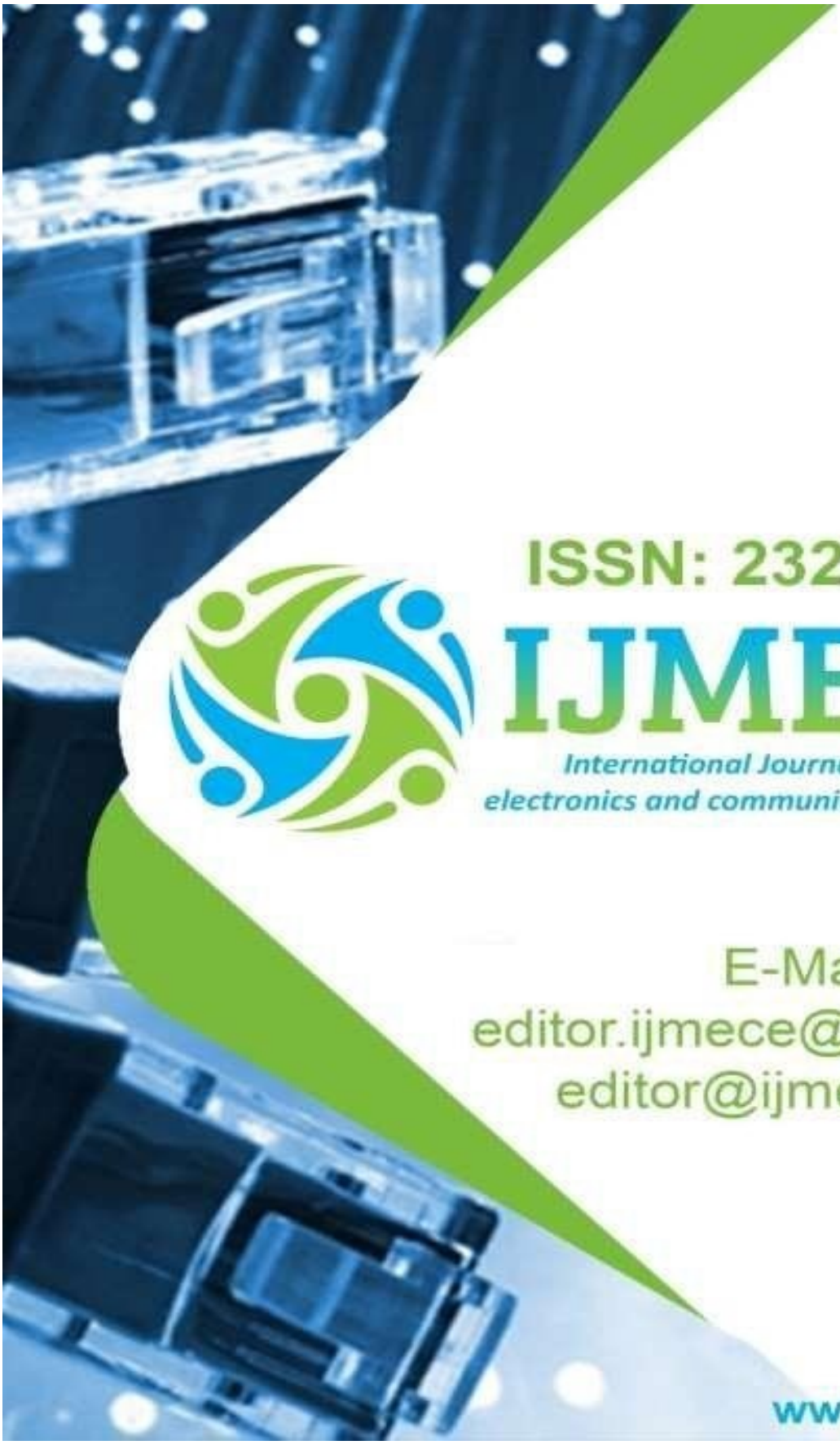


ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN2321-2152
www.ijmece .com
Vol 6, Issue 3, 2018

