Migration Letters

Volume: 20, No: S12 (2023), pp. 1558-1568

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

An Enhanced Security Mechanism For Strengthening Electronic Health Data With Iot In Cloud

Dr. Thavamani. S[1] & Rajakumar. M [2, 3]

Abstract:
The proposed research work titled "An Enhanced Security Mechanism for Strengthening Electronic Health Data with Internet of Things (IOT) in Cloud" addresses critical security concerns within the Se-Health (Secured electronic Health) Cloud system. The focus is particularly on enhancing security during the transition from e-Health Cloud to Se-Health Cloud. The existing paper, "Migration of e-Health Cloud to Se-Health Cloud", lacks specificity regarding security algorithms, prompting the need for a more robust approach. In response to these challenges; this research introduces a novel and secure data security algorithm. To access patient data stored in the cloud, users, comprising patients, family members, doctors, and clinical staff, are required to register their details, thereby establishing a comprehensive user validation process. The paper delves into the exploration of benchmarking with real-time data, presenting detailed information on the experimental setups and simulation tools used. The outcomes of this research include heightened security measures within the Se-Health Cloud ecosystem. Additionally, the paper provides a thorough parameter analysis, focusing on key aspects such as the number of packets, bandwidth, transmission speed, packet loss, and memory usage. These efforts collectively contribute to ensuring the confidentiality and integrity of sensitive public health data, paving the way for a more secure and reliable Se-Health infrastructure.

Keywords: *Se-Health data, Security Algorithms, Health data, Internet of Things.*

1. Introduction:

In recent years, the integration of information technology into healthcare systems has led to the evolution of e-Health Cloud, pro[1]viding a platform for the storage and analysis of vast amounts of health-related data. As the reliance on cloud-based solutions grows, so does the imperative to address and enhance the security measures within these systems. This research embarks on a journey to fortify the security of the e-Health Cloud ecosystem, focusing on the specific context of migrating from e-Health Cloud to Se-Health Cloud.

The initial groundwork, as presented in the paper "Migration of e-Health Cloud to Se-Health Cloud", laid the foundation for the transition process but identified a critical gap concerning the lack of explicit security algorithms. Recognizing the paramount importance of safeguarding sensitive health data, this study aims to fill this void by proposing a comprehensive and innovative security-enhanced approach.

The research introduces a novel data security algorithm, recognizing the need for heightened protection measures during the migration process. By registering users,

[1] Associate Professor in Computer Science & Applications, [2] Research Scholar of Ph.D.in Computer Science,[3]Sri Ramakrishna College of Arts & Science (Autonomous) (Formerly S.N.R. Sons College (Autonomous), Affiliated to Bharathiar University, Coimbatore, T.N-641 006, India.
[3]Head, Department Computer Applications, Srinivasan College of Arts and Science, Perambalur, Affiliated to Bharathidasan University, Trichy, T.N-621 212, India.

encompassing patients, family members, doctors, and clinical staff, an error free user validation process is established, adding an extra layer of security to the Se-Health Cloud.

Beyond authentication mechanisms, this paper explores the integration of benchmarking with real-time data, offering insights into the experimental setups and simulation tools used. The outcomes of this research extend beyond the establishment of improved security measures. The study also delves into a comprehensive parameter analysis, addressing critical metrics such as the number of packets, bandwidth, transmission speed, packet loss, and memory usage [28,29]. This multifaceted approach ensures not only the confidentiality and integrity of public health data but also contributes to the overall efficiency and reliability of the Se-Health Cloud ecosystem.
As the healthcare landscape continues to evolve, the findings of this research aim to provide a secure and resilient foundation for the utilization of cloud-based technologies in the pursuit of enhanced healthcare solutions. By addressing existing security gaps and introducing innovative measures, this work contributes to the ongoing discourse on safeguarding the privacy and integrity of sensitive health information in the digital era.

