ISSN : 2347 - 2243

Indo - American Journal of Life Sciences and Biotechnology

www.iajlb.com
Email : editor@iajlb.com or iajlb.editor@gamil.com

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

Enhancing Healthcare Cloud Security with a Comprehensive Analysis for Authentication

[1]**Poovendran Alagarsundaram**
IBM,North Carolina, USA
poovasg@gmail.com

[2]**G. Arulkumaran**
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology
Associate Professor
chennai,india
arulkumarang.reva@gmail.com

Abstract

This research presents a robust cloud-based healthcare security framework that integrates Multi-Factor Authentication (MFA) and Secure Multi-Party Computation (SMPC) to safeguard sensitive patient data. The framework ensures data privacy, secure access control, and encryption for electronic health records (EHRs) stored in the cloud. The proposed system is evaluated based on authentication time, encryption/decryption performance, and computational overhead. Experimental results indicate that encryption time ranges from 0.5ms to 5.8ms as data size increases from 10 KB to 1 MB, with decryption following a similar pattern. Additionally, computational overhead increases by approximately 18% with each additional authentication factor, reinforcing security without significantly compromising efficiency. The integration of MFA ensures that unauthorized access is effectively minimized, while SMPC enhances privacy by enabling secure data computations without exposing sensitive information. This approach demonstrates a significant improvement in balancing security and system performance, making it a viable solution for real-time healthcare applications. Future enhancements may focus on optimizing encryption techniques and reducing computational complexity to further improve efficiency. This research contributes to the ongoing development of secure and scalable cloud-based healthcare solutions, offering a practical approach to addressing security challenges in modern healthcare data management.

Keywords: *Healthcare Cloud Security, Authentication using MFA, SMPC, Access Control.*

1. Introduction

The security of healthcare systems, particularly in e-healthcare, is becoming increasingly critical as more personal health data is transferred across digital platforms. A range of cryptographic methods and authentication schemes have been developed to ensure data integrity and user privacy. In this context, the focus is on the cryptanalysis and enhancement of a remote user mutual authentication and session key agreement scheme for e-healthcare systems. This study provides insight into the vulnerabilities of existing systems and proposes a more secure approach to safeguard sensitive health information during transmission in e-healthcare environments [1]. Similarly, emphasis is placed on the development of a comprehensive information security framework for mobile health (mHealth) systems. A detailed analysis of the various security requirements needed to protect mobile health data is conducted, proposing solutions that can address both privacy and security concerns inherent in mHealth systems [2].

In cloud computing environments, healthcare data faces numerous threats, including unauthorized access and potential data breaches. A standard mutual authentication protocol designed specifically for cloud computing-based healthcare systems is presented. The proposed protocol aims to ensure secure access to medical data stored in the cloud while preventing unauthorized interactions with the system. This mutual authentication process strengthens the overall security of cloud-based healthcare applications by employing advanced cryptographic techniques [3]. Further, a comprehensive meta-analysis of cryptographic security mechanisms employed in cloud computing is provided. The paper highlights the role of encryption and other cryptographic techniques in protecting sensitive data stored in the cloud, with an emphasis on the cloud's potential in e-healthcare and the challenges it faces in terms of secure data management [4].

As the healthcare industry increasingly moves towards cloud and wireless body area networks (WBANs), privacy concerns have escalated. Privacy authentication schemes based on cloud computing for medical

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

environments are improved, with enhancements to existing systems, emphasizing the need for more robust privacy-preserving measures in healthcare data handling, especially within cloud-based platforms [5]. Additionally, an exploration of the security landscape in wireless body area networks is conducted, with a comprehensive analysis of the authentication methods used to protect the health data collected by these networks. The findings contribute significantly to improving the security of personal health data collected through wearable medical devices [6].

