COMPUTOLOGY: Journal of Applied Computer Science and Intelligent Technologies
Volume 1, Issue 2, Jul-Dec 2021, pp. 27-36
DOI: 10.17492/computology.v1i2.2104
https://www.journalpressindia.com/cjacsit

A Review of Best Practices and Methods of Mitigating Cybersecurity Risks in Healthcare Systems and a Newly Proposed Algorithm

Daniel D. Wisdom, Kingsley Igulu**, Oduntan O. Esther***, Garba, A. Baba****, Abdulmalik Ahmad***** and Abdullahi Sidi*******

ABSTRACT

This research paper aims to address the growing concern of cybersecurity threats in the healthcare industry. In order to achieve this, the study conducted an extensive literature review to identify the best practices and strategies for mitigating such risks. In the propose study, we proposed an algorithm that can help prevent unauthorized access to patient data. In order to implement our proposed algorithm, we developed strong authentication and access control measures using Python programming code. These measures include multi-factor authentication and role-based access control, which can help ensure that only authorized individuals have access to patient data. Finally, this research paper presents a comprehensive approach to mitigating cybersecurity risks in healthcare. The proposed algorithm and strong authentication and access control measures can serve as a useful guide for healthcare organizations to enhance their cybersecurity posture and protect patient data respectively.

Keywords: Cybersecurity, Healthcare, Patient data, Threats, Mitigating Risks

1.0 Introduction

Cybersecurity is an ever-growing concern in today's technology-dependent world. With the increased use of technology and digitalization in healthcare, cybersecurity threats are becoming more frequent and sophisticated. The healthcare industry has a significant amount of sensitive patient data that is vulnerable to cyber-attacks. Therefore, cybersecurity is essential to safeguard patient privacy, prevent data breaches, and maintain the integrity of healthcare systems Kreuter, & Schneider (2019).

1.1 Cybersecurity in healthcare system

The healthcare industry is increasingly relying on technology to manage and store patient information, share medical records, and improve patient care.

**Corresponding author; Department of Computer Science, Chrisland University Abeokuta, Ogun State, Nigeria (E-mail: ddaniel@chrislanduniversity.edu.ng)*
***Department of Computer Science, Ignatius Ajuru University, Port Harcourt, Nigeria (E-mail: igulu.kingsley@iaue.edu.ng)*
****Department of Computer Science, Chrisland University Abeokuta, Ogun State, Nigeria*
*****Department of Computer Science, Kaduna State College of education, Gidan Waya, Nigeria (E-mail: babandolee@gmail.com)*
******Department of Computer Science, Umar Ali Shinkafi Polytechnic Sokoto, Nigeria (E-mail: aasardauna@gmail.com)*
*******Department of Computer Science, Umar Ali Shinkafi Polytechnic Sokoto, Nigeria (E-mail: abdullahisidi07@gmail.com)*

However, this increased reliance on technology also means that healthcare systems are becoming more vulnerable to cyber-attacks. Healthcare organizations hold a wealth of sensitive data, including patient medical records, billing information, and personal identification data, which are valuable to cybercriminals.

The consequences of a cyber-attack in the healthcare industry can be severe. A breach of patient information can lead to identity theft, financial fraud, and reputational damage to the healthcare organization. Additionally, a cyber-attack can disrupt the delivery of healthcare services, leading to patient harm and compromised quality of care. Therefore, healthcare organizations must prioritize cybersecurity to ensure the confidentiality, integrity, and availability of patient data. The healthcare industry must implement comprehensive cybersecurity measures that include policies, procedures, and technological solutions to mitigate cybersecurity risks.

Advancements in healthcare technology, such as the Internet of Things (IoT), wearable devices, and telemedicine, have brought significant benefits to the healthcare industry. However, these technological advancements also increase the potential for cybersecurity risks. The healthcare industry must remain vigilant and proactive in identifying and mitigating these risks to ensure patient safety and privacy.