2. Literature Survey:

The landscape of e-Health Cloud and its security concerns has been a subject of considerable research and scholarly exploration. The following literature survey provides an overview of key studies, advancements, and challenges related to security in cloud-based healthcare systems, setting the stage for the current research endeavor. IoT-based healthcare systems have gained popularity due to their ability to provide continuous health monitoring [1]. This real-time monitoring allows healthcare providers to detect and respond quickly to changes in a patient's condition, potentially preventing serious health issues. IoT-based healthcare systems also enable cost-effective interactions between healthcare institutions [2]. In addition, the use of IoT-based healthcare systems has been found to improve the efficiency of healthcare delivery, reduce healthcare costs, and improve patient satisfaction [3]. Cloud computing has become increasingly popular in healthcare systems due to its ability to store and process large amounts of data securely [4]. It has been found to support digital transformation, streamline electronic record keeping, enable a patient-centric approach, and improve healthcare outcomes [5]. However, security remains a major concern when it comes to cloud computing in healthcare [6]. Ensuring that patient data is secure and HIPAA compliant is essential to the success of any healthcare system. Security is a top priority in healthcare systems, as they frequently handle sensitive data.

The rising ransomware threat, cloud vulnerabilities and misconfigurations, web application attacks, insider threats, and supply chain attacks are some of the biggest security threats in healthcare [8]. Therefore, ensuring that healthcare systems are secure and protected from cyber attacks is essential. A breach of patient data can have serious consequences, both for the patient and the healthcare provider [7]. Novel IoT-based healthcare systems are being developed to address the challenges of traditional healthcare systems. These systems provide integrated services to assist healthcare officials, minimize costs, maintain security, and upgrade disease management [9]. The development of a novel architecture that incorporates IoT in e-health systems is a current focus of research [10]. The efficiency of the developed system lies in its ability to manage big data in an IoT-based healthcare-monitoring system [11].

A secured cloud-supported IoT-based healthcare system can address the security and privacy concerns in healthcare systems. A comprehensive framework has been developed to address key issues in the layered architecture of an IoT-based health system [12]. The framework focuses on ensuring that data is secure, privacy is maintained, and the system is HIPAA compliant. The framework also ensures that the system is scalable, efficient, and cost-effective [13]. The work [14] highlights the inherent security challenges in cloud computing, particularly in the context of e-Health systems. The study underscores the need for robust security measures to safeguard sensitive health data, laying the groundwork for

subsequent research to address these concerns. Survey [15,30,31] examines security and privacy issues specific to healthcare cloud computing. It provides insights into the vulnerabilities associated with the storage and processing of health data in the cloud, guiding subsequent studies to explore innovative solutions for enhancing security.Various Case studies have demonstrated the potential of secured cloud-supported IoT-based healthcare systems in improving patient outcomes and reducing costs. For instance, a real-time health monitoring system was created as an IoT-based solution that is HIPAA and GDPR compliant [16,17]. The study explores encryption techniques and their application in cloud computing, providing insights into securing data during transmission and storage. The findings contribute to the broader understanding of security measures applicable to e-Health Cloud [18]. With a focus on user authentication, this study explores the application of many technologies in cloud-based healthcare systems.

IoT-based healthcare systems have gained traction due to their ability to provide real-time remote patient monitoring and improve healthcare outcomes [19]. Recent studies have explored the security requirements associated with IoT in healthcare systems to ensure data privacy and security [20]. A systematic review of IoT-based healthcare-monitoring systems has also been conducted to understand their features and concepts [21]. The research [22] introduces a framework for benchmarking security measures in cloud computing environments. The study emphasizes the importance of establishing benchmarks for assessing the effectiveness of security enhancements. This framework serves as a valuable reference for the current work's exploration of benchmarking with real-time data. Addressing the migration aspect, [23] this recent study focuses on secure migration strategies for e-Health systems to the cloud. The research delves into potential security risks during migration and proposes solutions to mitigate these risks, aligning with the objectives of the current research endeavor. The system uses gateways and cloud-based analysis to manage the storage of data [24,27]. However, ensuring the security and privacy of patient data remains a key challenge to the successful implementation of IoT-based healthcare systems. To address these challenges, data management methods for IoT-based healthcare systems with cloud facilities have been systematically analyzed [25,26].