Finally, in the area of telecare medicine information systems, cryptanalysis and improvement of authentication and key agreement protocols are performed. This work targets enhancing the security of telecare systems by identifying vulnerabilities in the existing protocols and suggesting more resilient methods for authentication and session management. This ensures that sensitive health data remains secure during remote medical consultations [7]. A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments is presented. The approach focuses on the integration of big data analytics with cloud-based healthcare platforms to enhance security while providing robust data protection mechanisms in the processing and storage of health information [8].

1.1 Objectives

- Developed a cloud-based healthcare security model integrating Multi-Factor Authentication (MFA) and Secure Multi-Party Computation (SMPC) to protect sensitive patient data.
- Implemented an authentication process that balances security and usability, ensuring secure access control with minimal computational overhead.
- Conducted extensive performance analysis, demonstrating that encryption time scales efficiently from increasing data sizes, while computational overhead increases authentication factor.
- Designed a security architecture that can handle growing data volumes, making it suitable for real-time healthcare applications.
- Suggested future enhancements, such as integrating homomorphic encryption and blockchain, to further improve security and privacy in cloud-based healthcare systems.

2. Literature Survey

Cloud computing in healthcare systems presents numerous security challenges, especially with the increasing adoption of cloud technologies for storing and processing sensitive medical data. A systematic analysis of the security challenges in healthcare cloud computing highlights various issues such as data confidentiality, privacy, and integrity, and proposes solutions for enhancing the security of cloud-based healthcare systems. The study emphasizes the need for a robust security framework to protect patient data in cloud environments while maintaining compliance with health data regulations[9]. Similarly, the integration of smart environments with cloud-based user authentication for telecare medical information systems has been explored, proposing a three-factor authentication model that aims to ensure secure user access in telemedicine systems, addressing vulnerabilities in traditional healthcare systems[10].

The concept of integrating the Internet of Things (IoT) with cloud computing for healthcare systems has gained significant attention due to its potential for improving healthcare delivery. A new secure healthcare system that leverages the cloud of things (CoT) is proposed to provide scalable and secure healthcare services. This work emphasizes the importance of ensuring the security of medical devices and sensors that communicate with the cloud, highlighting key security requirements such as authentication, access control, and data encryption for the healthcare ecosystem[11]. In a similar vein, the authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring is examined, with a protocol designed to ensure that data collected by wearable sensors remains secure when transmitted to cloud platforms for processing and analysis, focusing on minimizing data loss during transmission[12].

The importance of authentication and access control in e-health systems hosted in the cloud is also addressed. Secure authentication mechanisms are crucial to ensure that only authorized users can access sensitive healthcare data. The study highlights the need for access control models that provide fine-grained control over who can access patient data, preventing unauthorized access in a cloud-based healthcare environment [13]. Additionally, a survey on authentication methods in mobile cloud computing, particularly in healthcare contexts, reviews various authentication schemes used to protect sensitive medical data in mobile cloud applications. This highlights the need for secure user verification and data protection in mobile healthcare environments [14].

2.1 Problem Statement

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

The increasing adoption of cloud-based healthcare systems has raised significant concerns regarding the security and privacy of patient data. One study highlights vulnerabilities in wireless body area networks (WBANs), emphasizing risks such as data breaches, identity theft, and unauthorized access, necessitating robust cryptographic techniques and authentication protocols [15]. Another study discusses weaknesses in biometric-based authentication schemes for telecare medicine information systems, which are prone to replay attacks and impersonation threats, and suggests incorporating nonce-based authentication to enhance security [16]. Research analyzing security and privacy challenges in cloud-based electronic health record (EHR) systems identifies issues related to data integrity, compliance with healthcare regulations, and exposure to cyberattacks [17]. A proposed three-factor authentication protocol integrates passwords, biometrics, and smart card verification to enhance security in e-health clouds [18]. Another authentication scheme introduces an RFID-enabled system to ensure secure data transmission in vehicular mobile cloud healthcare applications [19]. These studies collectively emphasize the need for advanced security frameworks to mitigate cyber threats and protect patient confidentiality in evolving cloud-based healthcare environments [20].

