MSRDG International Journal of Computer Scientific Technology & Electronics Engineering ISSN: 3107 - 426X
Volume 1 Issue 6, 1-7, December 2025

KRB22 Based Security Method for Generalized Data Security

Govind Manu[1], Tony Giji[2], K. Muhammed Fasil[3]

[1,2,3]*Department of CSE, Aarupadai Veedu Institute of Technology, Vinayaka Missions Research Foundation, Chennai, Tamil Nadu, India.*
[1]*govindmanum10@gmail.com*

Abstract - *The new world is information world in citizen life; since information just chose live or not on the planet. Information is more accessible in government, clinic, online entertainment and so on.. For this information have smidgen security, so programmers can hack the information without any problem. For this issue, we presenting the new technique is KRB22 and it has two phases. The first stage is applying for T-test strategy and 0th network esteem start from end then, at that point, trade values; and the second stage is secret key and that key applying in n(n+1)/2 activities. The KRB22 strategy give high security while contrasted with ChaCha technique*

Keywords - *KRB-22, Encryption, Prime, T-test, ChaCha*

1. Introduction

Nowadays public health data was increased day by day in the current global world. To investigate the general clinical issues data by using artificial intelligence computation. The classification support process is Yes or No and unpredictable area process is "Mean Square Error". The generated data are not secured properly and can easily get hacked by the hackers. To overcome from this data security issue, we have planned to apply KRB(KarthikRajaBagath) 22. They execution showed and very basic and grasped estimation is structure computation [1]. The CBB21 computation is appeared differently in relation to the Salsa20/4 estimation and primarily took a time of gander [2]. They examined data with simulated intelligence computations and moreover analyzed data applied to the CBB20 estimation [3]. They focused on the explored twitter data with applied the "SRB21" security [4]. They analyzed first "Twitter data", then examined guessed that data by computer based intelligence estimation, and applied the security of "SRB18" [5]. The "RBJ25"is computationdata is differentiated the "AES and ChaCha" [6]. They focused on the "AES and Salsa encryption"is computation with"RB20" [7]. The "CBB22" estimation is shows the security of summarized data [8]. They focused on the time of speed for "Salsa" and security of "SRB21" [9]. The primarily examination the analysis of films through assessment by portrayal and SVM computations [10]. They separated the huge data and put away that data with the protection cycle is "RBJ20" computation [11].They proposed 7 phases for giving the security of the information [12].

2. Methodology

The proposed KRB22 technique has 6 stages. 1. To get the key of S prime. 2. To get the both values X1 and X2, then a and b also. 3. To transfer the values for a and b but assign the value of 0th position from end and again do swap from first. 4. To use the formula n(n+1)/2 in Figure 1.

- To get the input values and apply to that values in Eq(1), Eq(2) and Eq(3).
- T-Test Equation = $(\bar{Z}1-\bar{Z}2)/\sqrt{((Z_1^{\,2}/N_1)+(Z_2^{\,2}/N_2))}$ (1)
- $\bar{Z}1=\Sigma Z_1/N_1 \quad \bar{Z}2=\Sigma Z_2/N_2$ (2)
- $S_1=\sqrt{\Sigma(Z_1-\bar{Z}1)^2/(N_1-1)} \qquad S_2=\sqrt{\Sigma(Z_2-\bar{Z}2)^2/(N_2-1)}$ (3)
- To coordinate the T-test esteem from left..
- To make secret key as n and apply the way to n(n+1)/2

3. Result

The text of your paper should be formatted as follows:

- Matrix Input (IP).

$$IP=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 316/5 & 317/5 & 318/5 & 319/5 & 320/5 \\ 321/5 & 322/5 & 323/5 & 324/5 & 325/5 \end{bmatrix}$$

Using Equation (1) the values are (1,1) (5,1) (0,9) (0,6)