By building upon the insights gained from these key studies, the current research aims to contribute to the evolving discourse on security in e-Health Cloud, offering a nuanced and innovative approach to fortify the transition from e-Health Cloud to Se-Health Cloud [27]. The integration of additional authentication mechanisms and the exploration of benchmarking parameters represent pivotal aspects of this contribution, aiming to enhance the overall security posture of cloud-based healthcare systems.

3. Proposed Methodology:

The implementation of a secured cloud-supported IoT-based healthcare system involves integrating sensor-enabled smart devices that accurately collect data for analysis and actions. However, there are challenges to implementing IoT-based healthcare systems, including the integration of medical devices and systems. To overcome these challenges, research has focused on designing and implementing IoT-based healthcare-monitoring systems that improve healthcare delivery, reduce costs, and improve patient satisfaction.

The components of an IoT-based healthcare system typically include sensors, which collect patient data for status monitoring, and an Arduino board to store medical data for multiple patients. Additionally, cloud-based IoT devices require external or implantable sensors to collect patient data for monitoring or to make automated decisions. The data processing process is typically divided into three stages: collection and aggregation, the classification and analysis of collected data, and the decision-making process. A multi-layered architectural pattern is often used to support different aspects of IoT system deployments, such as scalability, modularity, flexibility, and configuration.

3.1. Proposed Architecture:

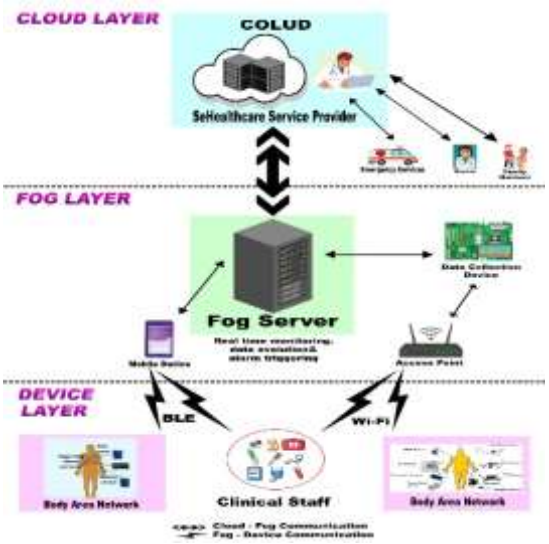

Fig. Architecture design for a secured cloud-supported IoT-based healthcare system.

This system will be comprised of **three main layers**:

- Device (Edge) Layer: This layer consists of various medical devices and sensors that collect patient data, such as heart rate, blood pressure, and blood glucose levels. These devices can be wearable, implantable, or attached to medical equipment.
- Fog Layer: This layer is responsible for pre-processing and filtering the data collected by the devices. It also performs edge computing tasks such as anomaly detection and real-time alerts.
- Cloud Layer: This layer stores and analyzes the processed data from the fog layer. This layer will handle the data processing & decision making process. It also provides various services such as data visualization, reporting, and machine learning-based insights for healthcare providers.

Security Considerations:

- Data encryption: All data transmitted between devices, the fog layer, and the cloud layer will be encrypted to prevent unauthorized access.
- Access control: Granular access control mechanisms will be implemented to ensure that only authorized users can access patient data.
- Regular security audits: The system will be subjected to regular security audits to identify and address vulnerabilities.
- Compliance with regulations: The system will comply with all relevant healthcare data privacy regulations, such as HIPAA.

Additional Components:

- API Gateway: This component will act as a single point of entry for all applications and devices that interact with the system.
- Data Lake: This is a central repository for storing all raw and processed data collected from the devices.
- Analytics Engine: This engine will be used to analyze the data in the data lake and generate insights for healthcare providers.
- Machine Learning Models: These models can be used for tasks such as predicting patient outcomes, detecting early signs of disease, and recommending personalized treatment plans.

Benefits of this Architecture:

- Scalability: The architecture can be easily scaled to accommodate an increasing number of devices and users.

- Flexibility: The architecture can be adapted to support different types of medical devices and sensors.
- Security: The architecture incorporates multiple security measures to protect patient data.
- Cost-effectiveness: The cloud-based approach can help to reduce the cost of deploying and maintaining the system.

