ISAA Literature Survey

| S. No. | Title | Author | Conference/Journal | Limitations |
| --- | --- | --- | --- | --- |
| 1 | Secure blockchainized Decentralized Messaging Application (DMApp) for Educational Institute (2023) | Jani, C., Mishra, R. A., & Kalla, A. (2023) | Software Impacts, 16 | The developed DMApp is a first-level implementation with the potential limitation of scalability. |
| 2 | Decentralized Chat Application using Blockchain Technology (2023) | Khalkar, K., Dhake, N., Kelzarkar, S., & Shinde, T. | [Conference/Journal Name] | The proposed decentralized chat application addresses the centralization issues of traditional messaging platforms. However, specific limitations were not explicitly mentioned in the abstract. |
| 3 | Blockchain-based Secure Communication Application Proposal: Cryptouch (2018) | Sarıtekin, R. A., Karabacak, E., Durgay, Z., & Karaarslan, E. | 2018 6th International Symposium on Digital Forensic and Security (ISDFS) | The study proposes Cryptouch, a communication application based on blockchain technology, utilizing InterPlanetary File System (IPFS) to overcome blockchain limits. It aims for transparent, reliable, fast, and uninterrupted communication. Specific limitations were not detailed in the abstract. |
| 4 | A Decentralized Application for Secure Messaging in a Trustless Environment (2018) | Abdulaziz, M., Çulha, D., & Yazici, A. | 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT) | The article proposes a decentralized messaging application using the Ethereum Whisper protocol, designed to ensure the integrity, confidentiality, and availability of data in a trustless environment. The application aims to send encrypted messages securely and anonymously, deploying on the Ethereum platform. Its distributed nature and adaptable communication protocol make it resistant to most suppression tactics. Specific limitations were not explicitly outlined in the abstract. |
| 5 | Security Issues of a Decentralized Blockchain-Based Messaging System (2021) | González, C. E. C., & Romero, F. J. C. | 2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI) | The paper presents a decentralized messaging system based on blockchain technology. It enables users to securely send and receive digital messages in the network. To address privacy concerns, messages are encrypted using public-key cryptography, ensuring anonymity for both sender and recipient. The proposed system incorporates a browser-based user interface for seamless peer-to-peer interaction. Specific security issues, if any, are not explicitly mentioned in the abstract. |
| 6 | Grasping the Concept of Decentralized Systems for Instant Messaging (2022) | Gebhardt, L., Leinweber, M., Jacob, F., & Hartenstein, H. | Proceedings of the 17th Workshop in Primary and Secondary Computing Education | The practical report explores the impact of centralized, distributed, and decentralized system approaches on sovereignty and responsibilities in Internet-based services. Focusing on instant messaging, the authors analyze three algorithms with varying degrees of centralization. They propose a teaching activity, Klemmchat, using computer science unplugged to educate students on key aspects and trade-offs. Results from teaching in two classes (grades 11 and 12) show the activity's suitability for conveying trade-offs, yet it remains uncertain if the understanding gained affects usage decisions. Specific limitations of the proposed teaching approach were not explicitly mentioned in the abstract. |
| 7 | Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees (2021) | Weidner, M., Kleppmann, M., Hugenroth, D., & Beresford, A. R. | Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security | The paper addresses the challenges of secure group messaging in decentralized networks, focusing on end-to-end encryption for group communication. It adapts existing work for a decentralized model, introducing decentralized continuous group key agreement (DCGKA) as a cryptographic primitive. The authors provide a practical construction of a DCGKA protocol, prove its security, and describe how to build a full messaging protocol from DCGKA. The protocol achieves forward secrecy and post-compromise security in the face of device compromise. A prototype implementation is evaluated for practical efficiency. Specific limitations of the proposed protocol were not explicitly mentioned in the abstract. |