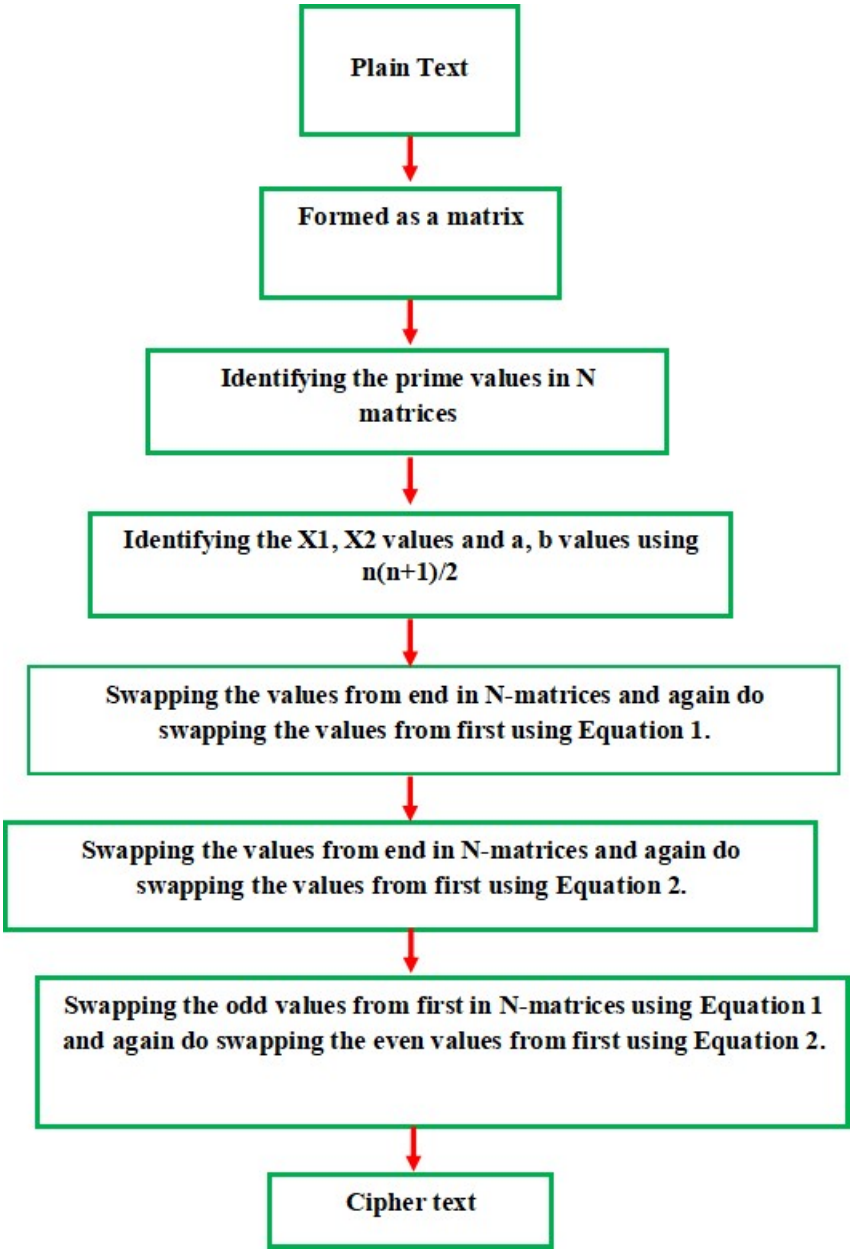

Fig. 1 KRB22 Methodology

1: (1,1)

$$TTE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 316/5 & 317/5 & 318/5 & 319/5 & 320/5 \\ 321/5 & 322/5 & 323/5 & 324/5 & 325/5 \end{bmatrix}$$

2: (5,1)

$$TTE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 316/5 & 317/5 & 318/5 & 319/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 325/5 \end{bmatrix}$$

3: (0,9)

$$TTE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 319/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 316/5 \end{bmatrix}$$

4: (0,6)

$$TTE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

5: (1,1)

$$TTE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

6: (5,1)

$$TTE=\begin{bmatrix} 301/5 & 306/5 & 303/5 & 304/5 & 305/5 \\ 302/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

7: (0,9)

$$TTE=\begin{bmatrix} 310/5 & 306/5 & 303/5 & 304/5 & 305/5 \\ 302/5 & 307/5 & 308/5 & 309/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

8: (0,6)

$$TTE=\begin{bmatrix} 307/5 & 306/5 & 303/5 & 304/5 & 305/5 \\ 302/5 & 310/5 & 308/5 & 309/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

- **Using Equation (2)& (3) the values are** (4,2), (8,1), (3,6), (3,1)

9: (4,2)

$$TSE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 323/5 & 322/5 & 321/5 & 320/5 & 319/5 \end{bmatrix}$$