3. Proposed Methodology

A secure healthcare cloud framework incorporating Multi-Factor Authentication (MFA) and Secure Multi-Party Computation (SMPC) encryption to ensure data security and privacy. The process begins with a healthcare dataset, which undergoes MFA-based authentication to verify user identity before accessing the data. Once authenticated, users can retrieve and interact with the data securely. Additionally, sensitive data is encrypted using SMPC, ensuring privacy before storage in the cloud. This model enhances data security, access control**,** and confidentiality while minimizing unauthorized access and breaches in cloud-based healthcare systems figure 1 shows secure healthcare cloud framework with MFA and SMPC Encryption.

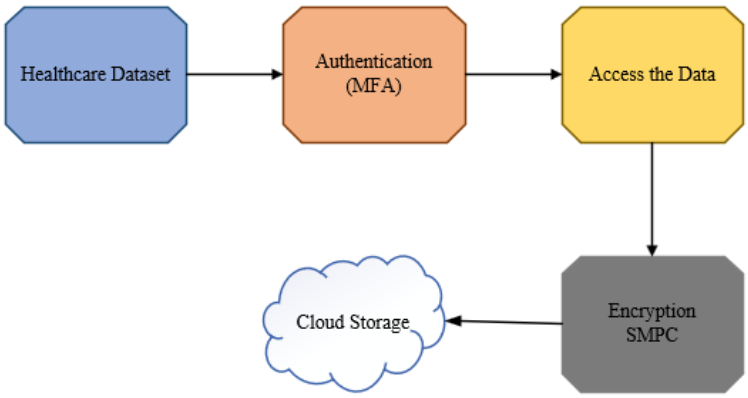

Figure 1: Secure Healthcare Cloud Framework with MFA and SMPC Encryption

3.1 Data Collection

A healthcare dataset contains sensitive medical information, including patient records, diagnostic reports, treatment history, and personal details. This dataset must be protected to ensure confidentiality, integrity, and availability, especially when stored in cloud-based systems. Unauthorized access to healthcare data can lead to privacy breaches, identity theft, and regulatory non-compliance. To enhance security, access to the dataset is restricted to authenticated users, and encryption techniques are applied before storing the data in the cloud.

3.2 Authentication Using MFA

Multi-Factor Authentication (MFA) enhances healthcare data security by requiring users to verify their identity using multiple authentication factors, such as passwords, OTPs, or biometrics. This approach reduces the risk of unauthorized access by ensuring that a user must pass multiple security checks. Let UUU be the user, and C_1, C_2, C_3 be authentication credentials. Authentication is granted only if all credentials are valid:

$$A(U) = \begin{cases} 1, & \text{if } (C_1 \text{ is valid }) \wedge (C_2 \text{ is valid }) \wedge (C_3 \text{ is valid }) \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

Where $A(U)$ represents the authentication function that determines whether the user U is granted access, $C_1\ C_2\ C_3$ Different authentication credentials such as password (C_1), OTP (C_2), and biometric data (C_3), 1 Authentication is effective (user is granted access) if all authentication credentials are valid, Authentication is effective (user is granted access) if all authentication credentials are valid and 0 Authentication fails (access is denied) if any one of the credentials is invalid.

3.3 Access the Data

After effective Multi-Factor Authentication (MFA), users gain access to healthcare data based on their roles and permissions. This ensures that only authorized doctors, nurses, or administrators can retrieve, update, or analyze patient records. Unauthorized users are denied access, protecting patient confidentiality and data integrity.

$$D = \begin{cases} H', & \text{if } A(U) = 1 \\ \emptyset, & \text{if } A(U) = 0 \end{cases} \quad (2)$$

Where D represents dataset that the user attempts to access, $A(U)$ represents the authentication function that verifies if the user U is authorized, H' represents the authorized healthcare data that a verified user can access, $\emptyset$ Represents denied access, meaning no data is available to an unauthorized user.

