MSRDG International Journal of Computer Scientific Technology & Electronics Engineering ISSN: 3107 - 426X
Volume 2 Issue 1, 1-7, February 2026 ©2026 Multi-Sense Research Developing Group
https://doi.org/10.66037/MSRDG-IJCSTEE/V2I1P101

Improving the Security of the Internet of Things with the Implementation of the PrimeDigitBR Methodology

Pusa Prashanth[1], Sathwika Gade[2]

[1]*Department of Data Science and Artificial Intelligence, Sheffield Hallam University, Sheffield, London, UK.*
[2]*Department of Data Science and Computational Intelligence, Coventry University, Coventry, West Midlands, United Kingdom.*
[1]*c5055216@hallam.shu.ac.uk*

Abstract - *Encryption, which is indispensable for safeguarding sensitive information, can also render any malevolent content illegible, allowing it to remain undetected in any network. The objective of concealing the malicious payload is achieved through encryption, which is employed by malware authors to conceal their code. A distinctive approach that goes by the name of PrimeDigitBR. This recommendation is being made in the hopes that it will be an effective solution to the difficulties. There are three steps in the first stage. First, change the text from plain text to "ASCII code" as P. The second step is to use the "ASCII code" of N to find the prime number. To do the third step, you need to use Equation 1. Take the numbers from P1 and pair them up. Then, change the cells in the matrix. There are also three steps in the second stage. The first step is to figure out what Q is worth. The second step is to find the numbers for N-1. The last step is to use and apply Equation 2. From the Q1 values, make a pair and swap the cell values in the matrix. However, the values in the 0th cell start from the backwards. The process of decryption is understood to be the opposite of this conversion, and it is via this process that the message is eventually received in its original format. In compared to encryption methods that are considered more traditional, the suggested solution offers a greater degree of security.*

Keywords - *Encryption, Performance, RB22, Shor's, PrimeDigitBR*

1. Introduction

The internet's swift evolution has facilitated the connection and interaction of individuals and devices from various countries. This interconnectivity facilitated humans in a variety of ways. Nevertheless, the volume of personal and confidential information that was generated was a direct result of the increased reliance of "corporate, healthcare, and individual entities" on the internet to perform even the most basic of daily activities.

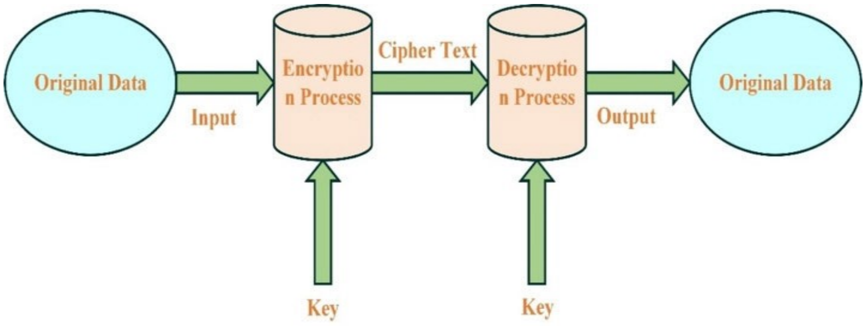

Fig. 1 The process of transmitting and receiving data

The problems with "privacy and security" that used to be connected to desktop computers have changed because of the rise of "low-power devices". Because of these big steps forward in computing and cryptanalysis, encryption methods will need to be changed in order to keep up. One method that uses both a Feistel structure and sequences is symmetric key encryption. Using replacements, permutations, and the ideas of genetic algorithms, the method makes new subkeys for each round. This makes the process faster and safer. Lightweight cryptography is different from regular computer gear and software in the way the user needs to approach it.

From Figure 1. When the process of encryption is being carried out, the plaintext that represents the original data is encoded by using a specific key, which leads to the eventual production of encrypted text.

