Symmetric Key and Polynomial Based Key Generation Mechanism for Secured Data Communications in 5G Networks

Pradeep Suthanthiramani (pradeep.suthanthiramani@gmail.com)  
Anna University Chennai

Muthurajkumar Sannasy  
Anna University

Sannasi Ganapathy  
VIT University - Chennai Campus

Arputharaj Kannan  
Anna University

Research Article

Keywords: Pascal Triangle, Polynomial, differential calculus, two degree polynomial, three degree polynomial, Symmetric key, security, fuzzy rules, encryption and decryption

DOI: https://doi.org/10.21203/rs.3.rs-565284/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Symmetric Key and Polynomial based Key Generation Mechanism for Secured Data Communications in 5G Networks

S.Pradeep*¹, S.Muthurajkumar², Sannasi Ganapathy³, A.Kannan⁴

¹Dept. of IST, CEG Campus, Anna University, Chennai, Tamilnadu, INDIA
²Dept. of Comp. Tech., MIT Campus, Anna University, Chennai, Tamilnadu, INDIA
³Centre for Cyber Physical Systems & School of Computer Science and Engineering, VIT-Chennai Campus, Chennai, Tamilnadu, INDIA.
⁴Dept. of IST, CEG Campus, Anna University, Chennai, Tamilnadu, INDIA
pradeep.suthanthiramani@gmail.com, muthurajkumarsri@gmail.com, sganapathy@vit.ac.in, akannan123@gmail.com

Abstract – Fifth Generation (5G) networks provide data communications through various latest technologies including Software Defined Network (SDN), Artificial Intelligence, Machine Learning and Cloud Computing. In 5G, secure data communication is a challenging issue due to the presence of enormous volume of users including malicious users communicating with latest technologies and also based their own requirements. In such a scenario, fuzzy rules and cryptographic techniques can play a major role in providing security to the data which are either communicated through the network or stored in network based databases including distributed databases and cloud databases with cloud networks. Therefore, new and efficient mechanisms for generation and exchange of keys are necessary since they are the most important component of cryptographic methods. Since most of the existing key generation techniques are focusing on 3G and 4G networks, new key generation methods that can be generalized to n-th order polynomials are necessary to suit the security requirements of 5G networks which is smart by using rules from Artificial Intelligence. This paper proposes a new key generation and encryption/decryption mechanism which is based on both symmetric key cryptography and polynomial operations for providing effective security on data communication in 5G networks. In this work, we introduce the usage of fuzzy rules and Binomial Theorem (Pascal triangle) technique for performing the data encryption process more efficiently since it is not used in any of the existing cryptographic algorithms. Moreover, two different polynomial equations, one of degree three and another of degree two are used in the proposed work for effective key generation. Here, we have applied differential calculus for finding the second-degree polynomial. In the decryption part of the proposed mechanism, nᵗʰ root operation is applied which is able to reduce the number of steps used in a single mode operation. The experimental results of the proposed work proved that the
proposed security model with fuzzy rule-based approach is better than other related systems that are available in the literature in terms of reduction in computational complexity and increase in security.

**Keywords** - Pascal Triangle; Polynomial; differential calculus; two degree polynomial; three degree polynomial; Symmetric key; security; fuzzy rules, encryption and decryption.