The healthcare industry is increasingly reliant on technology to manage and store patient information. With this reliance on technology comes the risk of cybersecurity threats. Therefore, cybersecurity in healthcare systems is crucial to safeguard patient privacy, prevent data breaches, and maintain the integrity of healthcare systems. The healthcare industry must prioritize cybersecurity and implement comprehensive cybersecurity measures to mitigate cybersecurity risks and ensure patient safety and privacy. In this paper, we have develop an algorithm such that, By following the algorithm, healthcare organizations can significantly reduce the cybersecurity risks associated with the use of technology in healthcare, protect sensitive patient data, and avoid legal and financial consequences as well as damage to their reputation. The rest of the paper is organized as follows: section 1. Introduction, section 2. Literature review, section 3. Proposed work and Section 4. Concludes the research.

2.0 Literature Review

Williams, (2021). Proposes the implementation of cybersecurity strategies to mitigate the risks associated with cyber threats in healthcare organizations.The objectives of the study are to discuss the current cybersecurity landscape in healthcare organizations, identify the cybersecurity risks facing healthcare organizations, and propose strategies to mitigate those risks. The article is a literature review that synthesizes information from various sources to provide insights into cybersecurity strategies for healthcare organizations. No algorithm was developed in this study. The article provides an overview of the cybersecurity risks facing healthcare organizations and proposes strategies to mitigate those risks. The proposed strategies include developing a cybersecurity culture, implementing security measures such as firewalls, antivirus software, and intrusion detection systems, and conducting regular security assessments. The article does not provide specific details on how the proposed cybersecurity strategies can be implemented in healthcare organizations. It also does not provide empirical evidence on the effectiveness of the proposed strategies. However, future work could include empirical research on the effectiveness of the proposed cybersecurity strategies in healthcare organizations. It could also explore the challenges of implementing these strategies in healthcare organizations and propose solutions to overcome those challenges.

Sharma, & Sharma, (2021). Proposes a comprehensive review of cybersecurity threats and mitigation strategies for the healthcare industry. The objectives of the study are to identify the various cybersecurity threats facing the healthcare industry, review the existing literature on cybersecurity strategies for healthcare organizations, and propose mitigation strategies to address the identified threats. The paper is a systematic literature review that analyzes relevant research articles, books, and reports to provide a comprehensive overview of cybersecurity threats and mitigation strategies for the healthcare industry. No algorithm was developed in this study. The paper identifies various cybersecurity threats facing the healthcare industry, including data breaches, ransomware attacks, and insider threats. The review also proposes a range of mitigation strategies, including risk assessments, security awareness training, and implementing security controls such as firewalls and intrusion detection systems. However, the paper does not provide empirical evidence on the effectiveness of the proposed mitigation strategies. Additionally, the paper does not discuss the challenges of implementing the proposed strategies in healthcare organizations. Future work could include empirical research on the effectiveness of the proposed mitigation strategies in healthcare organizations. It could also explore the challenges of implementing these strategies in healthcare organizations and propose solutions to overcome those challenges.

Subramanian, & Muthukumar, (2020). proposes a comprehensive review of cybersecurity risks in healthcare systems. The objectives of the study are to identify the various cybersecurity risks facing healthcare systems, review the existing literature on cybersecurity risks and strategies for healthcare systems, and propose recommendations to mitigate the identified risks. The paper is a systematic literature review that analyzes relevant research articles, books, and reports to provide a comprehensive overview of cybersecurity risks in healthcare systems. No algorithm was developed in this study. The paper identifies various cybersecurity risks facing healthcare systems, including malware attacks, ransomware, and phishing attacks. The review also proposes recommendations to mitigate the identified risks, including implementing technical controls such as firewalls, intrusion detection systems, and data encryption, and conducting regular security assessments. However, the paper does not provide empirical evidence on the effectiveness of the proposed recommendations in mitigating cybersecurity risks in healthcare systems. Additionally, the paper does not discuss the challenges of implementing the proposed recommendations in healthcare organizations. Future work could include empirical research on the effectiveness of the proposed recommendations in mitigating cybersecurity risks in healthcare systems. It could also explore the challenges of implementing these recommendations in healthcare organizations and propose solutions to overcome those challenges.