| 8 | Secure Messaging Platform Based on Blockchain (2020) | Ellewala, U. P., Amarasena, W. D. H. U., Lakmali, H. S., Senanayaka, L. M. K., & Senarathne, A. N. | 2020 2nd International Conference on Advancements in Computing (ICAC) | The paper addresses the challenge of maintaining secure communication in organizations, emphasizing the risk of using unsecured applications in workplaces. It highlights the limitations of publicly available communication platforms in regulating, tracking, and scaling organizational communication, leading to potential cross-industry system risks. The authors propose a chat application leveraging blockchain technology for enterprise-level communication, aiming to enhance confidentiality, integrity, availability, and advanced auditing features. Specific limitations of the proposed secure messaging platform were not explicitly mentioned in the abstract. |
| 9 | Chat Application Security: Implementing Blockchain-based End-to-End Encryption (2023) | Pansara, P., Patel, R., Shah, K., Jhaveri, R., & Parmar, V. | 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) | The paper addresses security and privacy concerns in instant messaging applications by proposing the use of blockchain technology in combination with Elliptic Curve Diffie-Hellman for End-to-End Encryption. The decentralized and secure nature of blockchain, along with the strong key agreement from Elliptic Curve Diffie-Hellman, ensures that only the intended recipient has access to encrypted messages, providing an additional layer of security compared to traditional solutions. The implementation and performance of the proposed solution are evaluated, demonstrating its feasibility and effectiveness in securing instant messaging communication. Specific limitations of the proposed solution were not explicitly mentioned in the abstract. |
| 10 | Chatease: A Blockchain-based Chat Application (2023) | Kuchimanchi, A., Vagdevi, M., Reddy, M., Avugaddi, G., & Kumar, S. S. | 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) | The paper addresses traditional security issues in message exchange through unsecured channels, emphasizing concerns about information gathering and centralized data storage in most applications. It proposes Chatease, a blockchain-based chat application, leveraging blockchain technology for data privacy, censorship resistance, immutability, and decentralization. Each network node receives a copy of the data directly into the blockchain, and only approved persons with private keys can access the data, eliminating the need for trustworthy intermediaries. The software demonstrates how to hash and mine messages in the blockchain, utilizing a distributed hash table (DHT) for decentralized storage and quick lookup. The paper provides insights into building a decentralized chat program. Specific limitations of Chatease were not explicitly mentioned in the abstract. |
| 11 | Uncuffed: A Blockchain-based Secure Messaging System (2021) | Dimitriadis, V., Maglaras, L., Polemi, N., Kantzavelou, I., & Ayres, N. | Proceedings of the 25th Pan-Hellenic Conference on Informatics | The article addresses security issues in messaging systems used in critical applications, such as communication in autonomous vehicles. It proposes Uncuffed, a blockchain-based secure messaging system using the Bitcoin protocol to prevent personal data leakage. The selected mechanism leverages the decentralization of blockchain for data storage and facilitates private interchange of secure messages and images. The UNCUFFED system supports two groups of users, Miners and Clients, where Miners collect rewards as active blockchain members, and Clients send messages out of the platform. Specific limitations of the proposed Uncuffed system were not explicitly mentioned in the abstract. |
| 12 | WebRTC-based Decentralized Chat Application with Minimal Latency (2022) | Berg, D. R., Tharunraj, M., Kumar, B. R., Sumalatha, M. R., Palivela, L. H., & Karthikeyaa, P. V. V. | 2022 International Conference on Intelligent Innovations in Engineering and Technology (ICIIET) | The WebRTC-based chat is a decentralized chat application designed for minimal latency, low packet loss and jitter, high reliability, and scalability. It implements a Complex Event Processing (CEP)-based session establishment, message transmission, and session termination scheme. The application incorporates a peer discovery scheme and a Routing Information Protocol (RIP) traversal scheme for scalability and robustness. End-to-end encryption with AES256 is employed for security. The WebRTC specification facilitates peer-to-peer communication over the Web, and the application uses it to communicate with peers, storing and retrieving data from a decentralized database. Gun.eco, providing the AXE (Advanced eXchange Equation) API, is proposed for data redundancy and consistency in the decentralized database, enabling the chat application to work with minimal latency and real-time updates. The proposed application aims to help users in remote places with poor network connectivity connect seamlessly with others. Specific limitations of the proposed WebRTC-based chat application were not explicitly mentioned in the abstract. |