*Corresponding Author: S.Pradeep, pradeep.suthanthiramani@gmail.com*

1. **INTRODUCTION**

Nowadays, the mobile network providers are working with 5G technology with Software Defined Networks (SDN) at their next level of technology improvement for replacing the existing 4G mobile networks due to the integration of Artificial Intelligence and Machine Learning techniques with networking technologies. The advanced concepts like virtualization, intelligent rule based decision making and software defined networks are the base points of the 5G network development. In addition, Device to Device (D2D) communication is the main concept underlying behind the growth of the 5G technology because it provides the short-range communication. The D2D is considered to be beneficial because it does not require any big infrastructure like base stations and Wireless Fidelity (Wi-Fi), access points. The fully autonomous functionality of the D2D communications is achieved by the application of soft computing techniques which saves huge money for the network service providers. Moreover, the number of Internet of Things (IoT) devices with intelligent and smart sensors is increasing in a regular speed and so the capacity of the network also needs to be improved to fulfill the expectation of the consumers. The fifth-generation mobile network has the advantage of reduced latency, higher capacity and also the speed can be increased to greater than 10 Gigabits per second (Gbps) while comparing to 4G technology. In future, the 5G can develop a mobile connected world in that some of the emerging concepts such as unmanned vehicles, smart parking facilities, mobile and fog computing, block chain based services, car to car communications and smart grid [1] are the major applications and they are successfully implemented with the support of Artificial Intelligence and Machine learning techniques. Some of the services provided by Artificial Intelligence to 5G networks include Intelligent Agent
Based Communication, Fuzzy rule based decision making on routing algorithms, intelligent clustering techniques for performing cluster based routing and the provision of soft computing based Intrusion detection and prevention mechanisms for enhancing the security of communication.

In this modern world, every one of us are depending on the computer networks for processing, sharing and accessing the data in a large stream in a scattered environment. The data transmission through the network in the scattered environment has the security issues like wire tappers and intruders. To fulfill the requirements of the users who need the confidential communication, the cryptographic algorithms have been applied in the network path where the intruders will view only the cipher text, but at the destination the plain text will be recovered by the authorized user with the security key. Here, both the sender and the receiver need to have a shared secret key to do the secured communication using cryptography in the network [21].

Cryptographic technique is not only used in network path but also in storage area network. The storage point of the data is a secured place in secure storage area networks. It provides the infrastructure for protecting confidential data with improved performance and flexibility. In the data centre, the data will be encrypted and stored in the encrypted format. When the authorized user needs to access those data from the data centre, they will decrypt the data by using the secret key they have. Advanced Encryption Standard (AES) algorithm was one of the selected symmetric key algorithms approved by National Institute of Standards and Technology (NIST) in the year of 2000 for encryption and decryption because of its better level of efficiency, larger key size and increased security [22].

Now a days, sharing of confidential as well as commercial information via internet is a common part and this is possible because of the networking technology only. When enormous number of users are connected in network, there is risk of security and privacy of the data so the concept of cryptographic methods have been introduced. Cryptography is a method of protecting the user data over the network from the third party who is unauthorized. Non-repudiation, integrity, confidentiality and authenticity are the properties of cryptography. Encryption and decryption are the two operations of the cryptographic technique. Initially, if the message to be transmitted through the network, it will be converted into unreadable format using some secret keys. The
unreadable format of message is named as cipher text and the process is called as encryption. The reverse process of encryption is called as decryption where the actual plain text message can be retrieved. There are two types of keys in which the first one is public key and the other is private key. Public key is the encryption and decryption key which is accessible publically by everyone who wants to encrypt or decrypt the message and it is actually an open key. Private Key is highly confidential key which will be disclosed only to the authorized user for decrypting the message.

Based on the key type, the cryptography is categorized into symmetric key and asymmetric key cryptography. In Asymmetric key cryptography, both the public and private keys are used in the process and the actual message will be encrypted by public key and the decryption of the cipher text can be done only by the private key. In Symmetric key cryptography, only single private is utilized in the process and hence the actual message will be encrypted using the private key at the sender side and at the other end, decryption will be done by using the same private key only. In this process, the secret key must be shared confidentially to the other end called receiver along with the encrypted message.

The security levels of the symmetric key completely rely on the size and the complexity of the key generation algorithm only. Some of the existing asymmetric key cryptography algorithms are Elliptic Curve Cryptography (ECC), the public key algorithm proposed by Rivest, Shamir and Adleman (RSA) and the Digital Signature Algorithm (DSA). In the fields like digital signature and message authentication, asymmetric key cryptography is applied. Some of the existing symmetric key cryptographies are Blowfish, Data Encryption Standard (DES), AES and 3-DES algorithms. In protected online transfer/online communication, symmetric key cryptography is used. Symmetric key cryptography is 1000 times faster than the Asymmetric key cryptography and comparatively the key size also lesser the Asymmetric cryptography [20]. Many other key management schemes are also present in the literature [36, 37, and 38].