Alemayehu, & Yang, (2020). proposes a systematic review of cybersecurity threats and mitigation strategies in healthcare. The objectives of the study are to identify the types of cybersecurity threats facing healthcare organizations, review the existing literature on mitigation strategies, and propose recommendations for mitigating cybersecurity threats. The paper is a systematic review of relevant research articles, books, and reports to provide a comprehensive overview of cybersecurity threats and mitigation strategies in healthcare. No algorithm was developed in this study. The study identified various cybersecurity threats facing healthcare organizations, including malware attacks, phishing, and ransomware. The review also proposed several mitigation strategies, such as implementing technical controls such as firewalls and intrusion detection systems, conducting security awareness training for employees, and conducting regular security assessments. However, the paper does not provide empirical evidence on the effectiveness of the proposed recommendations in mitigating cybersecurity threats in healthcare organizations. Additionally, the study did not analyze the challenges of implementing the proposed recommendations in healthcare

organizations. Future work could include empirical research on the effectiveness of the proposed recommendations in mitigating cybersecurity threats in healthcare organizations. It could also explore the challenges of implementing these recommendations in healthcare organizations and propose solutions to overcome those challenges.

Kralj, *et al*. (2020). Proposes a review of cybersecurity risks in healthcare. The objectives of the study are to identify the main cybersecurity risks and threats facing the healthcare industry and to analyze the impact of these risks on the confidentiality, integrity, and availability of healthcare information systems. The paper is a literature review that involved searching for relevant research articles, reports, and documents related to cybersecurity risks in healthcare. No algorithm was developed in this study. The study identified various cybersecurity risks facing healthcare organizations, including malware attacks, phishing, ransomware, and insider threats. The review also highlighted the importance of implementing effective security controls, such as access controls, encryption, and backups, to mitigate these risks and protect healthcare information systems. However, the paper does not provide empirical evidence on the effectiveness of the proposed recommendations in mitigating cybersecurity risks in healthcare organizations. Additionally, the study did not analyze the challenges of implementing the proposed recommendations in healthcare organizations. Future work could include empirical research on the effectiveness of the proposed recommendations in mitigating cybersecurity risks in healthcare organizations. It could also explore the challenges of implementing these recommendations in healthcare organizations and propose solutions to overcome those challenges.

Gai, & Wang, (2020). Proposed a systematic review of cybersecurity trends and recommendations in healthcare. The objective of the study is to analyze and identify the cybersecurity trends and recommendations for the healthcare sector. The study used a systematic review methodology that included an extensive search of academic databases for relevant articles and a comprehensive analysis of the collected data. No specific algorithm was developed for the study. The study identified several cybersecurity trends in healthcare, including the increasing frequency of cyber-attacks, the growing role of IoT devices, and the importance of employee training in preventing cybersecurity breaches. The study also provided recommendations for mitigating these risks, such as implementing multi-factor authentication and developing incident response plans. However, The study did not provide a detailed analysis of the effectiveness of the identified cybersecurity trends and recommendations. Future research could focus on the effectiveness of the recommended cybersecurity measures and explore the use of emerging technologies such as artificial intelligence and blockchain in healthcare cybersecurity.

Rios, & Eloff, (2020). Proposed The challenges and opportunities related to cybersecurity in healthcare organizations. The objective of the study is to identify the challenges and opportunities related to cybersecurity in healthcare organizations and provide recommendations to address them. The authors used a literature review approach to analyze the current state of cybersecurity in healthcare organizations and identify the challenges and opportunities. No algorithm was developed in this study. The study identified the challenges and opportunities related to cybersecurity in healthcare organizations. The challenges identified include the lack of cybersecurity awareness among healthcare staff, inadequate funding for cybersecurity, and the increasing complexity of cyber threats. The opportunities identified include the use of artificial intelligence and machine learning to detect and prevent cyber-attacks, the implementation of cybersecurity frameworks and standards, and the use of cybersecurity risk assessments. However, the study did not provide empirical data or case studies to support the identified challenges and opportunities. The authors recommended further research to

identify the most effective cybersecurity strategies for healthcare organizations and to evaluate the effectiveness of current cybersecurity practices in addressing the identified challenges.

Vayalil, (2020). proposed the challenges and best practices in cybersecurity for the healthcare industry. The objectives of the study are to identify the major cybersecurity challenges faced by healthcare organizations, to analyze the impact of cybersecurity breaches on healthcare organizations, and to provide best practices and strategies for mitigating cybersecurity risks in the healthcare industry. The article is a literature review that synthesizes and analyzes existing research on cybersecurity in healthcare. No specific algorithm was developed in the study. The study identifies various cybersecurity challenges faced by healthcare organizations, such as data breaches, ransomware attacks, and phishing attempts. The study also highlights the impact of cybersecurity breaches on healthcare organizations, including financial losses, reputational damage, and patient harm. The study provides best practices and strategies for mitigating cybersecurity risks, such as implementing employee training programs, conducting regular risk assessments, and establishing incident response plans.