Where TSE is T-test Secret Encryption

10: (8,1)

$$TSE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 320/5 & 318/5 & 316/5 & 324/5 \\ 323/5 & 322/5 & 321/5 & 317/5 & 319/5 \end{bmatrix}$$

11: (3,6)

$$TSE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 320/5 & 318/5 & 322/5 & 324/5 \\ 323/5 & 316/5 & 321/5 & 317/5 & 319/5 \end{bmatrix}$$

12: (3,1)

$$TSE=\begin{bmatrix} 301/5 & 302/5 & 303/5 & 304/5 & 305/5 \\ 306/5 & 307/5 & 308/5 & 309/5 & 310/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 320/5 & 318/5 & 322/5 & 324/5 \\ 323/5 & 317/5 & 321/5 & 316/5 & 319/5 \end{bmatrix}$$

13: (4,2)

$$TSE=\begin{bmatrix} 307/5 & 305/5 & 303/5 & 304/5 & 306/5 \\ 302/5 & 310/5 & 308/5 & 309/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

14: (8,1)

$$TSE=\begin{bmatrix} 307/5 & 309/5 & 303/5 & 304/5 & 306/5 \\ 302/5 & 310/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

15: (3,6)

$$TSE=\begin{bmatrix} 307/5 & 309/5 & 303/5 & 310/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

16: (3,1)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

17: (1,1)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

18: (0,9)

$$TSE=\begin{bmatrix} 301/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 307/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

19: (8,1)

$$TSE=\begin{bmatrix} 301/5 & 305/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 310/5 & 307/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

20: (3,1)

$$TSE=\begin{bmatrix} 309/5 & 305/5 & 303/5 & 301/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 310/5 & 307/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

21: (1,1)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 325/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 319/5 \end{bmatrix}$$

22: (0,9)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 319/5 & 317/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 320/5 & 325/5 \end{bmatrix}$$

23: (8,1)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 319/5 & 320/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 322/5 & 323/5 & 317/5 & 325/5 \end{bmatrix}$$

24: (3,1)

$$TSE=\begin{bmatrix} 307/5 & 310/5 & 303/5 & 309/5 & 306/5 \\ 302/5 & 304/5 & 308/5 & 305/5 & 301/5 \\ 311/5 & 312/5 & 313/5 & 314/5 & 315/5 \\ 319/5 & 320/5 & 318/5 & 316/5 & 324/5 \\ 321/5 & 317/5 & 323/5 & 322/5 & 325/5 \end{bmatrix}$$

The proposed algorithm KBR-22 compares the performance with "ChaCha". The existing method is to do the process for move "all diagonal values" into the first column. The file size are (24, 76, 312, 812, 1531, 6580) bytes => (6x6, 10x10, 15x15, 20x20, 40x40) matrix as shown in the Table 1.

Table 1. Combination of 2 matrices

File Size	ChaCha	KRB22
Two-Four	01.6	1.8
Seven-Six	01.2	1.9
Three-One-Two	02.7	2.8
Eight-Two-Two	02.6	2.9
One-Five-Three-One	03.4	3.5

