A Novel Cycle Leader Permutation with Elgamal Algorithm for Image Encryption

Boggana. Vandana, Kanusu. Srinivasa Rao, Buduri. Reddaiah, Bodi. Susheel Kumar

***Abstract:** As more people use networks in whatever capacity, security-related issues come up more frequently. These issues could be external to the network or inside to it. To address the security-related issues The science of cryptography and network security makes it possible to protect the resources, data quality, and network infrastructure. Firewalls and filters are utilized across many workstations to safeguard the resources. However, security services are required to safeguard the data during transmission to prevent unauthorized access. To guard against attacks, these services must be changed often. This paper integrates Cycle Leader permutation with Elgamal algorithms to construct such a system. These hybrid solutions can be used to stop hackers from gaining unauthorized access different commercial applications.*

***Keywords**: Encryption, Decryption, Key, Cycle Leader Permutation, Elgamal.*

I. INTRODUCTION

Electronic commerce is becoming the norm for most corporate organizations, and they are pushing users in that direction. The widespread usage of networks and the internet has made this possible. Currently, the most important thing for industry is to securely communicate via secure communication channels to transmit confidential information about individuals engaged in commercial activities. It is necessary for the hackers to transfer sensitive data in an unexplainable way [4]. To accomplish this kind of safe communication One technique and field of study that contributes to security is cryptography. The security services in the secured communication channel are provided by this sequence of events and activities. In places where data is sent across networks, security services are required. Unauthorized users attempt to have control over moving data. Confidentiality, authenticity, and data integrity may be compromised if control is obtained on data. A suitable protection method must be employed to transfer the data securely in order to guard against such security breaches.

The study of cryptography is concerned with protecting data during transmission from unauthorized access. This science uses mathematical ideas to both encode and decode the data. The strength of each newly constructed system depends on the encryption that is created during encoding [5]. This science aids in the investigation and creation of novel cryptosystems that might help to prevent the actions of unauthorized users. Elgamal algorithms and Cycle Leader permutation are used in this study to develop a novel hybrid system. These techniques aid in the creation of complex cryptosystems. These kinds of systems are particularly challenging to understand and need more effort to break.

A. Types of Attacks in Network

A threat is something that has the potential to harm the user's data. A threat can be an object or an unit or a program that characterizes to be scheme of risk. Due to the widespread usage of the internet these days, a sizable number of people are linked, and their data is kept on internet servers. Likewise, social, personal, and professional activities rely on the internet. These factors make it possible for unauthorized users to destroy resources and affect the availability of internet services. Network security becomes essential considering all the anomalies, assaults, and threats. Attacks are classified as either passive or active because they provide the greatest harm to the interconnected systems. In terms of passive attack, it simply involves data flow analysis, traffic analysis, eavesdropping, and monitoring [6]. Active attacks include stopping data while moving, as it travels from one place to another, as well as altering, fabricating, and stopping data [7].

II. BACKGROUNG STUDY

Moatsum Alawida proposes a novel picture encryption technique with minimal processing time that is based on an improved chaotic map. They introduced a unique hybridized forward-backward perturbation map, based on a novel perturbed logistic chaotic map.

Compared to other chaotic systems already in use, it has superior chaotic qualities such a wide chaotic range, increased sensitivity, and unpredictability. Based on this, a novel image encryption method is described that uses two substitution operations and a special permutation operation to achieve superior encryption speed and efficiency. They used a chaotic data sequence as its basis, the unique permutation operation generates 8-bit values by using all chaotic states. The last 8-bit number's indexes are combined into a single block [1].

Sandip Kumar Bhowmick et al., suggested a modified version of ElGamal encryption that offers high information rate digital signatures and data secrecy.