Overall, this architecture provides a secure and scalable foundation for building a cloud-supported IoT-based healthcare system that can improve patient outcomes, reduce costs, and increase efficiency.

3.2. Proposed Algorithm in Pseudo-code form:

This pseudo-code provides a conceptual representation of the algorithm, detailing the steps for data collection, processing at different layers, and security considerations in an IoT based healthcare system.

```
# Define MedicalDevice class for data collection at the Device Layer
class MedicalDevice:
method collectData():
# Simulate data collection (e.g., heart rate, blood pressure)
patientData = collectPatientData()
      return patientData

# Define FogLayer class for data preprocessing and edge computing at the Fog Layer
class FogLayer:
method preprocessData(patientData):
# Simulate data preprocessing
processedData = preprocess(patientData)
return processedData

method edgeComputing(processedData):
# Simulate edge computing tasks (e.g., anomaly detection, real-time alerts)
performEdgeComputing(processedData)

# Define CloudLayer class for data processing and services at the Cloud Layer
class CloudLayer:
method storeData(encryptedData):
# Simulate storing encrypted data in the cloud
storeEncryptedData(encryptedData)

method analyzeData(encryptedData):
# Simulate data analysis
analyzedData = analyzeEncrypted Data(encryptedData)
return analyzedData

method provideServices(analyzedData):
# Simulate providing various services (e.g., data visualization, reporting, insights)
provideDataServices(analyzedData)
```

```
# Define SecurityManager class for security-related
tasks
class SecurityManager:

method encryptData(processedData):
# Simulate data encryption
encryptedData = encrypt(processedData)
return encryptedData

method decrypt Data(processedData)
# Simulate data decryption
decryptedData = decrypt(processedData)
return decryptedData

method accessControl(authorizedUser):
# Simulate access control for authorized users
performAccessControl(authorizedUser)

method performSecurityAudit():
# Simulate a security audit
performAudit()

method ensureRegulatoryCompliance():
# Simulate compliance checks (e.g., HIPAA)
ensureCompliance()

# Main Algorithm
method mainAlgorithm():
# Step 1: Data Collection (Device Layer)
      device = new MedicalDevice()
      patientData = device.collectData()

# Step 2: Fog Layer Processing
  fog = new FogLayer()
  processedData = fog.preprocessData
  (patientData)
  fog.edgeComputing(processedData)

# Step 3: Cloud Layer Processing
  cloud = new CloudLayer()
  securityManager = new SecurityManager()
  encryptedData = securityManager. Encrypt
Data(processedData)
decryptedData = securityManager.decrypt
Data(processedData)
authorizedUser = "AuthorizedUser123"

securityManager.accessControl(authorizedUser)
cloud.storeData(encryptedData)
analyzedData = cloud.analyze Data(encryptedData)
cloud.provideServices(analyzedData)

# Step 4: Security Considerations
securityManager.performSecurityAudit()
securityManager.ensureRegulatoryCompliance()

# Execute the main algorithm
```

```
mainAlgorithm()
```

4. Results and Discussions:

To evaluate the effectiveness of a secured cloud-supported IoT-based healthcare system, researchers have explored the latest trends in healthcare monitoring systems by implementing the role of IoT. An intelligent IoT-based embedded healthcare system has also been conducted to understand the potential benefits of such systems. However, despite the potential benefits, security and privacy concerns remain a significant challenge to the success of IoT-based healthcare systems. This paper focus simulation of a secured IoT-based healthcare system, showcasing the seamless flow of patient data from the device layer to the cloud layer while prioritizing security and regulatory compliance. The integration of encryption, access control, security audits, and regulatory checks ensures the confidentiality and integrity of sensitive health information in the digital era.

The provided output represents the simulated execution of the main algorithm in the IoT-based healthcare system. Each step in the process is detailed below:
1. Edge Computing: Anomaly detection for a heart rate of 80 is performed at the edge computing layer.
2. Access Control: User 'Authorized User123' is granted access through access control.
3. Cloud Storage: Encrypted data, {'encrypted_heart_rate': 160}, is stored in the cloud.
4. Cloud Services: Data analysis is performed on the encrypted data, resulting in a normal analysis result.
5. Security Audit: A security audit is performed.
6. Regulatory Compliance Checks: Checks for regulatory compliance are completed.