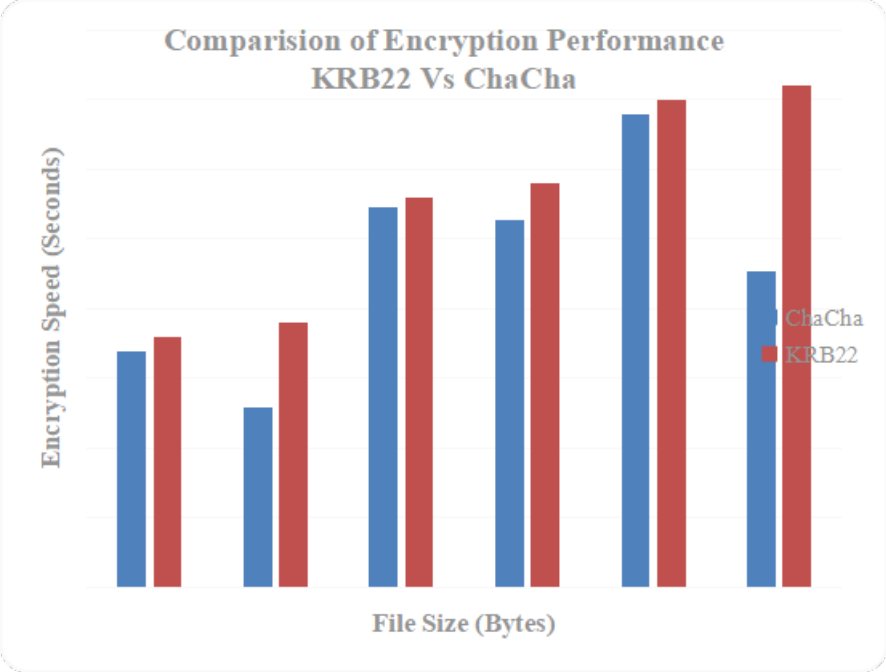

Fig. 2 Encryption performance

The KBR-22 method has compared the performance of encryption 1.8 (s), 1.9 (s), 2.8 (s), 2.9 (s), 3.5 (s) and 3.6 (s) for the KBR-22. The KBR-22 provide "more protection" of the data; when compared to existing method in Figure 2.

4. Conclusion

Nowadays public health data was increased day by day in the current global world. To investigate the general clinical issues data by using artificial intelligence computation. For this information have low level security, so programmers can hack the information without any problem. For this issue, we presenting the new technique is KRB22 and it has two phases. The first stage is applying for T-test strategy and the second stage is applying the secret key. The KRB22 strategy give high security while compared with ChaCha technique.

References

[1] C. Bagath Basha, and K. Somasundaram K 2019 A Comparative Study of Twitter Sentiment Analysis Using Machine Learning Algorithms in Big Data (International Journal of Recent Technology and Engineering) p 591-599

[2] C. Bagath Basha, and S. Rajaprakash 2020 Applying The CBB21 Phase 2 Method For Securing Twitter Analyzed Data (Advances in Mathematics: Scientific Journal) p 1085-1091

[3] C. Bagath Basha, S. Rajaprakash, S. Muthuselvan, P. Saisatishsunder, and SVL Alekhya Rani, 2020 Applying the CBB20 Algorithm for Twitter Analyzed Data (In: Proc. of First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India)

[4] C. Bagath Basha, and S. Rajaprakash 2020 Applying the SRB21 Phase II Methodology for Securing Twitter Analyzed Data (In: Proc. of the International Confererence on Mechanical Electronics and Computer Engineering).

[5] C. Bagath Basha, and S. Rajapraksh 2020 Enhancing The Security Using SRB18 Method of Embedding Computing (Microprocessor and Microsystems)

[6] S. Rajaprakash, C. Bagath Basha, S. Muthuselvan, N. Jaisankar, and Ravi Pratap Singh 2020 RBJ25 Cryptography Algorithm For Securing Big Data (In: Proc. of First International Conference on Advances in Physical Sciences and Materials, Coimbatore, Tamil Nadu, India).

[7] K. Karthik, C. Bagath Basha, U. Bhaswanth Thilak, T. Sai Kiran, and J. Raj 2020 Securing Social Media Analyzed Data Using RB20 Method (Advances in Mathematics: Scientific Journal) v 3

[8] C.Bagath Basha, S. Rajaprakash, V.V.A. Harish, M.S. Krishna, and K. Prabhas 2020 Securing Twitter Analysed Data Using CBB22 Algorithm (Advances in Mathematics: Scientific Journal) p 1093-1100

[9] C. Bagath Basha, and S. Rajaprakash 2019 Securing Twitter Data Using SRB21 Phase I Methodology (International Journal of Scientific & Technology Research) p 1952-1955

[10] R. Jaichandran, C. Bagath Basha, K. L. Shunmuganathan, S. Rajaprakash, and S. Kanagasuba Raja 2019 Sentiment Analysis of Movies on Social Media using R Studio (International Journal of Engineering and Advanced Technology) v 8

[11] S. Rajaprakash, N Jaisankar, C.Bagath Basha, A. Jayan, G. Sebastian 2022 RBJ20 Cryptography Algorithm for Securing Big Data Communication using Wireless Networks (WorldS4, Springer, LNNS Book Series (ISSN: 237 – 3370, London, July 29-30, 2021)) v 334, p 499-507

[12] C. Bagath Basha, S. Rajaprakash, R. Meenakumari, M. Suresh, P. Hitesh, T. Kokilavani, and R. Ashok Kumar A novel security algorithm RPBB31 for securing the social media analyzed data using machine learning algorithms (Wireless Personal Communications) https://doi.org/10.21203/rs.3.rs-1860348/v1