| 13 | Preventing the Man-in-the-Middle Attack on Internet Communication using Blockchain Technology (2019) | Kulkarni, O. | NORMA eResearch | The paper addresses the security issues in internet communication, focusing on the rise of tampering and Man-in-the-Middle (MITM) attacks despite the use of HTTPS. It explores the ability to compromise a single trusted certificate in HTTPS, leading to the proposed solution of preventing MITM attacks using notary systems in HTTPS with the integration of blockchain technology. The paper explains the working of HTTPS and how MITM attacks are carried out, presents the developed solution, and evaluates the system while acknowledging some shortcomings and suggesting future work. Specific limitations of the proposed solution were not explicitly mentioned in the abstract. |
| 14 | Blockchain-based Messenger for Providing Secure Peer-to-Peer Communication Facilities (2019) | Kilichenko, H., & Komleva, N. O. | Materials of the Ninth International Scientific Conference of Students and Young Scientists | The work evaluates the applicability of blockchain technology for achieving secure private communication between peers. While the standard client-server architecture has proven efficient, the central point of control raises privacy concerns. The paper explores ways to address this issue in a distributed system, considering the possibilities and limitations of blockchain technology in enhancing secure peer-to-peer communication. Specific limitations of the proposed blockchain-based messenger were not explicitly mentioned in the abstract. |
| 15 | Group Communication With Secure Process Based On Identity Crypto System (2020) | Malathi, G., & Priya, D. E. N. | Ilkogretim Online, 19(2), 1888-1893 | The paper addresses the critical nature of group communication in applications such as board meetings, group discussions, and teleconferencing. It focuses on collaborative and distributed applications for secure group communication, emphasizing the use of Group Key Agreement (GKA) protocols, both conventional and unconventional, to manage secure group keys and dynamics. The asymmetric Group Key Agreement (AGKA) is introduced, allowing a group of members to establish a public group encryption key dynamically in an identity-based cryptosystem for group communication. The introduction section briefly mentions the relevance of Big Data in organizational efficiency but does not provide specific details related to the main topic of group communication with a secure process based on an identity crypto system. Specific limitations of the proposed secure group communication process were not explicitly mentioned in the abstract. |
| 16 | A Blockchain-Based Secure Communication Framework for Community Interaction (2021) | Sharma, R., Wazid, M., & Gope, P. | Journal of Information Security and Applications, 58, 102790 | The paper addresses the impact of globalization on network communication and the use of closed and centralized systems, leading to privacy issues. It focuses on the inadequacy of existing communication frameworks for community interactions based on intermediary trust and proposes a blockchain-based secure communication framework. The framework utilizes blockchain with a tamper-proof distributed ledger and enhances security with the RAFT algorithm, implementing a key management system. An android application is developed based on the proposed framework for real-time usability. The provided security analysis demonstrates resilience against various possible attacks, and performance comparisons show the superiority of the proposed framework over similar approaches. Specific limitations of the proposed blockchain-based secure communication framework were not explicitly mentioned in the abstract. |