There are many of the following parameters are evaluated, such are: No. of Sensors used, data Load, Pocket Loss, Memory usage in Cloud and Accuracy of the data / results in the System. In this system we have applied some security mechanisms to improve the data' security. In this research paper, secured data will be used for this work.

Below figure represents, the comparative evaluation of no. of sensors and with load (secured data). Data which is in encrypted form which lead total size of the data is reduced. Hence more amount of data can be transmitted when sensors are increased.

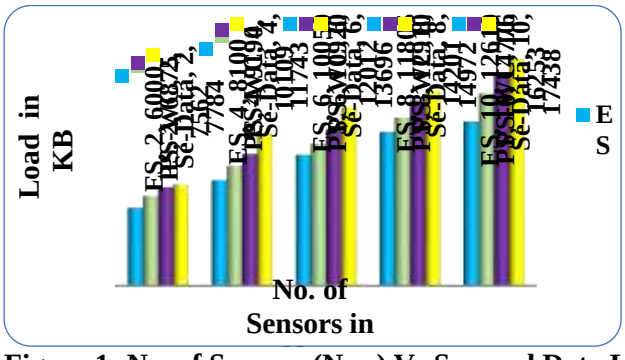

Figure 1: No. of Sensors (Nos.) Vs Secured Data Load (KB).

Below figure represents, the comparative evaluation of secured data load with packet loss. Load of the system is in encrypted form, which will reduce the data and packet loss also reduced. If load is increased, packet loss also increased, but compared with proposed system with compression technique, this system will have less number in packet loss.

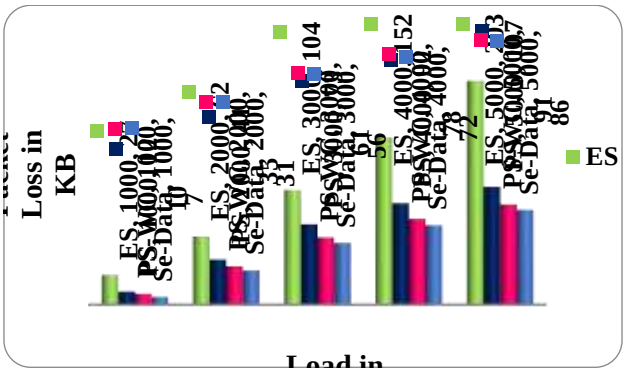

Figure 2: Load (KB) Vs Packet Loss (KB)

Figure 3 represents the comparative evaluation of secured data load with memory usage in Cloud. In this work, load is encrypted form then, total size of the original data will be little bit reduced. Hence, memory usage in percentage of the Cloud for storing the patient data is also less.

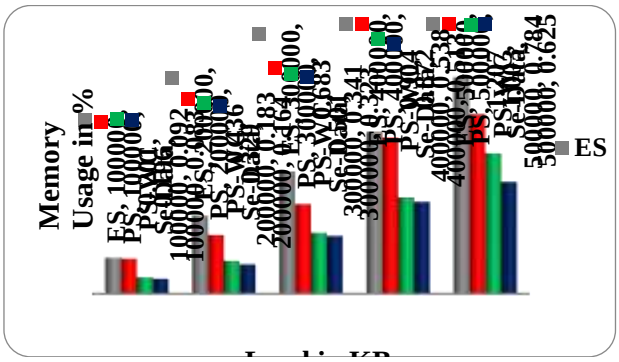

Figure 3: Load (KB) Vs Memory Usage (%)

Figure 4 represents the comparative evaluation of packet loss with accuracy of the data which are to be transferred / stored in this system. If packet loss is reduced from original data, it's accuracy of the original information will be in more / increased and in more packet loss, data accuracy will be in less / decreased.