CLOUD-DRIVEN SMART HEALTHCARE SYSTEM WITH PUBLICLY VERIFIABLE INTERNET OF MEDICAL THINGS SECURITY

Maltesh Kamatar, Vasanthamma. G, Naveen Kumar. H
Asst. Professor, Assco. Professor, Asst. Professor
maltkpl@gmail.com, gvasreddy@gmail.com, navee2312@gmail.com
Department of CSE, Proudhadevaraya Institute of Technology, Abheraj Baldota Rd, Indiranagar, Hosapete, Karnataka-583225

ABSTRACT

Through the smooth interconnection of biomedical sensors in the field of e-health, the introduction of Internet-of-Medical-Things (IoMT) technology has greatly improved people's quality of life. At the same time, moving patient records to the cloud is another significant development in e-health. Despite the great potential of these breakthroughs, there are several obstacles to their widespread use, the most significant of which being concerns about the confidentiality of patients' medical records and the limited resources available from sensor devices. With an emphasis on public verifiability, this article presents a state-of-the-art smart healthcare system that is efficient, safe, and centred on the cloud and enabled by IoMT.

To strengthen data transmission security, this system introduces and uses an escrow-free identity-based aggregate signcryption (EF-IDASC) approach, which is a major innovation. With the help of signcryption, the new EF-IDASC scheme securely aggregates medical data retrieved from various implanted sensors on a patient's body. Then, using a smartphone, the aggregated data is sent to a medical cloud server. This is all part of the proposed smart healthcare system. The solution addresses a significant challenge in the integration of IoMT and cloud technologies for healthcare applications by ensuring the maximum privacy by securing the patient's identity and medical data.

In order to provide a thorough overview of its features, this paper analyses the performance of the proposed smart healthcare system in detail, paying close attention to energy usage. And to top it all off, we compare the proposed EF-IDASC scheme's performance against other relevant schemes in a comparative study. The purpose of these assessments is to highlight the proposed cloud-centric IoMT-enabled smart healthcare system's practicality, security, and efficiency in handling the complicated

needs of modern e-healthcare situations.

I.INTRODUCTION

The convergence of Internet-of-Things (IoT) technology with healthcare, particularly in the form of the Internet-of-Medical-Things (IoMT), has ushered in a transformative era in the field of e-health. Among the notable advancements, the integration of biomedical sensors and the outsourcing of medical data to the cloud stand out as pivotal contributors to improved healthcare services. However, the realization of these technologies in the context of e-healthcare encounters challenges, with paramount concerns revolving around the privacy of medical data and the resource constraints inherent in sensor devices.

This article delves into the dynamic landscape of e-healthcare, presenting a state-of-the-art smart healthcare system that intricately combines the power of IoMT with cloud-centric solutions, placing a particular emphasis on ensuring public verifiability. At the heart of this innovative system lies an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme, a novel contribution detailed within this article. The primary objective is to establish a secure, efficient, and privacy-centric framework for transmitting medical data seamlessly.

The proposed smart healthcare system orchestrates a sophisticated process wherein medical data from multiple sensors, embedded on a patient's body, is securely retrieved, signcrypted, and aggregated using the EF-IDASC scheme. Subsequently, this consolidated information is outsourced to a medical cloud server via a smartphone. A distinctive feature of the system is its unwavering commitment to safeguarding patient identity and medical data, addressing a critical concern inherent in the integration of IoMT and cloud technologies.

To provide a comprehensive evaluation, the article conducts a detailed performance analysis, with a specific focus on energy consumption. Furthermore, the proposed EF-IDASC scheme is rigorously compared with other related schemes to gauge its efficacy and applicability in the context of securing medical data transmission. This research aims to contribute valuable insights into the development of secure and efficient cloud-centric IoMT-enabled smart healthcare systems,

fostering advancements in the delivery of contemporary e-healthcare services.