However, the most of the existing techniques were developed for wired networks and 2G, 3G and 4G wireless networks. They have to be enhanced to suit the 5G networks. Moreover, many of the existing systems used key generation mechanisms that are not based on stronger algorithms since such techniques did not use stronger algebraic and calculus methods for the
generation of keys. In addition, intelligent routing algorithms are necessary to improve the overall network performance by increasing the packet delivery ratio and by reducing the delay and energy consumption in networks [24]. Therefore, a new key generation mechanism and encryption/decryption mechanism is proposed in this paper by following the symmetric key cryptography with both polynomial operations using binomial theorem, application of fuzzy rules and the use of differential calculus to find the derivatives for developing a more efficient security mechanism for securing the communication in 5G networks. First, we introduced a new method for generating keys by forming a polynomial of degree n using the expansion of Binomial Theorem (which is also forming the Pascal triangle) which is applied to generate the key that is used in the encryption process. Since the generalized form of the binomial theorem expansion is used in this work, the key becomes stronger when the degree of the polynomial is high. Moreover, the two different polynomial equations are formed in this work in which the first one is of degree two and the second one is of degree three are used for effective key generation. Moreover, the proposed algorithm is more efficient since it can be generalized easily to form polynomials of higher degree. Moreover, we have applied differential calculus for finding the keys on higher degree polynomials starting from polynomials of degree two and three. In the decryption part of the proposed secured key generation algorithm, $n^{th}$ root operations are considered in order to reduce the number of steps used in the single mode operation. Finally, a cluster based secure routing algorithm is used in this work in which the clustering and routing decision are made efficiently by the application of fuzzy rules for sending and storing the encrypted data. The experimental results obtained from the of the proposed work implemented using Cloudsim and Network Simulator Version 3 (NS-3) simulator have proved that the proposed key generation, encryption and decryption algorithm is providing better security as well as energy efficiency when it is compared with other related systems which are designed with a focus on the reduction of computational complexity and also in the provision of increased security in 5G networks.

The major contributions of this work are as follows:

1. Proposed a new key generation mechanism by using symmetric key cryptography and polynomial by developing a key generation mechanism using two different polynomial equations such as three degree and two degree.

2. The differential calculus is applied for finding the two-degree polynomial which is the
inverse of three-degree polynomial.

3. Introduced a new concept called New Binomial Theorem (Pascal triangle) technique for performing the data encryption process.

4. The $n$th root operation is applied for performing decryption process. It is able to reduce the number of steps that are available in single mode operation.

5. A fuzzy rule-based clustering scheme and also a cluster based intelligent routing algorithm with fuzzy rules have been proposed in this work for performing intelligent and secured routing in 5G networks.

The rest of this paper is organized as below: Brief literature survey in the direction of cryptographic algorithms especially the key generation schemes are shown in section 2. The overall proposed system architecture and the necessary explanations have been given in section 3. Section 4 explains the flow of the proposed model. Section 5 demonstrates the efficiency of the proposed model by showing the performance of the proposed model in various graphs and tables with necessary network evaluation metrics. Moreover, the reason for the performance improvements are also given under all the graphs and tables. Section 6 concludes the proposed work by highlighting the contributions and also suggests some future works.

2. LITERATURE SURVEY

Works on 5G network-based security mechanisms, trust-based schemes for network security, intrusion detection systems, cryptographic algorithms for performing encryption, decryption, key generation schemes have been carried out in the past by enormous researchers [23]. Among them, Biswas et al [1] proposed a new cryptographic system to overcome the limitations of complexities in computation, vulnerabilities in security and hardware implementation expenses. In this system, the nodes communication is verified and the pseudorandom bit sequence have been generated by utilizing elliptic curve points. The data lock encryption is done by using the generated sequence with the operations like crossover, mutation and Exclusive OR (XOR). From the implementation results, they proved that their proposed system is faster than Light Emitting Diode (LED) and Twine protocols. Wu et al [2] developed a new encryption scheme that generates shorter ciphertext. This scheme is based on Bilinear Diffie-Hellman Exponentiation and it is completely resistant against collusion. In addition, the authors have also presented a new aggregate encryption system called as broadcast encryption. The comprehensive property of their
proposed system will be highly useful during the construction of complex protocols.