2. Literature Survey

The author looked into “Shor's Algorithm” and “Quantum Fourier Transform”. This method is how safe cryptosystems are [1]. During their conversation, they brought up the idea of “Las Vegas algorithms” and the quantum computer. People use this method of factorization and the logarithms of discrete [2]. The authors are now using “machine learning methods” [3] and they have put in place a number of methods [4].The author looked into how safe the “RSA” method was and gave out the encryption key in a way that anyone could understand [5]. The strong “encryption methods” are made possible in AI [6] and how machine learning models work. They looked into the cryptosystems of the elliptic curve as part of their academic work. This shape is used when performing the discrete logarithm, and it is a very reliable method [7]. The piece talked about how the elliptic curve can be used for encryption. Both the key and the attack that was started by hackers are traded, and this curve helps protect against the attack [8]. The “encryption and decryption” worked as expected in terms of both security and usefulness [9]. The authors focus on the security of encrypted data [10]. The RSA method [11] is used to demonstrate this cryptographic idea for comparison purposes. In this research paper, the author talked about how to use machine learning techniques to get data from social media sites [12]. A lot of attention has been paid to support vector machine (SVM) methods in the field of machine learning. The writers looked at and studied all 67 different areas that make up this field [13]. They used maths to compare the different security algorithms and show which ones worked better than the others [14]. The cloud computing piece [15] that this study refers to shows proof that mobile devices can keep a person's health information very safe. For the most part, this text is about ways to use cryptography. We came up with the Security of PrimeDigitBR method after reading a lot of related literature. We are going to talk about this method in this part.

3. Methodology

There are two steps to the new method. First stage has 3 steps, 1st, change the text from plain text to “ASCII code” as P. 2nd is to use the “ASCII code” of N to find the prime number. 3rd, you need to use Equation 1. Take the numbers from P1 and pair them up. Then, change the cells in the matrix. Second stage has 3 steps. 1st is to figure out what Q is worth. 2nd is to find the numbers for N-1. The last step is to use and apply Equation 2. From the Q1 values, make a pair and swap the cell values in the matrix. However, the values in the 0th cell start from the backwards are shown in Figure 2.

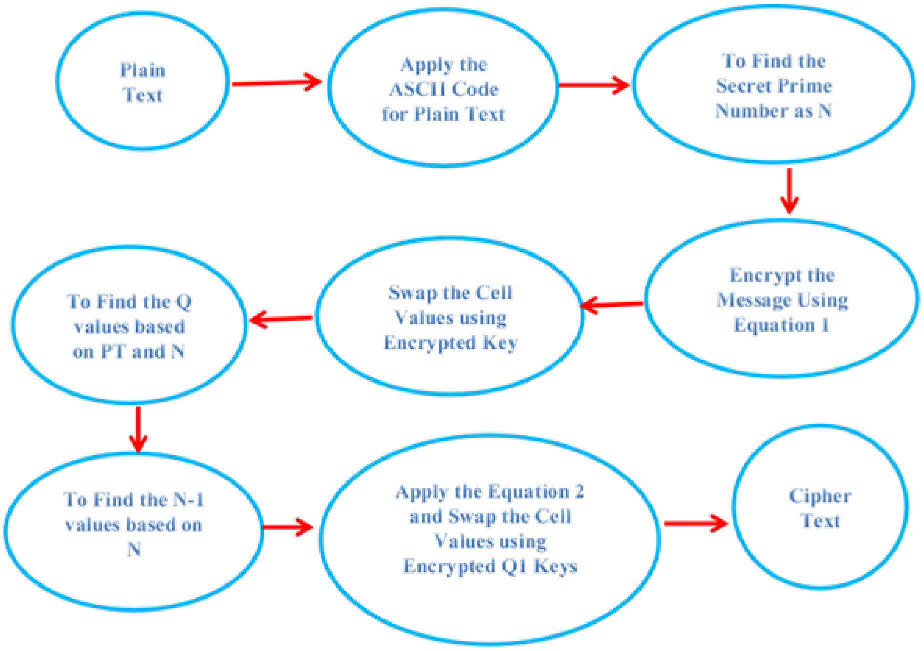
Plain Text
Apply the ASCII Code for Plain Text
To Find the Secret Prime Number as N
Encrypt the Message Using Equation 1
Swap the Cell Values using Encrypted Key
To Find the Q values based on PT and N
To Find the N-1 values based on N
Apply the Equation 2 and Swap the Cell Values using Encrypted Q1 Keys
Cipher Text

Fig. 2. PrimeDigitBR Methodology

Algorithm

- Get the social media data that has been studied and put it in a grid style.

  $P1 = P^{N}$
  where P is ASCII code for plain text (1)
  N is secret prime number

- To find the Q value from N and P.
- $Q2 = Q^{N-1}$ (2)
- To use P1 and Q2 numbers to make a pair and switch the cells.