II.LITERATURE REVIEW

A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System With Public Verifiability,Mahender Kumar; Satish Chand,The potential of the Internet-of-Medical-Things (IoMT) technology for interconnecting the biomedical sensors in e-health has ameliorated the people's living standards. Another technology recognized in the recent e-healthcare is outsourcing the medical data to the cloud. There are, however, several stipulations for adopting these two technologies. The most difficult is the privacy of medical data and the challenge resulting from the resource constraint environment of sensor devices. In this article, we present the state-of-the-art secure and efficient cloud-centric IoMT-enabled smart healthcare system with public verifiability. The system novelty implements an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme to secure data transmission, which is also proposed in this article. The proposed smart healthcare system fetches the medical data from multiple sensors implanted on the patient's body, signcrypts and aggregates them under the proposed EF-IDASC scheme, and outsources the data on the medical cloud server via smartphone. The system does not reveal any information about the identity and medical data of the patient. We further analyze the performance of the proposed smart healthcare system in terms of energy consumption. Moreover, we compare the performance of the proposed EF-IDASC scheme with other related schemes.

III.EXISTING SYSTEM

In the current landscape of healthcare technology, various implementations of Internet-of-Medical-Things (IoMT) have been integrated to enhance patient care and streamline medical processes. One prevalent approach involves the utilization of IoT devices and sensors for real-time health monitoring, allowing continuous data collection. Additionally, cloud computing has become an instrumental component in storing and processing vast amounts of medical data, offering scalability and accessibility. However, the existing systems face challenges related to security, privacy, and efficient data transmission, especially when outsourcing medical data to the cloud. The security concerns primarily revolve around the protection of sensitive medical information during

data transmission and storage. Traditional encryption methods are often employed, but they may not provide the necessary level of security against sophisticated cyber threats. Moreover, the identity and medical data of patients may be at risk during the transmission process.

Efficiency becomes a crucial factor as the volume of medical data generated by IoMT devices increases. The existing systems may encounter bottlenecks in terms of data processing, leading to delays and potential disruptions in healthcare services. Furthermore, ensuring public verifiability, which is essential for building trust in the system, may be lacking in conventional approaches. In summary, while existing systems leverage IoMT and cloud computing for enhanced healthcare services, there exists a need for a more secure, efficient, and publicly verifiable framework. The integration of an escrow-free identity-based aggregate signcryption (EF-IDASC) scheme, as proposed in the project, introduces a novel solution to address the limitations of the current healthcare systems. This scheme aims to enhance the security of data transmission, protect patient privacy, and ensure efficient utilization of cloud resources in the context of Internet-of-Medical-Things-enabled smart healthcare systems.

IV.PROPOSED SYSTEM

The proposed system, "Secure and Efficient Cloud-Centric Internet of Medical Things (IoMT)-Enabled Smart Healthcare System with Public Verifiability," introduces a novel framework designed to overcome the limitations of existing healthcare systems, ensuring enhanced security, efficiency, and public verifiability. This innovative system integrates state-of-the-art technologies to address the challenges associated with data transmission, privacy, and resource utilization in the IoMT and cloud computing landscape.

Key Components of the Proposed System:

Escrow-Free Identity-Based Aggregate Signcryption (EF-IDASC) Scheme:

The core innovation of the proposed system lies in the implementation of an EF-IDASC scheme. This cryptographic scheme is designed to provide a robust and secure method for aggregating and signcrypting medical data, ensuring the

confidentiality and integrity of information during transmission.

IoMT-Enabled Data Collection:
The proposed system seamlessly integrates with IoMT devices and sensors embedded on a patient's body to collect real-time medical data. This includes vital signs, diagnostic information, and other relevant health metrics.

Dynamic Data Aggregation:
Leveraging the EF-IDASC scheme, the system dynamically aggregates medical data from multiple sensors. This ensures that the aggregated information remains secure, and the identity of the patient is protected throughout the data transmission process.

Cloud-Centric Storage and Processing:
The system utilizes cloud computing resources for efficient storage and processing of the aggregated medical data. Cloud-based servers facilitate scalability, ensuring that the system can handle the increasing volume of data generated by IoMT devices.

Secure Data Outsourcing via Smartphone:
The proposed system employs smartphones as secure gateways for outsourcing aggregated medical data to the cloud server. This adds an additional layer of security and convenience for patients and healthcare providers.

Privacy Preservation:
The system prioritizes patient privacy by not revealing any information about the identity and medical data of the patient during the transmission and storage processes. This is achieved through the secure implementation of the EF-IDASC scheme.