Muradore et al [3] proposed an efficient energy saving security system which is completely based on packets. Here, the encryption is done selectively over the packets on which an attack occurs and it reduces the energy utilization. If the attack occurs during the packet transmission the energy utilization rate is high, so this system is designed by the authors in a way to act spontaneously. Liu et al [4] proposed a new coding model for secured network, which protects the nodes from the wiretap attacks. In this model, the authors have used inter/intra generation coding to overcome the drawback of complication in computations. The advantages of their model are, this can be easily integrated with other security methods, reduced complexity and utilization of very less bandwidth. Tan et al [5] proposed a new combined framework to protect the network from various attacks by providing router security. Trusted management system, trust based platform module and cryptographic mechanism are all together combined with this framework. Adding to the authors, the security framework proposed by them also detects false routing messages. Finally, they established that through the comparison of their work with other existing security frameworks, they proved that the performance of the network has been improved and attacks have been resisted by using their system.

Peng et al [6] proposed a new data transmission system to overcome the energy and security issues in the network. Comparing with the classic compressive sensing, the chaotic compressive sensing utilizes less storage space because it stores the parameters that are generated by matrix. In addition, chaos is highly sensitive and it increases the data transmission security. Mask and confusion are the two encryption techniques used in their proposed method which improves the quality of the encryption. After the results analysis, it proved by the authors that the security key complexity and efficiency have been improved and the storage space utilization has been reduced in their work. Liu et al [7] introduced a state estimation approach based on authentication and dynamic encryption in a smart grid for protecting the transmission and also for providing measurement reports between the remote terminal units and the control centers. The integrity and the confidentiality of the communication are ensured in their model by applying a set of two keys. The experimental results obtained by them show that their approach provides better security, less computational cost and increased error correction rate while comparing with other approaches in smart grid.
Tourani et al [8] carried out a detailed survey on information centric networking. The authors have focused mainly on three areas namely access control, privacy and security. Initially, the mechanisms like session based, encryption based, proxy re-encryption based and attribute based access controls have been reviewed by them. Next anonymity, signature privacy, name, content privacy and user privacy have been discussed. Finally, the security issue fields like cache pollution; content poisoning and denial of service have been discussed in their paper. Aguado et al [9] proposed a secured system by combining the known methodologies with quantum key distribution systems for protecting the control plane in the environment of Software Defined Networks and Network Function Virtualization. In addition, the authors have demonstrated their proposed workflow and created a secure shell by using the enhanced encryption process within Software Defined Networks and Cloud. After the demonstration, the authors established that their proposed system is proved to be applicable with other cryptography methodologies.

Schinianakis et al [10] introduced a new term known as lightweight cryptography which is completely interchangeable within symmetric and asymmetric keys. The traditional cryptographic attributes like Key exchange, no repudiation, authentication, integrity protection, identification and encryption/decryption were covered. The author have proved that their proposed cryptography is practically possible. Gill et al [11] proposed an improved future generation passive optical network which is depended over hash algorithm and uncontrolled signal scrambling to speed up the signal frequency in a decoded format. In this system, the symbols of orthogonal frequency division multiplexing have been pushed into time and frequency domains. The data restoration is done by comparing and computing the transmitted signals at the unit and terminal of the optical fiber. From the demonstrated results, it has been proved by the authors that physical layer of the network discussed by them is secured from the eavesdroppers and bad actors. Szyrkowiec et al [12] designed a new architecture for intent based automated secure service provisioning in optical network, multilayer IP and Ethernet while selecting the layer for encryption by adopting SDN orchestrator. The results of this work show that it provides completely negligible process impact. Aguado et al [13] designed a node construction method with improved end-to-end secure services and quantum key distribution for providing secure services in networks. In addition, the requirements of the control plane have
been analyzed by the authors. The demonstration is done by them with several scenarios and their proposed work has been integrated with virtual router. Tang et al [14] developed an enhanced encryption method with three layered dynamic approach to provide dynamic defense for the moving targets. This method is depending over network coding and DES with the property of partial key update and less complexity level. The implementation results provided by the authors have proved that the running time of their proposed method is comparatively less than triple DES method. Hu et al [15] introduced a new encryption method based on chaotic orthogonal matrix transformation for developing the security of the physical layer in passive optical networks. The authors have done the encryption by employing 4D hyper chaotic system for matrices generation which provides the encrypted codes that are highly complex and unpredictable while comparing with other physical security methods.