Manuscript received on 30 March 2024 | Revised Manuscript received on 05 April 2024 | Manuscript Accepted on 15 April 2024 | Manuscript published on 30 April 2024.
**Correspondence Author(s)*

Boggana Vadana, Department of Computer Science and Technology, Yogi Vemana University, Kadapa-516005, India. Email: bbogganavandana@gmail.com, ORCID ID: 0009-0006-5090-2792

Kanusu. Srinivasa Rao, Associate Professor, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: kanususrinivas@gmail.com

Buduri. Reddaiah*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: prof.reddaiah@yvu.edu.in, ORCID ID: 0000-0002-5851-2194

Bodi. Susheel Kumar, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: bjayakarunya@gmail.com

ElGamal's security is solely dependent on how hard it is to factor discrete logarithmic issues, where it is highly challenging to determine discrete logarithms over finite fields using statistical or brute force assaults. This suggested technique improves the algorithm by adding an additional key and an arbitrary number to the standard one, increasing the deciphering difficulty and decreasing the time complexity to decode the message, in response to the ongoing challenges to the security of the ElGamal scheme [2].

Alejandro Freyre Echevarrıa provided a graph description of S-boxes along with optimization techniques to generate full cycle per mutations that are cryptographically secure [3].

Rajesh P. Singh presented a permutation polynomial-based multivariate encryption technique that is effective across finite fields. The authors developed a trapdoor function for the cryptosystem by using polynomials in L(2,m), where $m = 2k$ for any $k > 0$ [8].

To increase security, Rahmadi Asri et al., suggested using the split merge approach with the El-Gamal algorithm. The paper explains the design and analysis of the system. Large prime number computations are used in the combination, which makes it more difficult for cryptanalysts to decipher the plaintext [9].

Akash Thakkar, Ravi Gor presented a technique for cryptography that uses the Kamal Transform and ElGamal algorithm to increase communication security. Further security for information communication cannot be achieved by encryption and decryption systems based on Kamal Transform applications. The discrete logarithm issue is the foundation of the public key ElGamal algorithm [10][19][20][21][22].

III. PROPOSED SCHEME

This proposed system is mainly based on cycle leader permutation that permutates the values generated from the input image. Along with cycle permutation Elgamal algorithm is used in encryption and decryption.

A. Cyclic Permutation

In group theory in particular, a cyclic permutation is a permutation consisting of a single cycle [11,12][23]. Cyclic permutations are sometimes called cycles [13]. A cyclic permutation may be referred to as a k-cycle if it has k elements. More than just one non-trivial cycle, a few authors expanded this idea to include permutations with fixed points [13, 14]. Cycles are also the separate cyclic components of a permutation. Cyclic permutations are represented in cycle notation by a list of their elements, permuted in the order indicated by the parenthesis around the elements. A cyclic permutation's orbit is the collection of items that it does not fix. It is possible to break down every permutation on a limited number of components into cyclic permutations on disjoint orbits.

B. Elgamal Algorithm

ElGamal's security is solely dependent on how hard it is to factor discrete logarithmic issues, where it is exceedingly challenging to use statistical or brute force assaults to determine discrete logarithms over finite fields. ElGamal, developed by Taher Elgamal in 1985 as a successful Diffie-Hellman algorithm implementation, rose to prominence as the most well-known public key cryptography algorithm after the Diffie-Hellman key exchange algorithm. Diffie and Hellman initially proposed the idea of asymmetric key cryptography, sometimes known as public key cryptography, in 1976.[15]. It is a modified version of the Diffie-Hellman algorithm that offers a digital signature for message authentication in addition to allowing the exchange of messages rather than simply keys [16][17].

Among the widely used encryption algorithms is El-Gamal. Generally, communications are encrypted using the El-Gamal algorithm. A straightforward and effective cryptographic technique is part of the El-Gamal algorithm [18]. Since this technique can do many factorings, calculating key creation using random values is relatively secure. El-Gamal is thereby able to withstand cryptanalyst assaults while maintaining communication security.

IV. PROPOSED SYSTEM

A. Framework of Key Generation

In this framework key for encryption and decryption process is generated using primitive roots as shown in figure 1.