| 17 | A Design of Medical Information Sharing Model Based on Blockchain Technology (2018) | Jiang, H., Peng, H., & Dian, S. | IOP Conference Series: Materials Science and Engineering, 428(1), 012006 | The paper addresses issues in the sharing of medical data within the traditional medical industry, highlighting the lack of communication among medical institutions and inefficient use of resources. To tackle this problem, the authors propose a medical information sharing model based on blockchain technology. The model establishes a peer-to-peer network connecting different medical institutions and nodes, utilizing two associated blockchains to store medical data digests and requests. Each node in the network can search for medical information across distributed medical institutions, enhancing integration, transparency, and sharing of medical data. The traditional Proof of Work (POW) algorithm is improved by introducing a double-chain structure to reduce block confirmation time. Specific limitations of the proposed medical information sharing model were not explicitly mentioned in the abstract. |
| 18 | A Formal Security Analysis of the Signal Messaging Protocol (2020) | Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. | Journal of Cryptology, 33, 1914-1983 | The paper presents a formal security analysis of the Signal protocol, a cryptographic messaging protocol providing end-to-end encryption for instant messaging in various platforms with over 1 billion active users. Signal incorporates uncommon security properties such as "future secrecy" and "post-compromise security," achieved through ratcheting, where session keys are updated with every message sent. The formal analysis focuses on Signal's initial extended triple Diffie–Hellman (X3DH) key agreement and Double Ratchet protocols as a multi-stage authenticated key exchange protocol. The authors extract a formal description of the abstract protocol, define a security model capturing the "ratcheting" key update structure, and prove the security of Signal's key exchange core in the model. The analysis finds no major flaws in the design, serving as a foundation for future analyses of this widely adopted protocol. Specific limitations of the Signal protocol were not explicitly mentioned in the abstract. |
| 19 | CoCoA: Concurrent Continuous Group Key Agreement (2022) | Alwen, J., Auerbach, B., Noval, M. C., Klein, K., Pascual-Perez, G., Pietrzak, K., & Walter, M. | Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 815-844). Springer International Publishing | CoCoA introduces a novel scheme for concurrent updates in group key agreement, addressing the challenge of key rotations in large groups. While the proposed approach offers T concurrent updates without adding future operational costs, it requires an increased number of rounds (up to log(n)), potentially impacting the efficiency of the protocol. Additionally, the reliance on a server-aided CGKA introduces new mechanisms for robustness, necessitating careful consideration of trust issues. |
| 20 | Content Addressed P2P File System for the Web with Blockchain-based Meta-data Integrity (2019) | Rahalkar, C., & Gujar, D. | 2019 International Conference on Advances in Computing, Communication and Control (ICAC3) (pp. 1-4). IEEE | This paper addresses the limitations of the standard HTTP protocol in the exponentially scaled World Wide Web by proposing a content-addressed P2P file system called IPFS. IPFS enables decentralized file storage, allowing retrieval from multiple sources and saving bandwidth. The integration of IPFS with Blockchain for meta-data integrity ensures the preservation of data integrity on the Web, offering a decentralized and secure approach to data storage and distribution. |
| 21 | DeExam: A Decentralized Exam Administration Model using Public Blockchain (2021) | Kaneko, Y., Tanaka, S., Kimura, T., Okumura, J., Azuchi, S., & Osada, S. | Proceedings of the 2021 3rd Blockchain and Internet of Things Conference (pp. 1-7) | DeExam presents a sustainable exam administration model leveraging a public blockchain to enhance reliability and transparency. The blockchain records hash values of correct answers, decision conditions, and results, ensuring tamper-proof exam records. Implementation using Bitcoin Core and testing in a CTF competition with 100+ participants demonstrated the method's viability, providing a decentralized approach to exam administration. |
| 22 | Hybrid Blockchain-enabled Security in Cloud Storage Infrastructure using ECC and AES Algorithms (2022) | Bakro, M., Bisoy, S. K., Patel, A. K., & Naal, M. A. | Blockchain based Internet of Things, 139-170 | The paper explores the security aspects of cloud storage in the context of the Internet of Things (IoT) and cloud computing. Implementing a hybrid security system with blockchain technology and cryptographic algorithms ECC and AES, the framework aims to enhance data security and efficiency. The analysis suggests that the proposed approach offers superior security features compared to other methods, addressing the evolving challenges in data protection within the growing IoT and cloud computing landscape. |