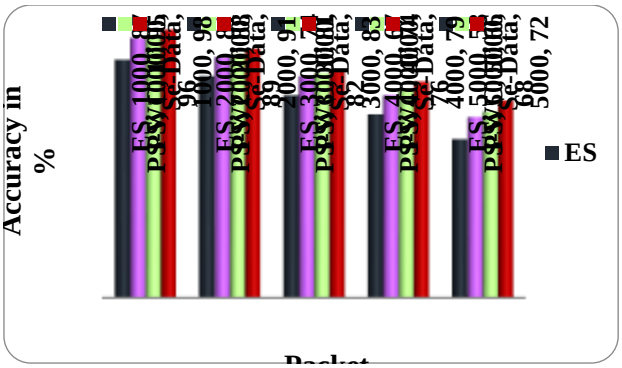

Figure 4: Packet Loss (KB) Vs Accuracy (%)

These output demonstrates the successful execution of the IoT-based healthcare system's main algorithm, including data processing, security measures, and regulatory compliance checks. The system operates cohesively, ensuring the integrity and security of patient data throughout the entire process.

This research has also focused on developing systems that can overcome security challenges, such as confidential medical reports and records stored in the cloud. Furthermore, the emergence of IoT devices has led to the development of various applications that can improve the efficiency and effectiveness of healthcare delivery.

5. Conclusion & Future work:

In conclusion, IoT-based healthcare systems have the potential to improve patient outcomes, reduce costs, and increase efficiency. Cloud computing has become increasingly popular in healthcare systems due to its ability to store and process large amounts of data securely. However, security and privacy concerns remain a significant challenge to the success of IoT-based healthcare systems. A comprehensive framework for a secured cloud-supported IoT-based healthcare system has been proposed to address these challenges. It ensures data privacy and security, scalability, efficiency, and cost-effectiveness of the system. Further research and development in this field can lead to improved healthcare outcomes and a better quality of life for patients. As a future work, integration of different medical devices and systems can be a challenging task. Further, interoperability can be achieved later by ensuring all components of the system can communicate with each other seamlessly is important.

6. References:

1. Khan. M.M, Alanazi. T.M, Albraikan. A.A and Almalki. F.A, IoT-based health monitoring system development and analysis. Security and Communication Networks, 2022.
2. Rejeb. A, Rejeb. K, Treiblmaier. H, Appolloni. A, Alghamdi. S, Alhasawi. Y and Iranmanesh. M, The Internet of Things (IoT) in Healthcare: Taking stock and moving forward. Internet of Things, p.100721, 2023.
3. Bovenizer. W, Chetthamrongchai. P, A comprehensive systematic and bibliometric review of the IoT-based healthcare systems. Cluster Computing, pp.1-27, 2023.
4. Mehrtak. M, SeyedAlinaghi. S, MohsseniPour. M, Noori. T, Karimi. A, Shamsabadi. A, Heydari. M, Barzegary. A, Mirzapour. P, Soleymanzadeh. M and Vahedi. F, Security challenges and solutions using healthcare cloud computing. Journal of medicine and life, 14(4), p.448, 2021.
5. Hossain. S. and Luby. D, Cloud computing in healthcare industry. In Proceedings of the Annual International Conference on Cloud Computing and Virtualization (CCV'10) (pp. 42-50), 2010.
6. Casola. V, Castiglione. A, Choo. K.K.R and Esposito. C, Healthcare-related data in the cloud: Challenges and opportunities. IEEE cloud computing, 3(6), pp.10-14, 2016.
7. Almalawi. A, Khan. A.I, Alsolami. F, Abushark. Y.B. and Alfakeeh. A.S, Managing Security of Healthcare Data for a Modern Healthcare System. Sensors, 23(7), p.3612, 2023.
8. Bakhtiyari-Shahri. A and Ismail. Z, Users as the biggest threats to security of Health Information Systems. International Journal of Communications and Information Technology, 1(2), pp.29-33, 2011.
9. Abdulmalek. S, Nasir. A, Jabbar. W.A, Almuhaya. M.A, Bairagi. A.K, Khan. M.A.M and Kee. S.H, IoT-based Healthcare-Monitoring System towards improving quality of life: A review in Healthcare, (Vol. 10, No. 10, p. 1993), 2022.
10. Safdar. Z, Farid. S, Qadir. M, Asghar. K, Iqbal. J and Hamdani. F.K, A Novel Architecture for Internet Of Things based E-Health Systems. Journal of Medical Imaging and Health Informatics, 10(10), pp.2378-2388, 2020.
11. Palli. G.H, Mirza. G.F and Chowdhry. B.S, Novel IoT-Based E-Health System: Hospital Management, Telemedicine and Quarantine Management for COVID-19. Third International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT) (pp. 1-9), IEEE, 2022.
12. Chattopadhyay. A.K, Nag. A, Ghosh. D and Chanda. K, A Secure Framework for IoT-based Healthcare System. In Proceedings of International Ethical Hacking Conference 2018: eHaCON 2018, Kolkata, India (pp. 383-393). Springer Singapore, 2019.
13. Hussain. A, Ali. T, Althobiani. F, Draz. U, Irfan. M, Yasin. S, Shafiq. S, Safdar. Z, Glowacz. A, Nowakowski. G and Khan. M.S, Security Framework for IoT based Real-Time Health Applications. Electronics, 10(6), p.719, 2021.
14. Butpheng. C, Yeh. K.H and Xiong. H, Security and Privacy in IoT-Cloud-based e-Health Systems - A Comprehensive Review. Symmetry, 12(7), p.1191, 2020.
15. Sai. G.H, Tripathi. K and Tyagi. A.K, Internet of Things-Based e-Health Care: Key Challenges and Recommended Solutions for Future. In Proceedings of Third International Conference on Computing, Communications, and Cyber-Security: IC4S 2021, Singapore: Springer Nature Singapore, (pp. 461-474), 2022.