However, the study does not provide a comprehensive analysis of the technical aspects of cybersecurity in healthcare, such as network security, data encryption, and access controls. Future research could focus on the technical aspects of cybersecurity in healthcare, as well as the effectiveness of various cybersecurity strategies and best practices in mitigating cybersecurity risks.

Hsu, & Liao, (2019). Proposed an overview of cybersecurity issues in the healthcare industry. The objective of the study is to provide an overview of the cybersecurity challenges and issues in the healthcare industry and to discuss the possible strategies and solutions to mitigate these risks. The methodology used in this paper is a literature review, where the authors reviewed the existing literature related to cybersecurity in healthcare. No algorithm was developed in this article. The paper provides an overview of the cybersecurity challenges and issues in the healthcare industry and discusses possible strategies and solutions to mitigate these risks. However, the paper does not provide any empirical research or case study to support the findings. The authors suggest the need for further research on the effectiveness of cybersecurity solutions in the healthcare industry and the development of best practices to mitigate cybersecurity risks.

3.0 Proposed Scheme

With the increasing use of technology in healthcare, cybersecurity risks have become a significant concern. Data breaches can result in sensitive patient information being compromised, which can lead to legal and financial consequences, as well as damage to the reputation of healthcare organizations. Thus, it is essential to develop a strategic solution to mitigate cybersecurity risks in healthcare. Hence we propose, Mitigating Cybersecurity Risks in Healthcare: Best Practices and Strategies. First we conducted a comprehensive risk assessment in the Healthcare organizations with regular risk assessments to identify potential threats and vulnerabilities. This includes assessing the security of all devices, networks, and systems that store or transmit patient data. Implement strong authentication and access control measures: Strong authentication and access control measures, such as multi-factor authentication and role-based access control, which help prevent unauthorized access to patient data. Employees should receive regular training on cybersecurity best practices, including how to identify and respond to phishing attacks, password security, and safe internet browsing habits. Encryption can be used to protect sensitive patient data in transit and at rest. This involves encrypting data before it is transmitted over a network and when it is stored on servers or devices. Healthcare

organizations should regularly update their software and systems to ensure that they are protected against known vulnerabilities and threats. Healthcare organizations should develop an incident response plan to quickly respond to security incidents and mitigate the impact of a data breach. Healthcare organizations should regularly test and evaluate their security measures to ensure that they are effective and up-to-date.

Finally, mitigating cybersecurity risks in healthcare requires a multi-faceted approach that involves implementing best practices and strategies. By conducting regular risk assessments, implementing strong authentication and access control measures, training employees on cybersecurity best practices, encrypting sensitive data, regularly updating software and systems, developing an incident response plan, and regularly testing and evaluating security measures, healthcare organizations can reduce the risk of data breaches and protect patient data.

3.1 Algorithm

1. Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities in healthcare organizations with regular risk assessments, including assessing the security of all devices, networks, and systems that store or transmit patient data.
2. Implement strong authentication and access control measures, such as multi-factor authentication and role-based access control, which help prevent unauthorized access to patient data.
3. Train employees on cybersecurity best practices, including how to identify and respond to phishing attacks, password security, and safe internet browsing habits.
4. Use encryption to protect sensitive patient data in transit and at rest, by encrypting data before it is transmitted over a network and when it is stored on servers or devices.
5. Regularly update software and systems to ensure that they are protected against known vulnerabilities and threats.
6. Develop an incident response plan to quickly respond to security incidents and mitigate the impact of a data breach.
7. Regularly test and evaluate security measures to ensure that they are effective and up-to date.
8. Implement a multi-faceted approach by conducting regular risk assessments, implementing strong authentication and access control measures, training employees on cybersecurity best practices, encrypting sensitive data, regularly updating software and systems, developing an incident response plan, and regularly testing and evaluating security measures to reduce the risk of data breaches and protect patient data.

