativamente al avance del conocimiento en el campo de la seguridad en el IoT. Al proporcionar una solución práctica y evaluada rigurosamente, se espera promover la adopción de sistemas IoT más

seguros y resilientes, sentando las bases para una mayor confianza y protección de la privacidad en un mundo cada vez más digitalizado. La capacidad de detectar y mitigar amenazas de seguridad en un entorno controlado, junto con la demostración de un rendimiento superior, validará las hipótesis planteadas y consolidará la blockchain y la encriptación como la nueva frontera de la seguridad digital en el IoT.

Referencias

1. Aboud, S. J. (2009). An efficient method for attack RSA scheme. *2009 Second International Conference on the Applications of Digital Information and Web Technologies*, 587–591.

2. Hamza, A., Abdel-Halim, I. T., Sobh, M. A., & Bahaa-Eldin, A. M. (2021). A survey and taxonomy of program analysis for IoT platforms. *Ain Shams Engineering Journal*, *12*(4), 3725–3736. https://doi.org/10.1016/j.asej.2021.03.026

3. Al-Kuwari, M., Ramadan, A., Ismael, Y., Al-Sughair, L., Gastli, A., & Benammar, M. (2018). Smart-home automation using IoT-based sensing and monitoring platform. *IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering*, 1–6.

4. A.A. da Cruz, M., Rodrigues, J. J., Lorenz, P., Solic, P., Al-Muhtadi, J., & Albuquerque, V. (2019). A proposal for bridging application layer protocols to HTTP on IoT. *Future Generation Computer Systems*, 145–152.

5. Avenía, J. (2017). *Vulnerabilidades lógicas: Una clasificación y análisis de impacto en la seguridad informática*.

6. Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2015). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, 4–15.

7. Das, M. L., Saxena, A., & Gulati, V. P. (2004). A dynamic ID-based remote user authentication scheme. *IEEE Transactions on Consumer Electronics*, 629–631.

8. Fadele Ayotunde, A., Mazliza, O., Ibrahim Abaker, T. H., & Faiz, A. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 1–19.

9. Galas, E. M., & Gerardo, B. D. (2019). Implementing randomized salt on round key for corrected block tiny encryption algorithm (XXTEA). *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 795–799.

10. Glaroudis, D., Iossifides, A., & Chatzimisios, P. (2019). Survey, comparison and research challenges of IoT application protocols for smart farming. *Future Generation Computer Systems*, 1–14.

11. González Díaz, J. E. (2010). *Diseño e Implementación Eficiente del Emparejamiento Óptimo "Ate"*. Centro de Investigación y de Estudios Avanzados.

12. Hernández, R. G. B. L. (2018). AES como Estándar Internacional de Cifrado. *Tecnología Educativa Revista CONAIC*, *V*(I), 6.

13. Huang, J. K., Zhang, Z. X., Li, W. J., & Xin, Y. (2019). Assessment of the impacts of TLS vulnerabilities in the HTTPS. *Procedia Computer Science*, 512–518.

14. Kashyap, M., Sharma, V., & Gupta, N. (2018). Taking MQTT and NodeMcu to IOT: Communication in Internet of Things. *Procedia Computer Science*, 1611–1618.

15. Kim, S.-M., Goo, Y.-H., Kim, M.-S., Choi, S.-G., & Choi, M.-J. (2015). A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP. *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 487–490.

16. Li, J. (2017). Sistemas informáticos de generación futura. *FGCS*, 1–2.

17. Lohachab, A. (2019). ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. *Journal of Information Security and Applications*, 1–12.

18. Malik, S., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2019). TrustChain: Trust management in blockchain and IoT supported supply chains. *2019 IEEE International Conference on Blockchain (Blockchain)*, 184–193.

19. Martínez Peláez, R., Saavedra Benítez, Y. I., Velarde Alvarado, P., Ruiz Ibarra, J., Toral Cruz, H., & Aguilar Vargas, E. (2016). Secure Dynamic ID-based user authentication scheme using symmetric encryption and smart cards. *Revista Ventana Informática*, 31–46.

20. Mendoza T., J. C. (2008). Demostración de cifrado simétrico y asimétrico. *Ingenius. Revista de Ciencia y Tecnología*, 46–53.

21. Patel, C., & Doshi, N. (2019). Cryptanalysis and Improvement of Barman et al.'s Secure Remote User Authentication Scheme. *Circuits Systems and Signal Processing*, 604–610.

22. Rajendra, Y., Subramanian, V., & Shukla, S. K. (2023). *BlockPaaS: Blockchain Platform as a Service*.

23. Sahmim, S., & Gharsellaoui, H. (2017). Privacy and Security in Internet-based Computing: Cloud. *Procedia Computer Science*, 1516–1522.

24. Saravanan, G., Chandraprabha, S., Dinesh, C., & Ibrahim, A. M. (2021). IoT materials enabled indoor light illumination monitoring system. *Materials Today: Proceedings*, *45*, 6277–6281. https://doi.org/10.1016/j.matpr.2020.10.705

25. Song, H. H. (2020). Testing and Evaluation System for Cloud Computing Information Security Products. *Procedia Computer Science*, 84–87.

26. Sood, S. K., Sarje, A. K., & Singh, K. (2010). An Improvement of Liou et al.'s Authentication Scheme. *International Journal of Computer Applications*, 16–23.

27. Vignau, B., Khoury, R., Hallé, S., & Hamou-Lhadj, A. (2021). The evolution of IoT Malwares, from 2008 to 2019: Survey, taxonomy, process simulator and perspectives. *Journal of Systems Architecture*, *116*(102143), 102143. https://doi.org/10.1016/j.sysarc.2021.102143