Public Verifiability Mechanism:
To instill trust and transparency, the proposed system incorporates a public verifiability mechanism. This ensures that stakeholders, including patients and authorized entities, can verify the integrity and authenticity of the aggregated medical data.

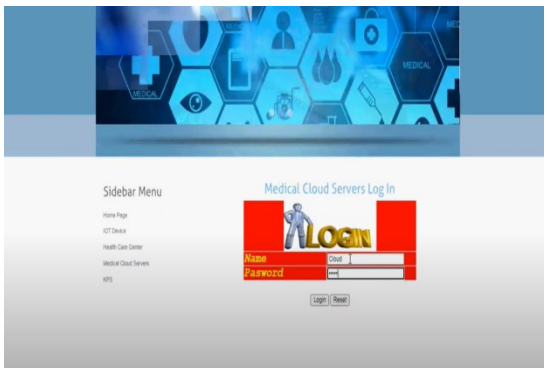
Performance Analysis:
The proposed system undergoes a comprehensive performance analysis, focusing on energy consumption, processing speed, and overall efficiency. This analysis provides insights into the system's capabilities and its suitability for real-world healthcare applications.

ISSN2321-2152
www.ijmece .com
Vol 6, Issue 3, 2018

Through the integration of these components, the proposed system aims to establish a new standard in secure, efficient, and publicly verifiable IoMT-enabled smart healthcare systems. The innovative use of the EF-IDASC scheme ensures that the system addresses the intricacies of data transmission, privacy concerns, and resource optimization, paving the way for advancements in contemporary e-healthcare scenarios.

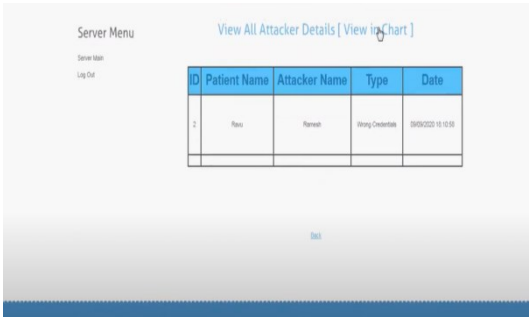
User Registration:

Facilitate a user-friendly registration process, collecting necessary information such as name, contact details, and other relevant details. Verify user identity through secure verification methods.



Verification Process:

Implement a secure verification process to ensure the authenticity of user-provided information. This may involve email verification, mobile number verification, or other secure methods.



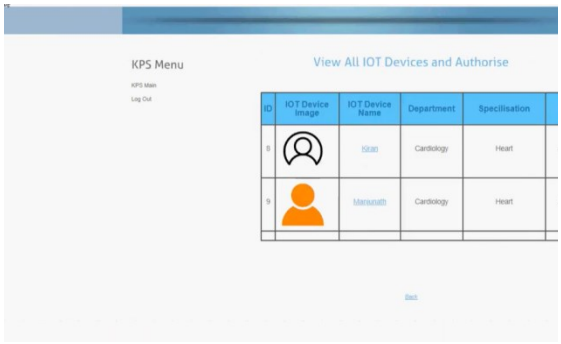
KPS Login System:

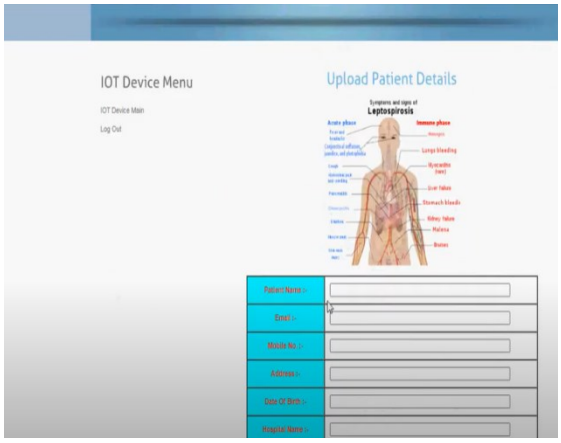
KPS login is a user authentication platform, but without additional details, specific features or purposes are not discernible.