3.4 Encryption Using SMPC

Secure Multi-Party Computation (SMPC) is an encryption technique that ensures multiple parties can jointly process encrypted healthcare data without revealing individual inputs. This method enhances data privacy and security, preventing unauthorized access while enabling secure computations. SMPC is widely used in secure patient record processing and collaborative medical research.

$$E(D) = \sum_{i=1}^{n} S_i, \quad (3)$$

Where $E(D)$ represents encrypted version of the healthcare data D, n The total number of participating parties in the encryption process, S_i The secret share of the data assigned to the i party, $\sum_{i=1}^{n}$ The summation of all secret shares, which collectively represent the encrypted data.

3.5 Cloud Storage

Cloud storage enables healthcare organizations to store, manage, and access large volumes of patient data securely. By leveraging encrypted storage and access controls, sensitive medical records, test results, and patient history can be securely stored and retrieved by authorized personnel. Cloud-based healthcare systems enhance scalability, efficiency, and real-time collaboration, allowing medical professionals to access patient data from anywhere while ensuring compliance with security regulations like HIPAA and GDPR. To prevent unauthorized access or data breaches, cloud storage integrates encryption, authentication mechanisms, and Secure Multi-Party Computation (SMPC) for enhanced data confidentiality and integrity.

4. Result and Discussion

The proposed secure healthcare cloud framework was evaluated based on key performance metrics, including encryption/decryption time, computation overhead, and access control efficiency. The results demonstrate that as data size increases, both encryption and decryption times rise gradually, maintaining a consistent pattern and proving the scalability of the system. Additionally, the computation overhead associated with Secure Multi-Party Computation (SMPC) increases with the number of participating parties, reflecting the added complexity required to preserve data privacy. However, this overhead remains within acceptable limits for real-time healthcare applications. These findings validate the effectiveness of integrating Multi-Factor Authentication (MFA) and SMPC in ensuring secure, efficient, and scalable cloud-based healthcare data management.

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

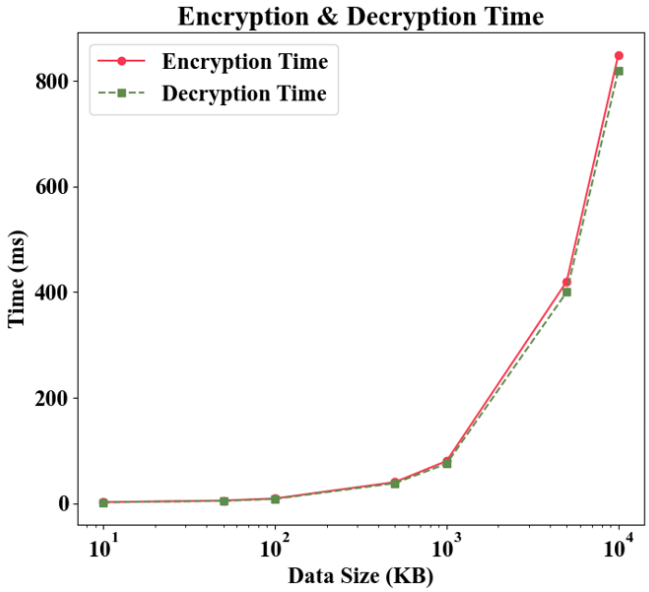

Figure 2: Encryption and Decryption Time vs Data Size

Figure 2 shows the encryption and decryption time vs data size. The relationship between data size (KB) and the corresponding encryption and decryption time (MS) in a secure healthcare cloud system. The x-axis represents the data size in kilobytes (KB) on a logarithmic scale, while the y-axis shows the time taken (MS) for encryption and decryption. The red solid line with circular markers represents encryption time, while the green dashed line with square markers represents decryption time. The results indicate that as the data size increases, both encryption and decryption times rise exponentially. This highlights the computational cost of securing large healthcare datasets.