4. Result

Working for Encryption

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{13} & PD_{14} & PD_{15} \\ PD_{21} & PD_{22} & PD_{23} & PD_{24} & PD_{25} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{42} & PD_{43} & PD_{44} & PD_{45} \\ PD_{51} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

Where PD is Plain Text

Stage 1:

P=SMARTSMART
P=83776582848377658284
N=7
P1=2.8964E+139
P1=2.8964639

- Using equation 1, (2,8), (9,6), (4,6), and (3,9)

1st Process (2,8)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{14} & PD_{15} \\ PD_{21} & PD_{22} & PD_{23} & PD_{13} & PD_{25} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{42} & PD_{43} & PD_{44} & PD_{45} \\ PD_{51} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

2nd Process (9,6)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{14} & PD_{15} \\ PD_{21} & PD_{25} & PD_{23} & PD_{13} & PD_{22} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{42} & PD_{43} & PD_{44} & PD_{45} \\ PD_{51} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

3rd Process (4,6)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{14} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{22} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{42} & PD_{43} & PD_{44} & PD_{45} \\ PD_{51} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

4th Process (3,9)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{22} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{14} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{42} & PD_{43} & PD_{44} & PD_{45} \\ PD_{51} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

Stage 2:

Q=-13

N-1=6

Q1=4826809

- Using equation 2, (4,8), (2,6), (8,0), and (9,0)

5th Process (4,8)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{22} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{14} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{51} & PD_{43} & PD_{44} & PD_{45} \\ PD_{42} & PD_{52} & PD_{53} & PD_{54} & PD_{55} \end{bmatrix}$$

6th Process (2,6)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{22} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{14} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{51} & PD_{43} & PD_{53} & PD_{45} \\ PD_{42} & PD_{52} & PD_{44} & PD_{54} & PD_{55} \end{bmatrix}$$

7th Process (8,0)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{22} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{14} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{41} & PD_{55} & PD_{43} & PD_{53} & PD_{45} \\ PD_{42} & PD_{52} & PD_{44} & PD_{54} & PD_{51} \end{bmatrix}$$

8th Process (9,0)

$$PD = \begin{bmatrix} PD_{11} & PD_{12} & PD_{24} & PD_{22} & PD_{25} \\ PD_{21} & PD_{15} & PD_{23} & PD_{13} & PD_{14} \\ PD_{31} & PD_{32} & PD_{33} & PD_{34} & PD_{35} \\ PD_{51} & PD_{55} & PD_{43} & PD_{53} & PD_{45} \\ PD_{42} & PD_{52} & PD_{44} & PD_{54} & PD_{41} \end{bmatrix}$$

Table 1 provides a comparison of the three distinct encryption speeds that may be accessed by clicking on this link. It has been observed that the technique known as PrimeDigitBR, which is unique due to the important features it has, exhibits faster speed performance than the other methods that are now in use. The technology that goes by the name PrimeDigitBR has been shown to have performance rates of 1.44, 1.82, 2.21, 2.78, 3.12, 3.88, and 4.11 milliseconds, according to research that has been conducted. In addition to this, it has shown the performance when compared to its competitors, which include the “Shor’s” approach in Figure 3, as well as the “RB22” method in Figure 4. A depicts an approach that is original in Figure 5.

Table 1. PrimeDigitBR performance for encryption

File Size (Bytes)	Shor's	RB22	PrimeDigitBR
46	1.05	0.95	1.44
98	1.35	1.15	1.82
159	1.95	1.64	2.21
256	2.33	2.02	2.78
698	2.76	2.41	3.12
1231	3.03	2.95	3.88
6580	3.66	3.22	4.11