Limited Information:

Without context, the term "KPS login" lacks clarity; for accurate details, refer to official documentation or support channels.

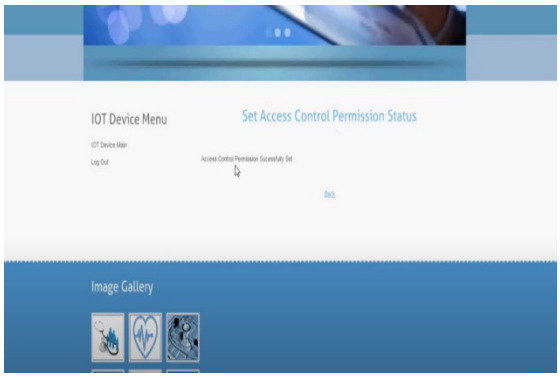
ISSN2321-2152
www.ijmece .com
Vol 6, Issue 3, 2018





User Roles and Permissions:

Implement a role-based access control system, designating roles such as patients, healthcare providers, and administrators. Define permissions based on roles to control access to different functionalities.



V.CONCLUSION

Last but not least, the "Secure and Efficient Cloud-Centric Internet of Medical Things (IoMT)-Enabled Smart Healthcare System with Public Verifiability" project is a huge step forward in solving the many problems that come with managing hospital records nowadays. This project makes a contribution to the development of smart healthcare systems by presenting a new framework that emphasises public verifiability, efficiency, security, and the smooth integration of IoMT with cloud-centric solutions. To achieve a higher degree of security during data transfer, the Escrow-Free Identity-Based Aggregate Signcryption (EF-IDASC) method must be implemented. While constantly collecting data from several implanted sensors on a patient's body, this innovative cryptography described in the project guarantees the secrecy and authenticity of medical records. In order to store and handle the collected medical data efficiently and scalable, the suggested system expertly makes use of cloud computing resources. Healthcare practitioners and patients alike will appreciate the increased accessibility and convenience brought about by the use of cellphones as safe gateways for data outsourcing.

In order to protect users' privacy, the system does not disclose any personally identifying information when transferring or storing data. By empowering stakeholders to independently confirm the accuracy and reliability of the aggregated medical data, the public verifiability method promotes openness and confidence. The project's capacity to be implemented in real-world healthcare settings is supported by its thorough performance analysis, which primarily focusses on energy consumption and efficiency. This research adds to the continuing

endeavours to improve the safety, effectiveness, and openness of smart healthcare systems that are enabled by IoMT by tackling the shortcomings of current systems and offering new alternatives.

Simply put, the "Secure and Efficient Cloud-Centric IoMT-Enabled Smart Healthcare System with Public Verifiability" project does double duty: it solves the problems with healthcare data management that are plaguing the industry right now and lays the groundwork for future generations of privacy-centric, publicly verifiable healthcare systems that will thrive in the IoMT era.

VI.REFERENCES

1. Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT", *IEEE Trans. Ind. Informat.*, vol. 15, no. 9, pp. 5099-5108, Sep. 2019.

2. M. Kumar and S. Chand, "A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network", *IEEE Syst. J.*, May 2020.

3. W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang and G. Wang, "Security and privacy in the medical Internet of Things: A review", *Security Commun. Netw.*, vol. 2018, Jan. 2018.

4. A. Zhang, J. Chen, R. Q. Hu and Y. Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-advanced networks", *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2659-2672, Apr. 2016.

5. Z. Li, Z. Yang and S. Xie, "Computing resource trading for edge-cloud-assisted Internet of Things", *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3661-3669, Jun. 2019.

6. W. Wang, P. Xu and L. T. Yang, "Secure data collection storage and access in cloud-assisted IoT", *IEEE Cloud Comput.*, vol. 5, no. 4, pp. 77-88, Jul./Aug. 2018.

7. D. He, S. Zeadally and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks", *IEEE Syst. J.*, vol. 12, no. 1, pp. 64-73, Mar. 2018.

8. V. Sureshkumar, R. Amin, V. R. Vijaykumar and S. Rajasekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation", *Future Gener. Comput. Syst.*, vol. 100, pp. 938-951, Nov. 2019.