16. Perumal. B, Nagarai. P, Venkatesh. R, Muneeswaran. V, GopiShankar. Y, SaiKumar. A, Koushik. A and Anil. B, Real Time Transformer Health Monitoring System Using IoT in R. In 2022 International Conference on Computer Communication and Informatics (ICCCI) IEEE, (pp. 1-5), 2022.
17. Khanna. A. and Kaur. S, Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. Wireless Personal Communications, 114, pp.1687-1762, 2020.
18. Kumar. M, Kumar. A, Verma. S, Bhattacharya. P, Ghimire. D, Kim. S.H and Hosen. A.S, Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges and Security Issues. Electronics, 12(9), p.2050, 2023.
19. Nasiri. S, Sadoughi. F, Tadayon. M.H and Dehnad. A, Security requirements of Internet of Things-based Healthcare System: A Survey Study. ActaInformaticaMedica, 27(4), p.253, 2019.
20. Kozak. S. and Elliot. S, Connecting the Dots. Toronto: Learning for a Sustainable Future. Search in, 2014.
21. Aivaliotis. V, Tsantikidou. K and Sklavos. N, IoT-based Multi-Sensor Healthcare Architectures and a Lightweight-Based Privacy Scheme. Sensors, 22(11), p.4269, 2022.
22. Nasiri. S, Sadoughi. F, Dehnad. A, Tadayon. M.H and Ahmadi. H, Layered Architecture for Internet of Things-based Healthcare System: A Systematic Literature Review. Informatica, 45(4), 2021.
23. Awotunde. J.B, Jimoh. R.G, Folorunso. S.O, Adeniyi. E.A, Abiodun. K.M and Banjo. O.O, Privacy and security concerns in IoT-based Healthcare Systems. In The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care Cham: Springer International Publishing, (pp. 105-134), 2021.
24. Khan. M.A, Challenges Facing the Application of IoT in Medicine and Healthcare. International Journal of Computations, Information and Manufacturing (IJCIM), 1(1), 2021.
25. Selvaraj. S and Sundaravaradhan. S, Challenges and Opportunities in IoT Healthcare Systems: A Systematic Review. SN Applied Sciences, 2(1), p.139, 2020.
26. Hussein. W.N, Hussain. H.N and Humod. I.M, A Proposed Framework for Healthcare based on Cloud Computing and IoT Applications. Materials Today: Proceedings, 60, pp.1835-1839, 2022.
27. Rajakumar.M, Dr.Thavamani.S, "Migration of e-Health Cloud to Se-Health Cloud", presented in International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), October-2021 & the same paper was published in IEEE Xplore,, ISBN: 10.1109/ICAECA52838.2021.9675613, Indexed in Scopus since March 2022.
28. AS Vijendran amd S Thavamani "An Efficient Algorithm for Clustering Nodes, Classifying and Replication of Content on Demand Basis for Content Distribution in P2P Overlay Networks", International Journal of Computer & Communication Technology (IJCCT) - @ Inter Science Open Access Journals, ISSN (ONLINE) : 2231-0371(PRINT): 0975-7449, Volume 4, Issue1, April-2013, PP.96-100.
29. AS Vijendran amd S Thavamani Published the research article entitled "Least Recently Used Replica Replacement Technique in Distributed Computing network", International Conference on Intelligent Computing Applications- ICICA2014, in proceedings of ICICA14 published by IEEE Xplore, Available in IEEE Xplore Digital Library, March-2014, Pages 104-108. Print ISBN: 978-1-4799-3966-4/14. https://ieeexplore.ieee.org/document/6965021 DOI : 10.1109/ICICA.2014.31
30. V.S.Ramya & S.Thavamani has published the research article entitled "A Study on Security Mechanism Employed on The Electronic Health Records in The Cloud" in the International Journal of Contemporary Research in Computer Science & Technology (IJCRCST)–ISSN 2395-5325, Volume.No.3, Special Issue.3, Pages:208-214.Sep-2017. www.ijcrcst.com.
31. V.S.Ramya & S.Thavamani has published the research article entitled "A Key Aggregation Based Signature Generation Towards Data Access and Revocation To Electronic Health Records in The Cloud Servers" in the International Journal of Advanced Research in Science and Engineering (IJARSE)–ISSN 2319-8354, Volume. No. 06, Issue. No.12, Pages 268-276 Dec-2017. (UGC Approved Journal) www.ijarse.com.