| 23 | Interoperability in End-to-End Encrypted Messaging (2023) | Len, J., Ghosh, E., Grubbs, P., & Rösler, P. | Cryptology ePrint Archive | The paper addresses the challenges posed by the interoperability requirement in the Digital Markets Act (DMA) for end-to-end encrypted messaging apps. Focusing on three main areas—identity resolution, protocol establishment, and abuse prevention—the authors identify security and privacy requirements, review existing proposals, and propose their design for an interoperable encrypted messaging system. With the DMA's mandate potentially taking effect in mid-2024, the paper highlights the need for research to understand and address the associated security, privacy, and functionality issues. |
| 24 | More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema (2018) | Rösler, P., Mainka, C., & Schwenk, J. | 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 415-429). IEEE | The paper addresses the cryptographic mechanisms and security guarantees of secure group communication in instant messaging, focusing on protocols like Signal, WhatsApp, and Threema. A comprehensive security model is proposed, revealing shortcomings in the analyzed protocols concerning security and reliability goals. The analysis emphasizes the lack of end-to-end protection for communication integrity and group management in these widely used group instant messaging protocols. Generic countermeasures are suggested to enhance the protocols, emphasizing the need for attention to security aspects in group communication. |
| 25 | Optimal Channel Security Against Fine-grained State Compromise: The Safety of Messaging (2018) | Jaeger, J., & Stepanovs, I. | Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38 (pp. 33-62). Springer International Publishing | The paper focuses on achieving optimal security for a cryptographic channel in the presence of adversaries capable of arbitrarily and repeatedly learning the secret state of communicating parties. It introduces a formal security definition and a construction that outperforms the Signal Double Ratchet Algorithm and other known channel constructions in terms of security against state compromise. The work introduces novel forms of public-key encryption and digital signatures that dynamically update their keys over time, contributing to enhanced security in bidirectional cryptographic channels. |
| 26 | Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology (2022) | Fathiyana, R. Z., Yutia, S. N., & Hidayat, D. J. | JOIV: International Journal on Informatics Visualization, 6(1), 109-116 | The paper presents a prototype for an Integrated National Identity Storage Security System in Indonesia utilizing blockchain technology. The existing centralized identity storage system faces challenges such as data replication and redundancy. The proposed blockchain-based solution aims to integrate the national identity system, addressing these challenges and providing advantages in population data utilization programs. The system ensures security, integrity, and transparency in sharing and updating population data, reducing the risk of data misuse. Blockchain's decentralized nature contributes to increased data security and transparency in information management. |
| 27 | Security Analysis and Improvements for the IETF MLS Standard for Group Messaging (2020) | Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. | Annual International Cryptology Conference (pp. 248-277). Springer International Publishing | The paper conducts a security analysis of the TreeKEM protocol, a core component of the IETF MLS standard for secure group messaging. While TreeKEM achieves post-compromise security (PCS), the paper identifies shortcomings in forward secrecy (FS). The authors propose a modification to TreeKEM, drawing inspiration from recent work, to address the FS issues without significant efficiency degradation. The modified TreeKEM achieves optimal continuous group key agreement (CGKA) security, including FS and PCS, and the paper outlines how a CGKA protocol can be utilized in designing a comprehensive secure group messaging protocol. |