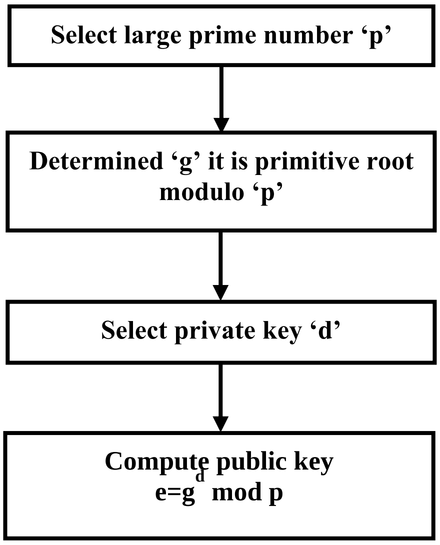
Select large prime number ‘p’
Determined ‘g’ it is primitive root modulo ‘p’
Select private key ‘d’
Compute public key
e=g^d mod p

Fig. 1. Block Diagram of Key Generation Process

B. Key Generation Algorithm

The proposed algorithm-1 illustrates step by step procedure for key generation by using primitive roots as shown in figure 1.

Proposed Key Generation Algorithm-1

```
Step 1. Select very large prime number denoted by p
Step 2. Determine ‘g’ and it is primitive root of modulo
        ‘p’
Step 3. Select private Key denoted by ‘d’
Step 4. Compute public key denoted by ‘e’
            $e = g^d \bmod p$
```

C. Framework of Encryption Process

The proposed framework illustrates step by step procedure of encryption that involves converting original images into encrypted image a shown in figure 2.

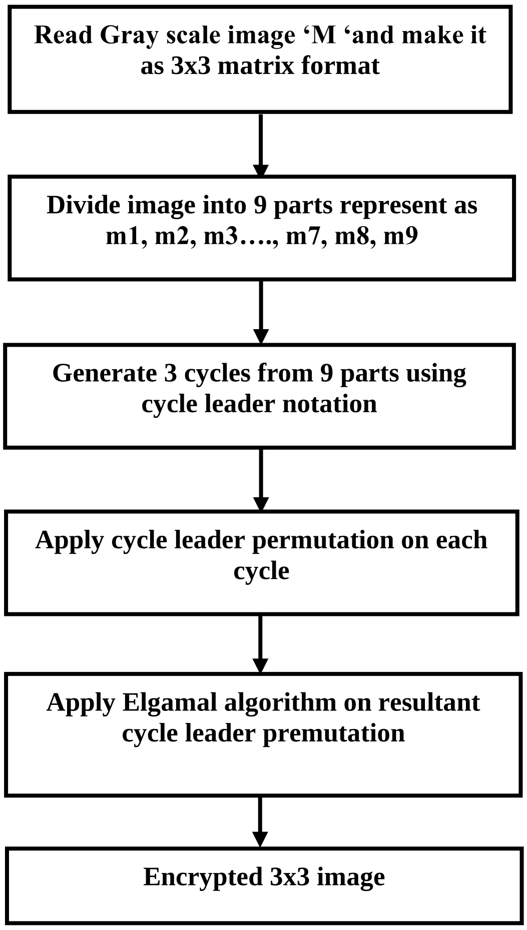
Read Gray scale image 'M 'and make it as 3x3 matrix format
Divide image into 9 parts represent as m1, m2, m3…., m7, m8, m9
Generate 3 cycles from 9 parts using cycle leader notation
Apply cycle leader permutation on each cycle
Apply Elgamal algorithm on resultant cycle leader premutation
Encrypted 3x3 image

Fig. 2. Block Diagram of Encryption Process

D. Encryption Algorithm

The proposed algorithm-2 illustrates step by step procedure of encryption that involves converting original images into encrypted image a shown in figure 2.

Proposed Encryption Algorithm-2

```
Step 1. Read gray scale image
Step 2. Convert gray scale image into 3x3 matrix format
          ('M'), with 9 parts.
Step 3. Among 9 parts, 3 cycles are generated using
          cycle leader notation.
           Cycle 1 – (1 3 5)
           Cycle 2 – (2 4 6 9)
           Cycle 3 – (7 8)
Step 4. Apply cycle leader permutation on each cycle
Step 5. Apply Elgamal technique on newly generated
            3x3 matrix.
Step 6. Resultant is the Encrypted image
```

E. Framework of Decryption Process

The proposed framework illustrates step by step procedure of decryption that involves converting encrypted images into original image a shown in figure 3.