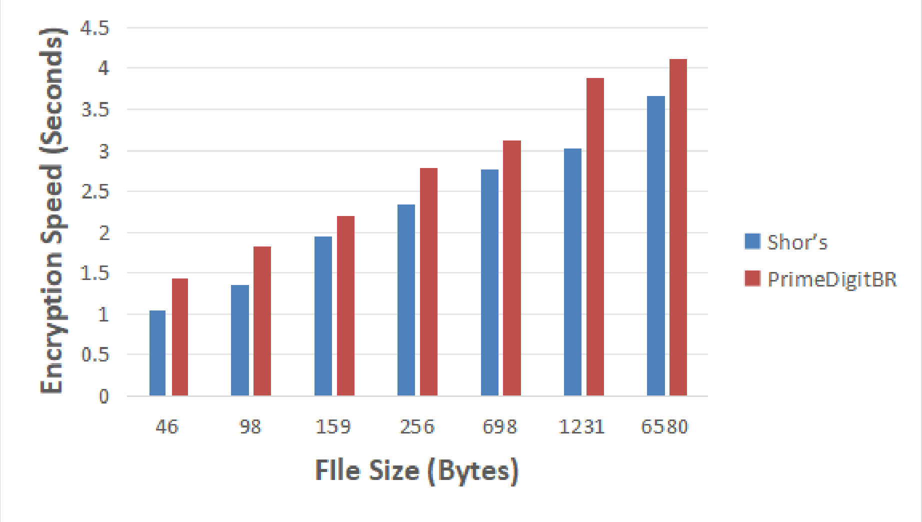

Fig. 3. Shor's Vs PrimeDigitBR Speed for Encryption

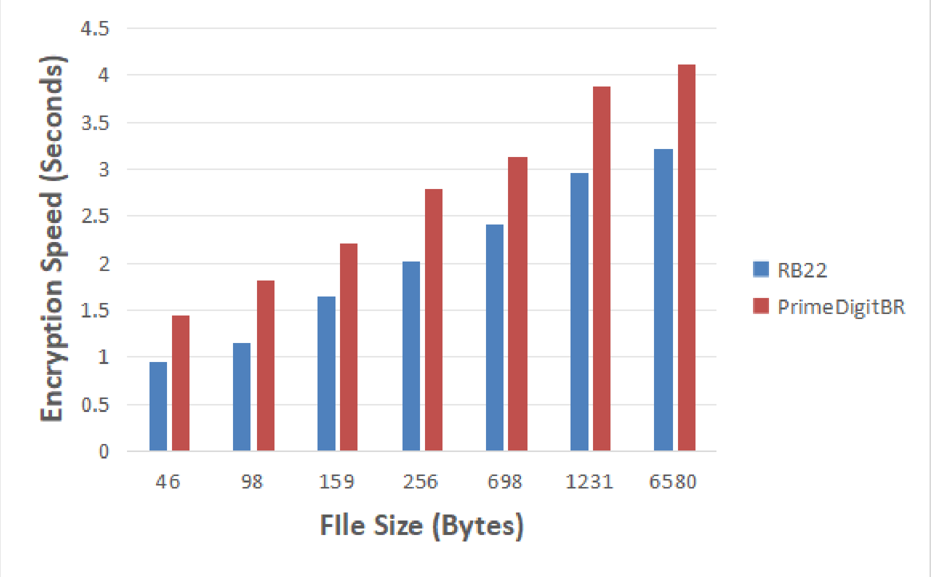

Fig. 4. RB22 Vs PrimeDigitBR Speed for Encryption

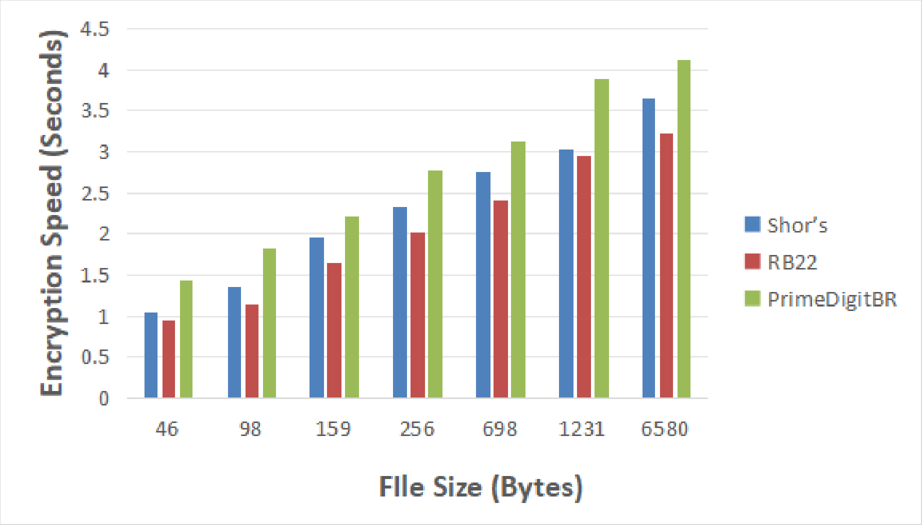

Fig. 5. Shor's Vs RB22 Vs PrimeDigitBR Speed for Encryption

5. Conclusion

A broad range of network devices will be able to "communicate with one another" without regard to the local networks to which they are linked or the quantity of resources. One of the most pressing issues that need to be solved as the Internet of Things continues to expand is how to safeguard the privacy, communication, and security of end users. Ensuring that secure connection is maintained across a broad range of applications is of the highest "significance when there are limited resources" available for communication devices. In order for the Internet of Things to come into reality. As a result of this, the Internet of Things has been beset by a plethora of serious vulnerabilities that may compromise trust and security. The distinctive approach that goes by the name of SPrimeBR has been suggested as a potential solution to these issues among the several other viable approaches. There are 2 steps to the new method. First stage has 3 steps. First, change the text from plain text to "ASCII code" as P. The 2nd is to use the "ASCII code" of N to find the prime number. the third step, you need to use Equation 1. Take the numbers from P1 and pair them up. Then, change the cells in the matrix. Second stage has 2 steps. The 1st is to figure out what Q is worth. The 2nd is to find the numbers for N-1. The last step is to use and apply Equation 2. From the Q1 values, make a pair and swap the cell values in the matrix. However, the values in the 0th cell start from the backwards. The act of reversing this conversion, which is referred to as decryption, ultimately leads in the retrieval of the message in its original format. It is the culmination of this procedure that allows the message to be acquired. In compared to other approaches to encryption that are more conventional, the method that has been offered offers a greater level of security.

References

[1] K. Oonishi and N. Kunihiro, "Shor's Algorithm Using Efficient Approximate Quantum Fourier Transform", in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-16, 2023, Art no. 3102016, doi: 10.1109/TQE.2023.3319044.

[2] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700.