| 28 | Tawki: Towards Self-Sovereign Social Communication (2019) | Westerkamp, M., Göndör, S., & Küpper, A. | 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON) (pp. 29-38). IEEE | Tawki introduces a decentralized service architecture for social communication, aiming to give users full control over their personal data. The platform utilizes personal data storages accessible through a unified API, allowing peer-to-peer communication without reliance on centralized platforms. The use of Ethereum Name Service (ENS) enhances identity management and data storage discovery, ensuring security against censorship and third-party control through the immutability of the Ethereum Blockchain. |
| 29 | Towards Bidirectional Ratcheted Key Exchange (2018) | Poettering, B., & Rösler, P. | Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38 (pp. 3-32). Springer International Publishing | The paper addresses limitations in prior work on ratcheted key exchange (RKE) by introducing alternative security definitions for both unidirectional and bidirectional RKE. The proposed definitions aim for strong and realistic notions, covering concurrent operation of both participants. The article also presents secure instantiations, overcoming weaknesses in existing protocols and models. |
| 30 | On Ends-to-Ends Encryption: Asynchronous Group Messaging with Strong Security Guarantees (2018) | Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. | Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (pp. 1802-1819) | The paper addresses the security concerns in group messaging by introducing Asynchronous Ratcheting Trees (ART), a design that achieves post-compromise security in realistic, asynchronous group messaging systems. ART utilizes tree-based Diffie-Hellman key exchange, allowing a secure derivation of shared symmetric keys in groups with members who are not online simultaneously. The proposed solution scales effectively to groups with thousands of members and has garnered interest in industry and standardization bodies, forming the basis for IETF RFC drafts and a working group. |

## APA

1. Jani, C., Mishra, R. A., & Kalla, A. (2023). Secure blockchainized Decentralized Messaging Application (DMApp) for Educational Institute. *Software Impacts*, *16*, 100494.
2. Khalkar, K., Dhake, N., Kelzarkar, S., & Shinde, T. Decentralized Chat Application using Blockchain Technology.
3. Sarıtekin, R. A., Karabacak, E., Durgay, Z., & Karaarslan, E. (2018, March). Blockchain based secure communication application proposal: Cryptouch. In *2018 6th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-4). Ieee.
4. Abdulaziz, M., Çulha, D., & Yazici, A. (2018, December). A decentralized application for secure messaging in a trustless environment. In *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)* (pp. 1-5). IEEE.
5. González, C. E. C., & Romero, F. J. C. (2021, September). Security Issues of a Decentralized Blockchain-Based Messaging System. In *2021 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)* (pp. 1-4). IEEE.
6. Gebhardt, L., Leinweber, M., Jacob, F., & Hartenstein, H. (2022, October). Grasping the Concept of Decentralized Systems for Instant Messaging. In *Proceedings of the 17th Workshop in Primary and Secondary Computing Education* (pp. 1-6).
7. Weidner, M., Kleppmann, M., Hugenroth, D., & Beresford, A. R. (2021, November). Key agreement for decentralized secure group messaging with strong security guarantees. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2024-2045).
8. Ellewala, U. P., Amarasena, W. D. H. U., Lakmali, H. S., Senanayaka, L. M. K., & Senarathne, A. N. (2020, December). Secure messaging platform based on blockchain. In *2020 2nd International Conference on Advancements in Computing (ICAC)* (Vol. 1, pp. 317-322). IEEE.
9. Pansara, P., Patel, R., Shah, K., Jhaveri, R., & Parmar, V. (2023, March). Chat Application Security: Implementing Blockchain-based End-to-End Encryption. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 496-500). IEEE.
10. Kuchimanchi, A., Vagdevi, M., Reddy, M., Avugaddi, G., & Kumar, S. S. (2023, May). Chatease: A Blockchain based Chat Application. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 1171-1176). IEEE.
11. Dimitriadis, V., Maglaras, L., Polemi, N., Kantzavelou, I., & Ayres, N. (2021, November). Uncuffed: A Blockchain-based Secure Messaging System. In *Proceedings of the 25th Pan-Hellenic Conference on Informatics* (pp. 340-345).
12. Berg, D. R., Tharunraj, M., Kumar, B. R., Sumalatha, M. R., Palivela, L. H., & Karthikeyaa, P. V. V. (2022, September). WebRTC-based Decentralized Chat Application with Minimal Latency. In *2022 International Conference on Intelligent Innovations in Engineering and Technology (ICIIET)* (pp. 210-215). IEEE.