Li et al [16] proposed a new encryption method called mimic encryption for protecting the network from the attacks. Depending on mimic security defense and dynamic defense, this method has been developed by using bases of divarication, randomization and dynamism. The issues in networks like cipher text only attacks, vulnerability attacks; user data leakage, search attacks and network sniffing have been prevented by this mimic encryption. Furthermore, this system highly secured. Wei et al [17] presented a creative privacy preservation technique to overcome the privacy and security issues in online social networks (OSN). Initially, a prediction model was developed by combining radial basis function, neural network and genetic algorithm. Next, the OSN information is preprocessed by applying a support vector machine and for the encryption, attribute based encryption has been adopted by them. At last, for improving the privacy and security, a particle swarm optimization algorithm have been employed in their work. The implementation results provided by them show that their proposed technique is effective.

Feng et al [18] proposed a new scheme with selective sharing for the data owner to share their confidential data only to the authorized users in the vehicular social networks. In this scheme, the data owner provides different privileges to each individual user for accessing the data. The issues of data leakage from the cloud have been completely protected. Their proposed scheme is proven to be practically efficient while comparing with other data sharing schemes. Aichhorn et al [19] have carried out the analysis over the security function of IPsec
and safety of the network. As a result of this analysis, the authors have concluded that additional performance of the Central Processing Unit (CPU) due to encryption protection does not damage the safety functionality of the system because the required bandwidth has been provided for the communicating channel.

Ahmed et al [25] developed two secured protocols that are depended over the hash functions of quantum walk. The hash functions are Quantum Walk Hash function 1 and Quantum Walk Hash function 2 which provide security for the data communicated over 5G networks. Moreover, since the 5G networks are vulnerable to various types of attacks, the authors considered the two secured protocols proposed by them as the best fit for securing the 5G network. Bidi et al [26] proposed a weightless and undetectable policy for authenticating the users in 5G networks with multiple servers. In this work, the user validation as well as the server validation are performed using the elliptic curve cryptography for the purpose of reducing the computation complexity. Their system is proven to be secured from the forgery attack and the computation problem of Diffie Hellman. Dongfeng et al [27] designed a new architecture for providing security for 5G wireless networks. By relying over the architecture, authentication and identity management analysis were done. Sooyeon et al [28] developed a new efficient architecture for the purpose of integrating wireless sensor networks and 5G networks. In addition, the authors have designed a scheme for key agreement and a two-factor authentication for the integrated architecture to protect the 5G network from different types of attacks.

Marcus et al [29] have carried out a survey over the Key Management in small cell 5G mobile networks. Their key management scheme protects the network from several privacy and security related issues by the cryptographic solutions. The authors have presented their survey on key management schemes and it is useful for evaluating the flexibility of the mobile small cell networks. Md. Abdul et al [30] developed a new key distribution methodology which is based on the hexagon modelling. In their model, the number of keys and the key allotment to the nodes are determined by the key distribution methodology proposed by the authors. The explained that the number of keys shared among two nodes is one and the path length of the key is also one. Jin et al [31] proposed effective and secured authentication protocols for massive machine type communication in 5G networks, at the same time the devices are roaming into the new networks. They proposed two new protocols namely re-authentication and group-based handover.
authentication protocols. These protocols are better when comparing with other authentication protocols and standard machines in the terms of security.

Ahmed et al [34] developed a new quantum walks aware data encryption technique to ensure the data security in communication scenario which is incorporated the Internet of Things (IoT) in 5G network. They have proved that their technique is better than other related work in terms of reduction in encryption time. Ahmed et al [35] proposed a cybersecurity mechanism that was developed by considering the quantum inspiring and blockchain technology for ensuring the data security in an IoT technology incorporated smart cities. They have proved the efficiency of their model by achieving higher security level than other methods.