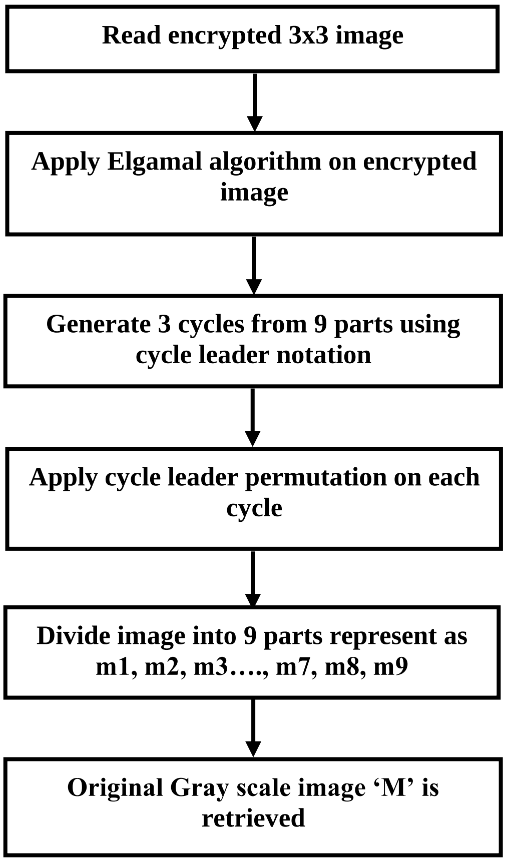
Read encrypted 3x3 image
Apply Elgamal algorithm on encrypted image
Generate 3 cycles from 9 parts using cycle leader notation
Apply cycle leader permutation on each cycle
Divide image into 9 parts represent as m1, m2, m3…., m7, m8, m9
Original Gray scale image 'M' is retrieved

Fig. 3. Block Diagram of Decryption Process

F. Decryption Algorithm

The proposed algorithm-3 illustrates step by step procedure for decryption that involves converting encrypted images into original image a shown in figure 3.

Proposed Decryption Algorithm-3

```
Step 1. Read encrypted image represented as 3x3 matrix
Step 2. Apply Elgamal algorithm on encrypted image
Step 3. Among 9 parts, 3 cycles are generated using
          cycle leader notation.
           Cycle 1 – (8 7)
           Cycle 2 – (2 9 6 4)
           Cycle 3 – (1 5 3)
Step 4. Apply cycle leader permutation on each cycle

Step 5. Generate 3x3 matrices with 9 parts represented as
          m1, m2, m3, m7, m8, m9.
Step 6. Resultant is the original Gray scale image
```

V. RESULT AND DISCUSSION

The key generation algorithm uses prime number and its primitive root. With this key for encryption and decryption is derived is shown in Table I.

Table- I: Outcome of Key Generation Process

Choose Random Prime Number 'p'	Primitive Root Modulo 'p'	Choose Random Private Key 'd'	Compute Public Key 'e' using Primitive Root 'g', Prime Number 'p' and Primitive Key 'd' $e = g^{d} \bmod p$
P=23	g=5	D=6	E=8

The original image's encryption technique, which utilized the ASCII of it is considered in 3x3 matrix is shown in Table I to get encrypted image.

Table-II: Outcome of Encryption Process

3x3 Matrix Pixel Values for Original Gray Scale Image	Cycle Permutation On original Gray Scale Image	Elgamal Algorithm on Cyclic Leader Permutation	Encrypted Gray Scale Image Pixel Values
$\begin{bmatrix} 100 & 150 & 200 \\ 50 & 75 & 125 \\ 25 & 175 & 225 \end{bmatrix}$	$\begin{bmatrix} 100 & 150 & 75 \\ 125 & 200 & 225 \\ 175 & 25 & 50 \end{bmatrix}$	$\begin{bmatrix} 4,200 & 4,300 & 4,150 \\ 4,250 & 4,400 & 4,450 \\ 4,350 & 4,50 & 4,100 \end{bmatrix}$	$\begin{bmatrix} 4,200 & 4,300 & 4,150 \\ 4,250 & 4,400 & 4,450 \\ 4,350 & 4,50 & 4,100 \end{bmatrix}$

The decryption algorithm used on the encrypted image where it is considered in 3x3 matrix as shown in Table II to get original image.