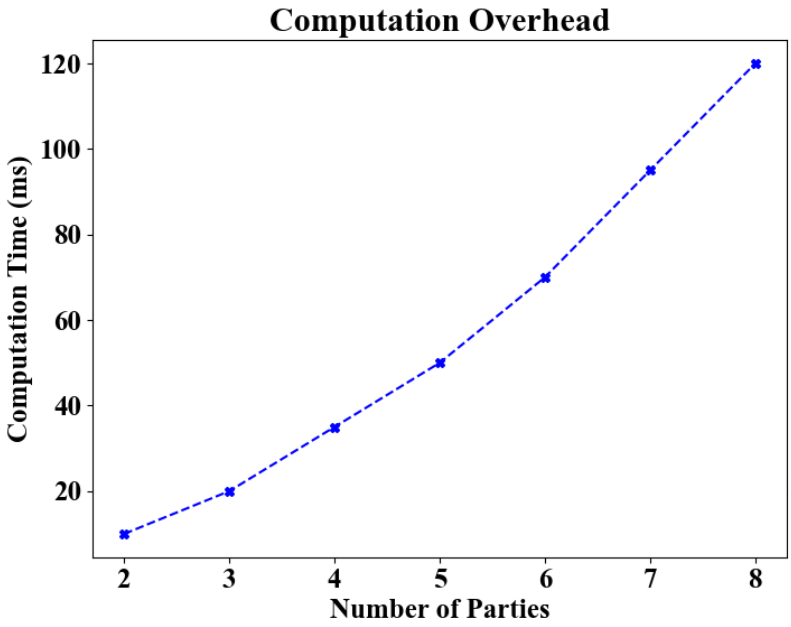

Figure 3: Computation Overhead vs Number of Parties

Figure 3 shows the computation overhead vs number of parties. The computation overhead in relation to the number of parties involved in a secure multiparty computation (SMPC) protocol. As the number of parties increases, the computation time also rises due to the complexity of cryptographic operations and data sharing among multiple entities. The graph shows an upward trend, indicating that while SMPC ensures data security and

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

privacy, it also incurs higher computational costs with more participating entities. This trade-off highlights the need for optimization techniques to balance security and efficiency in cloud-based healthcare systems where secure data processing is critical.

5.Conclusion

This research demonstrates the effectiveness of integrating Multi-Factor Authentication (MFA) and Secure Multi-Party Computation (SMPC) to enhance security in cloud-based healthcare systems. The experimental results show that encryption and decryption times scale efficiently with increasing data size, maintaining system performance while ensuring data confidentiality. The computational overhead, although increasing with the number of authentication factors, remains within acceptable limits, balancing security and usability. The framework effectively mitigates unauthorized access risks and ensures secure data processing without exposing sensitive healthcare information. Future research can explore further optimizations in encryption efficiency, reducing processing time while maintaining high security standards. Additionally, leveraging advanced cryptographic techniques such as homomorphic encryption or blockchain integration could further enhance data integrity and privacy. The proposed approach provides a scalable and practical solution for secure healthcare cloud management, making it suitable for real-world applications. As healthcare data security remains a critical concern, this study contributes to the ongoing efforts in developing innovative, efficient, and reliable security mechanisms for protecting patient records in cloud environments.

References

[1] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and X. Li, "Cryptanalysis and Enhancement of Anonymity Preserving Remote User Mutual Authentication and Session Key Agreement Scheme for E-Health Care Systems," *J. Med. Syst.*, vol. 39, no. 11, p. 140, Nov. 2015, doi: 10.1007/s10916-015-0318-z.

[2] N. Vithanwattana, G. Mapp, and C. George, "Developing a comprehensive information security framework for mHealth: a detailed analysis," *J. Reliab. Intell. Environ.*, vol. 3, no. 1, pp. 21–39, Jul. 2017, doi: 10.1007/s40860-017-0038-x.