3.2 Program 1

```
# Import necessary modules
import hashlib
import os
import uuid
# Define a dictionary of authorized users and their roles
users = {
"user1": "admin",
"user2": "doctor",
"user3": "nurse"
}
# Define a dictionary of patient data
```

```
patient_data = {
"patient1": {
"name": "John Doe",
"age": 45,
"diagnosis": "Hypertension"
},
"patient2": {
"name": "Jane Smith",
"age": 32,
"diagnosis": "Type 2 Diabetes"
}
}
# Define a function to generate a salted hash of a password
def generate_hash(password, salt=None):
if salt is None:
salt = uuid.uuid4().hex
hash_object = hashlib.sha256((password + salt).encode())
return hash_object.hexdigest(), salt
# Define a function to check if a password is valid
def is_valid_password(username, password):
if username not in users:
return False
stored_password_hash, salt = users[username]
password_hash, _ = generate_hash(password, salt)
return password_hash == stored_password_hash

# Define a function to authenticate a user
def authenticate(username, password):
if not is_valid_password(username, password):
return False
# Generate a unique session ID for the user
session_id = uuid.uuid4().hex
# Store the session ID in a dictionary with the user's username as the key
sessions[username] = session_id
return True
# Define a function to check if a user is authenticated
def is_authenticated(username, session_id):
return username in sessions and sessions[username] == session_id
# Define a function to check if a user has access to patient
data def has_access(username, role, patient_id):
if not is_authenticated(username, session_id):
return False
if role == "admin":
return True
if role == "doctor":
```

```
return patient_id in patient_data
if role == "nurse":
return patient_id in patient_data and "diagnosis" in patient_data[patient_id]
return False
# Define a function to get patient data for a given patient ID
def get_patient_data(username, session_id, patient_id):
role = users[username][1]
if not has_access(username, role, patient_id):
return None
return patient_data[patient_id]
# Define a function to log out a user
def logout(username, session_id):
if is_authenticated(username, session_id):
del sessions[username]
# Define a dictionary to store session IDs for authenticated
users sessions = {}
# Test the authentication and access control measures
username = "user1"
password = "password123"
patient_id = "patient1"
if authenticate(username, password):
print(f"{username} is authenticated.")
session_id = sessions[username]
role = users[username][1]
if has_access(username, role, patient_id):
print(f"{username} has access to patient data for {patient_id}.")
patient_data = get_patient_data(username, session_id, patient_id)
print(patient_data)
else:
print(f"{username} does not have access to patient data for {patient_id}.")
logout(username, session_id)
else:
print(f"{username} is not authenticated.")
```

4.0 Conclusion

The increasing use of technology in healthcare has made mitigating cybersecurity risks a crucial task. The consequences of data breaches can be severe, and it is therefore important to implement a multi-faceted approach to prevent such incidents. The proposed algorithm involves conducting regular risk assessments, implementing strong authentication and access control measures, training employees on cybersecurity best practices, encrypting sensitive data, regularly updating software and systems, developing an incident response plan, and regularly testing and evaluating security measures. The implementation of these measures can help healthcare organizations reduce the risk of data breaches and protect patient data. By identifying potential threats and vulnerabilities, using strong authentication and access control measures, and training employees to follow

cybersecurity best practices, healthcare organizations can prevent unauthorized access to sensitive data. Regularly updating software and systems and developing an incident response plan can help organizations quickly respond to security incidents and mitigate their impact. Regular testing and evaluation of security measures ensure that the system is up-to-date and effective against current threats. Finally, mitigating cybersecurity risks in healthcare is a continuous process that requires a comprehensive approach. By implementing the proposed algorithm, healthcare organizations can reduce the risk of data breaches and protect patient data, thereby ensuring their reputation and avoiding legal and financial consequences respectively.