Table- III: Outcome of Decryption process

Encrypted Gray Scale Image Pixel Values	Inverse Elgamal Algorithm on Cyclic Leader Permutation	Inverse Cycle Permutation On Original Gray Scale Image	3x3 Matrix Pixel Values for Original Gray Scale Image
$\begin{bmatrix} 4,200 & 4,300 & 4,150 \\ 4,250 & 4,400 & 4,450 \\ 4,350 & 4,50 & 4,100 \end{bmatrix}$	$\begin{bmatrix} 100 & 150 & 75 \\ 125 & 200 & 225 \\ 175 & 25 & 50 \end{bmatrix}$	$\begin{bmatrix} 100 & 150 & 200 \\ 50 & 75 & 125 \\ 25 & 175 & 225 \end{bmatrix}$	$\begin{bmatrix} 100 & 150 & 200 \\ 50 & 75 & 125 \\ 25 & 175 & 225 \end{bmatrix}$

VI. CONCLUSION

This study suggests an improved security version of the Elgamal cryptosystem-based signature creation and encryption. This paper provided a novel approach to experimental mathematics that blends the Elgamal algorithm, cyclic leader permutation-based computing, and traditional mathematical progress. Since the suggested method outperforms the original ElGamal scheme in terms of information rate, it is anticipated that digital data transmissions would be safe. Due to the discrete logarithm problem and the difficulty of factoring huge numbers to assume the private keys, the security of the modified method completely depends on how difficult it is to obtain the private keys. The strength and efficiency of cyclic permutation-based cryptography systems should be increased as part of further research in the future to make them competitive choices in the quickly evolving fields of data security and secure communications.

DECALARION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Moatsum Alawida, "A novel chaos-based permutation for image encryption", Journal of Kind Saud University-Computer and Information Sciences, 35 (2023) 101595, pp. 1–21. https://doi.org/10.1016/j.jksuci.2023.101595
2. Sandip Kumar Bhowmick et al., "Modified Elgamal Cryptosystem for Public-Key Encryption and Digital Signature", International Journal of Pharmacy & Technology", Dec-2016, Vol. 8, Issue No. 4, pp. 26578-26583.
3. Alejandro Freyre Echevarria et al., "A graph theory approach to heuristic generation of cyclic permutations", Springer Nature 2021, pp. 1-16.
4. A. H. Zahid, E. Al-Solami, and M. Ahamad, A Novel Modular Approach Based Substitution-Box Design for Image Encryption", IEEE Access, vol. 8, pp. 150326-150340. 2020. https://doi.org/10.1109/ACCESS.2020.3016401
5. R. Bhanot, and R. Hans, "A Review and comparative Analysis of Various Encryption Algorithms:, International Journal of Security and Its Applications, vol. 9, No. 4, pp. 289-306, 2015., to be published. https://doi.org/10.14257/ijsia.2015.9.4.27
6. Neha Khandelwal, Prabhakar. M, Kuldeep Sharma, "An Overview of Security Problems in MANET".
7. Stallings. W (2006), Cryptography and Network Security, Fourth Edition, Prentice Hall.
8. Rajesh P. Singh et al., "A Public Key Cryptosystem Using a Group of Permutation Polynomials", Mathematical Institute, Slovak Acadamy of Science, pp. 139-162.
9. Rahmadi Asri et al., " Modification of Ciphertext Elgamal Algorithm using Split Merge", The 3rd International Conference on Computing and Applied Informatics-2018, Journal of Physics: Conference Series, 1235 (2019) 012054, pp. 1-7. https://doi.org/10.1088/1742-6596/1235/1/012054
10. Akash Thakkar, Ravi Gor, "Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal Transform", IOSR Journal of Computer Engineering, vol. 24, Issue. 3, pp. 08-14.
11. Gross, Jonathan L. Combinational methods with computer applications. Discrete mathematics and its applications. Boca Raton, Fla.: Chapman & Hall/CRC. P.29 (2008).
12. Knuth, Donald E. The Art of Computer Programming. Addision-Wesley. P. 35 (2002).
13. Bogart. Kenneth P. Introductory combinatorics (3 ed). London: Harcourt Academic Press. P. 554 (2000).
14. Rosen, Kenneth H. Handbook of discrete and combinational mathematics. Boca Raton, London, New York: CRC press.
15. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126. https://doi.org/10.1145/359340.359342
16. Merkle, Ralph, and Martin Hellman. "Hiding information and signatures in trapdoor knapsacks." IEEE transactions on Information Theory 24.5 (1978): 525-530.4 4 https://doi.org/10.1109/TIT.1978.1055927
17. P. M. Durai Raj Vincent, Sathiyamoorthy E, " A Novel and efficient public key encryption algorithm" International Journal of Information and communication technology, Vol. 9, No. 2, pp 199-211, 2016. https://doi.org/10.1504/IJICT.2016.10000121
18. Z Wu, D Su, G Ding. 2014. ElGamal Algorithm for Encryption of Data Transmission. In Proc. of Int. Conf. on Mechatronics and Control (ICMC)
19. Rao, D., & Koolagudi, S. (2019). Music Cryptography based on Carnatic Music. In International Journal of Engineering and Advanced Technology (Vol. 9, Issue 1, pp. 5107–5114). https://doi.org/10.35940/ijeat.a1358.109119
20. Research on Various Cryptography Techniques. (2019). In International Journal of Recent Technology and Engineering (Vol. 8, Issue 2S3, pp. 395–405). https://doi.org/10.35940/ijrte.b1069.0782s319
21. Abualkas, Y. M. A., & Bhaskari, D. L. (2023). Methodologies for Predicting Cybersecurity Incidents. In Indian Journal of Cryptography and Network Security (Vol. 3, Issue 1, pp. 1–8). https://doi.org/10.54105/ijcns.f3677.053123
22. Narayanasamy, K., & Arumugam, P. (2019). Symmetric Cryptographic Framework for Network Security. In International Journal of Innovative Technology and Exploring Engineering (Vol. 8, Issue 10, pp. 3803–3808). https://doi.org/10.35940/ijitee.j9986.0881019