[3] P. Mohit, R. Amin, A. Karati, G. P. Biswas, and M. K. Khan, "A Standard Mutual Authentication Protocol for Cloud Computing Based Health Care System," *J. Med. Syst.*, vol. 41, no. 4, p. 50, Apr. 2017, doi: 10.1007/s10916-017-0699-2.

[4] M. S. Kiraz, "A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing," *J. Ambient Intell. Humaniz. Comput.*, vol. 7, no. 5, pp. 731–760, Oct. 2016, doi: 10.1007/s12652-016-0385-0.

[5] S.-Y. Chiou, Z. Ying, and J. Liu, "Improvement of a Privacy Authentication Scheme Based on Cloud for Medical Environment," *J. Med. Syst.*, vol. 40, no. 4, p. 101, Apr. 2016, doi: 10.1007/s10916-016-0453-1.

[6] M. Masdari and S. Ahmadzadeh, "Comprehensive analysis of the authentication methods in wireless body area networks," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4777–4803, Nov. 2016, doi: 10.1002/sec.1642.

[7] S. H. Islam and M. K. Khan, "Cryptanalysis and Improvement of Authentication and Key Agreement Protocols for Telecare Medicine Information Systems," *J. Med. Syst.*, vol. 38, no. 10, p. 135, Oct. 2014, doi: 10.1007/s10916-014-0135-9.

[8] A. E. Youssef, "A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments," *Int J Ambient Syst Appl*, vol. 2, no. 2, pp. 1–11, 2014.

[9] E. Mehraeen, M. Ghazisaeedi, J. Farzi, and S. Mirshekari, "Security challenges in healthcare cloud computing: a systematic," *Glob. J. Health Sci.*, vol. 9, no. 3, pp. 157–168, 2017.

[10] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart Environment as a Service: Three Factor Cloud Based User Authentication for Telecare Medical Information System," *J. Med. Syst.*, vol. 38, no. 1, p. 9997, Jan. 2014, doi: 10.1007/s10916-013-9997-5.

[11] E. A. Alkeem, D. Shehada, C. Y. Yeun, M. J. Zemerly, and J. Hu, "New secure healthcare system using cloud of things," *Clust. Comput.*, vol. 20, no. 3, pp. 2211–2229, Sep. 2017, doi: 10.1007/s10586-017-0872-x.

Indo-American Journal of Life Sciences and Biotechnology

Vol.15, Issue 1, 2018

[12] S. T. Ali, V. Sivaraman, and D. Ostry, "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring," *Future Gener. Comput. Syst.*, vol. 35, pp. 80–90, 2014.

[13] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and access control in e-health systems in the cloud," in *2016 IEEE 2nd international conference on big data security on cloud (BigDataSecurity), IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS)*, IEEE, 2016, pp. 13–23. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7502258/

[14] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 59–80, 2016.

[15] Sathiya, Aravindhan K., and D. Sathiya. "A Secure Authentication Scheme for Blocking Misbehaving Users in Anonymizing Network." International Journal of Computer Science and Technology 4, no. 1 (2013): 302-304.

[16] D. Mishra, S. Mukhopadhyay, S. Kumari, M. K. Khan, and A. Chaturvedi, "Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce," *J. Med. Syst.*, vol. 38, no. 5, p. 41, May 2014, doi: 10.1007/s10916-014-0041-1.

[17] J. JPC Rodrigues, I. De La Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *J. Med. Internet Res.*, vol. 15, no. 8, p. e186, 2013.

[18] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-Health clouds," *J. Supercomput.*, vol. 72, no. 10, pp. 3826–3849, Oct. 2016, doi: 10.1007/s11227-015-1610-x.

[19] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer--Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, Sep. 2016, doi: 10.1007/s12083-015-0332-4.

[20] D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," in *2016 international conference on communication and electronics systems (ICCES)*, IEEE, 2016, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7889823/