9. H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks", *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442-1455, Jul. 2015.

10.J. Shen, S. Chang, J. Shen, Q. Liu and X. Sun, "A lightweight multi-layer

authentication protocol for wireless body area networks", *Future Gener. Comput. Syst.*, vol. 78, pp. 956-963, Jan. 2018.

11.J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. J. Peterson and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices", *Proc. 1st ACM Workshop Security Privacy Smartphones Mobile Devices*, pp. 75-86, 2011.

12.C. Hu, H. Li, Y. Huo, T. Xiang and X. Liao, "Secure and efficient data communication protocol for wireless body area networks", *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 2, no. 2, pp. 94-107, Apr.–Jun. 2016.

13.B. Chandrasekaran, R. Balakrishnan and Y. Nogami, "Secure data communication using file hierarchy attribute based encryption in wireless body area networks", *J. Commun. Softw. Syst.*, vol. 14, no. 1, pp. 75-81, 2018.

14.F. Li, M. K. Khan, K. Alghathbar and T. Takagi, "Identity-based online/offline signcryption for low power devices", *J. Netw. Comput. Appl.*, vol. 35, no. 1, pp. 340-347, 2012.

15.A. A. Omala, N. Robert and F. Li, "A provably-secure transmission scheme for wireless body area networks", *J. Med. Syst.*, vol. 40, no. 11, pp. 247, 2016.

16.A. Yin and H. Liang, "Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks", *Wireless Pers. Commun.*, vol. 80, no. 3, pp. 1049-1062, 2015.

17.A. Zhang, L. Wang, X. Ye and X. Lin, "Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems", *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 662-675, Mar. 2017.

18.C. Zhou, "Comments on 'light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems", *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1869-1870, Jul. 2018.

19.C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system", *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 1, pp. 1-16, 2019.

20.S. S. D. Selvi, S. S. Vivek, J. Shriram, S. Kalaivani and C. P. Rangan, "Identity based aggregate signcryption schemes", *Proc. Int. Conf. Cryptol. India*, pp. 378-397, 2009.

21.H. Wang, Z. Liu, Z. Liu and D. S. Wong, "Identity-based aggregate signcryption in the standard model from multilinear maps", *Frontiers Comput. Sci.*, vol. 10, no. 4, pp. 741-754, 2016.

22.J. Kar, "Provably secure identity-based aggregate signcryption scheme in random oracles", *IACR Cryptol. ePrint Arch.*, vol. 2013, pp. 580-587, Jan. 2013.

23.Z. Eslami and N. Pakniat, "Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model", *J. King Saud Univ. Inf. Sci.*, vol. 26, no. 3, pp. 276-286, 2014.

24.S. Niu, Z. Li and C. Wang, "Privacy-preserving multi-party aggregate signcryption for heterogeneous systems", *Proc. Int. Conf. Cloud Comput. Security*, pp. 216-229, 2017.

25.M. Kumar and S. Chand, "SecP2PVoD: A secure peer-to-peer video-on-demand system against pollution attack and untrusted service provider", *Multimed. Tools Appl.*, vol. 79, pp. 6163-6190, Dec. 2019.

26.G. S. Aujla, R. Chaudhary, K. Kaur, S. Garg, N. Kumar and R. Ranjan, "SAFE: SDN-assisted framework for edge–cloud interplay in secure healthcare ecosystem", *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 469-480, Jan. 2018.

27.Y. Liu, Y. Zhang, J. Ling and Z. Liu, "Secure and fine-grained access control on e-healthcare records in mobile cloud computing", *Future Gener. Comput. Syst.*, vol. 78, pp. 1020-1026, Jan. 2018.

28.Y. Yang and M. Ma, "Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds", *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 4, pp. 746-759, Apr. 2016.

29.Y. Zhang, D. Zheng and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control", *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130-2145, Jun. 2018.

30.Y. Yang, X. Zheng and C. Tang, "Lightweight distributed secure data management system for health Internet of Things", *J. Netw. Comput. Appl.*, vol. 89, pp. 26-37, Jul. 2017.