Authors Profile:

Dr. S. Thavamani M.Sc., M.Phil., Ph.D. is working as an **Associate Professor**, Department of Computer Applications, Sri Ramakrishna College of Arts & Science (A), Coimbatore-6, T.N, India. She has a teaching experience of 23-years in the field of Computer science. She has received various awards like "Best Faculty Award" from ARUNAI International Research Foundation (AIRF Awards–2017), "Incessant Service Award" for recognizes "Being A Truly Inspirational Teacher", and "Best Team Award-MOOC–"Spoken Tutorial", from Sri Ramakrishna College of Arts and Science (A), "The Best Paper Award", from Tiruppur Kumaran College for Women, Tiruppur, Appreciation Award for the "Using ICT based Teaching and Learning methodology" for students of Tamil Nadu from Spoken Tutorial IIT Bombay. She has published 6-Books and 4-Book Chapters and 2 Design Patents. Her area of Specialization is Distributed Computing and Network Security. She has presented more than 35-Papers in various International and National Conferences and published 35-Research Articles in various International Journals, many of them indexed by Scopus & UGC-Care Journals. She is currently a supervisor for M.Phil. & Ph.D Research Scholars of various Universities. She acted as a Co-Ordinator of various FDPs, Workshops and Seminars.

M. Rajakumar, MCA., M.Phil., M.Teh., Research Scholar of **Ph.D.** in Computer Science at Sri Ramakrishna College of Arts and Science (A), Coimbatore, T.N, India. He has published 10-research papers in International Journals, many of them indexed by Scopus & UGC-Care Journals and presented 4-papers in National & International Conferences and had 1-Design Pattern. He has 18+ years of teaching experience in various Institutions (Arts and Engineering) in India and Abroad. He had acted as a Resource Person for various Universities in India. And he acted as an Editorial Board Member for 3- International peer reviewed Journals in India. At present serving as a Head in Department of Computer Applications, Srinivasan College of Arts and Science, Perambalur, T.N. India. And he is also a Life Member of ISTE professional body. His specialization areas are: Cloud Computing, Distributed Computing, Computer Networks, Distributed Operating Systems.