23. Priya, Dr. R. (2020). The Estimation of Risk on Cloud Computing Framework. In International Journal of Innovative Science and Modern Engineering (Vol. 6, Issue 4, pp. 5–10). https://doi.org/10.35940/ijisme.d1188.016420

AUTHORS PROFILE

Boggana Vandana is studying M.C.A in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. She is passionate in learning new technologies and developing new methods. She has a strong interest in creating new techniques and understanding new technology. She is keen to do security-related research with real-world applications and hopes to expand into a more complete security service provider. She also aspires to be a software developer in the security sector. Her leadership in several projects demonstrates her commitment to resource management and the growth of technological innovations. Sasikala's contributions to this study provide a comprehensive understanding of the scalability challenges facing the security sector.

Kanusu. Srinivasa Rao is working as Associate Professor in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. He has published 40 papers related to Image Processing and Security. His interested research areas are Image Processing and Cryptography and Network Security. Kanusa's commitment to investigating the nexus between security and technology is essential to the creation of reliable solutions. His research highlights the value of using systematic techniques to create models for security and upkeep. He symbolizes the collaborative attitude of this study team as the corresponding author.

Buduri. Reddaiah is working as Associate Professor in the department of Computer Science and Technology, Yogi Vemana University, Kadapa, Andhra Pradesh. His research interests are in security and Artificial Intelligence. With a focus on network security and Artificial Intelligence, his research endeavors to enhance data integrity and access control mechanisms. Reddaiah’s dedication to exploring the intersection of technology and security plays a crucial role in the development of robust systems. His work emphasizes the importance of methodical approaches to develop models in security and maintenance As the corresponding author, he embodies the collaborative spirit of this research team.

Bodi. Susheel Kumar is working as Academic Consultant in the department of Computer Science and Technology, Kadapa, Andhra Pradesh. His research areas is Cryptography and Network Security and published many papers in this area. He is an important contributor to this study because of his knowledge and commitment towards programming with new technologies and promoting a better comprehension of technology's role for this work. He has a strong desire to work as a developer. His dedication to his career is demonstrated by his leadership in a variety of activities. Susheel's contributions to this work provided a thorough understanding of the scalability issues associated with security-related online applicationin.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.