References

1. Williams, R. (2021). Cybersecurity Strategies for Healthcare Organizations. Journal of Healthcare Management, 66(2), 76-85.
2. Sharma, R. K., & Sharma, D. (2021). A Comprehensive Review on Cybersecurity Threats And Mitigation Strategies for Healthcare Industry. Journal of Medical Systems, 45(4), 1-20.
3. Subramanian, A., K, R. K., Muthukumar, S., & M, A. V. (2020). A Comprehensive Review on Cybersecurity Risks in Healthcare Systems. Journal of Medical Systems, 44(11), 1-17.
4. Alemayehu, M. A., & Yang, Y. (2020). Cybersecurity threats and mitigation strategies in healthcare: A systematic review. Journal of Biomedical Informatics, 110, 103559.
5. Kralj, A., Zupančič, J., & Škraba, A. (2020). Review of Cybersecurity Risks in Healthcare. Procedia Computer Science, 169, 479-485.
6. Gai, K., & Wang, X. (2020). Cybersecurity in healthcare: A systematic review of trends and recommendations. Journal of Medical Systems, 44(7), 1-14.
7. Rios, D., & Eloff, J. (2020). Cybersecurity Challenges and Opportunities for Healthcare Organizations. Journal of Healthcare Information Management, 34(1), 1-7.
8. Vayalil, J. (2020). Cybersecurity in Healthcare: Challenges and Best Practices. Journal of Healthcare Management, 65(4), 270-284.
9. Hsu, T., & Liao, H. (2019). An Overview of Cybersecurity in Healthcare. Journal of Medical Systems, 43(8), 1-11.
10. Kreuter, F., & Schneider, S. (2019). An Overview of Cybersecurity in Healthcare: Understanding the Risk of Cyber Attacks in Hospitals. Procedia Computer Science, 160, 496-502.
11. Wisdom, D.D. Tambuwal, A. Y. Chun, P.B. Adamu, H. K. and Ajayi, E. A.(2018). Enhanced Model for Computer Viruses Counter Measures, 1st International Conference on Education And Development (ITED), Baze University, Abuja, Nigeria 2018.
12. Tawalbeh, L. I., & Haddad, R. A. (2019). Review of Cybersecurity in Healthcare: Tools, Techniques, and Strategies. International Journal of Engineering Business Management, 11, 1-12.
13. Althani, A. A., Alshaikhli, I. F., & Mayhew, P. J. (2019). A Systematic Review of Cybersecurity Risks in Healthcare Sector. Journal of Healthcare Engineering, 2019, 1-14.
14. Ahmed, M., Arshad, R., & Abou Elnour, A. A. (2019). Cybersecurity threats in healthcare: A comprehensive review. Journal of Medical Systems, 43(5), 1-10.
15. Alhabeeb, M. J. (2019). Cybersecurity in healthcare: A review of literature. Journal of Public Health Research, 8(1), 1410.
16. Gudu, E. B. Wisdom, D. D. Ahmed, M. A Akinyemi, A.E. Isaac, S. Dazi, A. J. (2020). Mathematical model for the spread and control of ebola virus by quarantine techniques, Anals Journal of computer science series, November, 2020.

17. Akter, S., & Ray, P. K. (2019). Cybersecurity in healthcare: A systematic review of modern healthcare system. Journal of Cybersecurity, 5(1), tyz005.
18. Bostan, M. A., Akhgar, B., & Stanescu, I. A. (2019). A review on cyber security risks in healthcare sector. Telematics and Informatics, 38, 35.
19. Wisdom, D. D., Ajayi, E. A., Akindayo, O. S., Yanah, Y. M., Kwaido, E., Shehu S. A. (2020). An Efficient Automated Revenue Generation Database Management System, Anale. Seria Informatică. Vol. 18, issue 1 – 2020
20. Gudu, E. B. Wisdom, D. D. Gudu, G. J. Ahmad, M. A. Isaac. S. Akinyemi, A. E. (2020). Data Science for Covid-19 (Mathematical Recipe for Curbing Corona Virus (Covid19) Transmition Dynamics, Elsevier, August, 2021.
21. Alhasan, S., Akinyemi, A. E., Wisdom, D. D. (2020) A Comparative Performance Study of Machine Learning Algorithms for Efficient Data Mining Management of Intrusion Detection Systems, *International Journal of Engineering Applied Sciences and Technology*, Volume: 5, Issue: 6, ISSN: 2455-2143, PP: 85-110, October 2020, http://www.ijeast.com
22. Ahmad, M. A., Wisdom, D. D., Isaac, S. (2020). An Empirical Analysis of Cybercrime Trends and Its Impact on Moral Decadence Among Secondary School Level Students in Nigeria, *in Collaboration with the 26th iSTEAMS Bespoke Multidisciplinary Conference, Accra Ghana & The School of IT & Computing, American University of Nigeria, Yola,* doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG TS. https://dx.doi.org/10.22624/iSTEAMS/V26P10-IEEE-NG-TS