13. Kulkarni, O. (2019). Preventing the Man-in-the-Middle Attack on Internet Communication using Blockchain Technology.
14. Kilichenko, H., & Komleva, N. O. (2019). Blockchain-based messenger for providing secure peer-to-peer communication facilities. In *Materials of the Ninth International Scientific Conference of Students and Young Scientists* (pp. 51-52).
15. Malathi, G., & Priya, D. E. N. (2020). Group Communication With Secure Process Based On Identity Crypto System. *Ilkogretim Online*, *19*(2), 1888-1893.
16. Sharma, R., Wazid, M., & Gope, P. (2021). A blockchain based secure communication framework for community interaction. *Journal of Information Security and Applications*, *58*, 102790.
17. Jiang, H., Peng, H., & Dian, S. (2018, September). A design of medical information sharing model based on blockchain technology. In *IOP Conference Series: Materials Science and Engineering* (Vol. 428, No. 1, p. 012006). IOP Publishing.
18. Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2020). A formal security analysis of the signal messaging protocol. *Journal of Cryptology*, *33*, 1914-1983.
19. Alwen, J., Auerbach, B., Noval, M. C., Klein, K., Pascual-Perez, G., Pietrzak, K., & Walter, M. (2022, May). CoCoA: concurrent continuous group key agreement. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 815-844). Springer International Publishing.
20. Rahalkar, C., & Gujar, D. (2019, December). Content addressed P2P file system for the web with blockchain-based meta-data integrity. In *2019 International Conference on Advances in Computing, Communication and Control (ICAC3)* (pp. 1-4). IEEE.
21. Kaneko, Y., Tanaka, S., Kimura, T., Okumura, J., Azuchi, S., & Osada, S. (2021, July). DeExam: A Decentralized Exam Administration Model using Public Blockchain. In *Proceedings of the 2021 3rd Blockchain and Internet of Things Conference* (pp. 1-7).
22. Bakro, M., Bisoy, S. K., Patel, A. K., & Naal, M. A. (2022). Hybrid blockchain-enabled security in cloud storage infrastructure using ECC and AES algorithms. *Blockchain based Internet of Things*, 139-170.
23. Len, J., Ghosh, E., Grubbs, P., & Rösler, P. (2023). Interoperability in End-to-End Encrypted Messaging. *Cryptology ePrint Archive*.
24. Rösler, P., Mainka, C., & Schwenk, J. (2018, April). More is less: On the end-to-end security of group chats in signal, whatsapp, and threema. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 415-429). IEEE.
25. Jaeger, J., & Stepanovs, I. (2018). Optimal channel security against fine-grained state compromise: The safety of messaging. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38* (pp. 33-62). Springer International Publishing.
26. Fathiyana, R. Z., Yutia, S. N., & Hidayat, D. J. (2022). Prototype of Integrated National Identity Storage Security System in Indonesia using Blockchain Technology. *JOIV: International Journal on Informatics Visualization*, *6*(1), 109-116.
27. Alwen, J., Coretti, S., Dodis, Y., & Tselekounis, Y. (2020, August). Security analysis and improvements for the IETF MLS standard for group messaging. In *Annual International Cryptology Conference* (pp. 248-277). Springer International Publishing.
28. Westerkamp, M., Göndör, S., & Küpper, A. (2019, April). Tawki: Towards self-sovereign social communication. In *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)* (pp. 29-38). IEEE.
29. Poettering, B., & Rösler, P. (2018). Towards bidirectional ratcheted key exchange. In *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part I 38* (pp. 3-32). Springer International Publishing.
30. Cohn-Gordon, K., Cremers, C., Garratt, L., Millican, J., & Milner, K. (2018, October). On ends-to-ends encryption: Asynchronous group messaging with strong security guarantees. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1802-1819).