[3] Batcha, B.B.C., Singaravelu, R., Ramachandran, M. et al., "A Novel Security Algorithm RPBB31 for Securing the Social Media Analyzed Data using Machine Learning Algorithms", Wireless Pers. Commun., pp. 581–608, 2023.

[4] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, "The number field sieve", in Proc. 22nd Annu. ACM Symp. Theory Comput., 1990, pp. 564–572. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/100216.100295

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.

[6] Basha, C. B. ., Rajaprakash, S. ., Aggarwal, N. ., Riyazuddin, M. ., Sirajuddin, M. ., & Gole, S. B. . (2023). An Innovative Cryptography Safety Algorithm Called S-RSB-23 for Protecting Data Using Machine Learning Algorithm. International Journal of Intelligent Systems and Applications in Engineering, 12(2s), pp. 503–510, 2024.

[7] N. Koblitz, "Elliptic curve cryptosystems," Math. Computation, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.2307/2007884

[8] V. S. Miller, Use of Elliptic Curves in Cryptography. Berlin, Germany: Springer, 1986, doi: 10.1007/3-540-39799-X_31.

[9] A. S. D. Alluhaidan and P. Prabu, "End-to-End Encryption in Resource-Constrained IoT Device", in IEEE Access, vol. 11, pp. 70040-

70051, 2023, doi: 10.1109/ACCESS.2023.3292829.

[10] C. Bagath Basha, S. Rajaprakash, Nitisha Aggarwal, MD Riyazuddin, G. Sujatha, K. Karthik, "The Design of Security Algorithm RPBB-24-1 in Multi-Way Path over the Distributed Ledger," SSRG International Journal of Electrical and Electronics Engineering, vol. 11, no. 4, pp. 36-44, 2024. https://doi.org/10.14445/23488379/IJEEE-V11I4P105.

[11] M. A. Khan, M. T. Quasim, N. S. Alghamdi and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-Based Medical Sensor Data," in IEEE Access, vol. 8, pp. 52018-52027, 2020, doi: 10.1109/ACCESS.2020.2980739.

[12] Bagath Basha, C., & Somasundaram, K. (2019). A comparative study of twitter sentiment analysis using machine learning algorithms in big data. International Journal of Recent Technology and Engineering, 8, 591–599.

[13] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, “Machine Learning for Cloud Security: A Systematic Review”, in IEEE Access, vol. 9, pp. 20717-20735, 2021, doi: 10.1109/ACCESS.2021.3054129.

[14] Bagath Basha, C., & Rajaprakash, S. (2020). Applying the CBB21 phase 2 method for securing twitter analyzed data. Advances in Mathematics: Scientifc Journal, 9, 1085–1091.

[15] M. Shabbir et al., “Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing”, in IEEE Access, vol. 9, pp. 8820-8834, 2021, doi: 10.1109/ACCESS.2021.3049564.