Pradeep et al [32] proposed a Secured Data Storage and Retrieval model using Elliptic Curve Cryptography for effective storage and retrieval of data in Cloud. Here, the data are collected using sensors present in a sensor network. The main advantage this secured storage model is the increase in security achieved through the power of Elliptic Curve Cryptography. In another work, Pradeep et al [33] proposed a new approach for security using Matrix Translation and Elliptic Curve Based Cryptosystem in order to provide secured data communications in Wireless Sensor Networks (WSNs). The matrix translation method provides an efficient mechanism for secured key generation. Vijayakumar et al [36] proposed a Chinese remainder theorem based centralised group key management for secure multicast communication in computer networks. Moreover, Vijayakumar et al [37] proposed another centralised key management protocol using greatest common divisors. However, due to the development the cloud networks, centralised key management systems cannot be used in distributed data communication and hence distributed security schemes are necessary. Finally, a new Dual Authentication and Key Management Technique was proposed by Vijayakumar et al. [38] for providing ssecured and intelligent data transmission in Vehicular Ad Hoc Networks.

In spite of the presence of many algorithms for security using cryptographic key generation, encryption and decryption, the existing algorithms cannot be used in 5G networks for providing security through secured storage and secured routing as the existing techniques have many limitations. First, most of the existing methods used smaller key sizes for performing the encryption. Second, some of the existing works are suitable for wired networks. Third, the
security algorithms developed for wireless networks are also made for 3G and 4G network. Fourth, the security methods provided for 5G networks are not extendible through mathematical generalization. Finally, fuzzy rule-based decision making for secured routing was not focussed on many existing works. Therefore, a new key management scheme using polynomials that can be generalised to n-th order polynomials has been proposed in this work for effective key generation. Moreover, a fuzzy rule and cluster based secured routing algorithm is proposed in this work that can either store the data with security in the cloud database using encryption or it can perform cluster based secured routing to the end user efficiently and securely.

3. SYSTEM ARCHITECTURE

The overall architecture of the proposed key-based secured communication system is shown in Figure 5.1. This proposed system architecture contains seven major components: Web user component for sending the documents, Key Generation Module, Encryption Phase, Third Party Auditor (TPA) and routing module, Decryption Phase, End User component for receiving the documents, and Web Database which is a cloud database. Here, the cloud user sends the document to the key generation phase in plain text form. The key generation phase performs the key generation process by applying second and third degree polynomials. The keys are generated based on the polynomial values that are received from polynomial operations. Then, the key generation module sends the input document along with the generated key to the encryption phase for performing the encryption operation.

The encryption phase applies the new binomial theorem concept for identifying the various combinations for the two input values such as User Identity (ID) and the secret key which are received along with the input document. The encrypted document is stored in the web database and it can be accessed by TPA with a secret key. The TPA sends the document to the decryption phase which performs nth root operation. As per the TPA direction, the decryption phase sends the decrypted document in plain text form to the end-user based on the end-user request. In this way, the end-user receives the relevant document from the decryption phase under the supervision and verification of the receiver credentials by the TPA through the checking of the user identity.
In this proposed model, the user components namely the data owner (sender) and the End user (receiver) are the client side components. All the other modules are the server side modules. Therefore, the request is sent by the end user (requesting client) through the third party auditor. Upon receiving the request, the third party auditor retrieves it from the web database in encrypted form and decrypts it using the decryption module and ensures the delivery in plain text form. For this purpose, a cluster based intelligent and secured routing algorithm is proposed in
this work in which fuzzy rules are used for making clustering and routing decisions. The data owner (storing/sending client) can store or route the data by sending it to the key generation and encryption phases for performing encryption of data before it is stored in the database or it is sent to the receiver through the 5G network using the TPA and routing module. The overall control of the system is with the TPA and routing module and it has a fuzzy inference system and an intelligent agent based communication support system for making intelligent decisions in storage, retrieval and routing. It will either store the encrypted data or it will route it to the receiving client. The TPA will not allow the decryption of data when it is routed through the network. The decryption is initiated only at the receiver end with the supervision of TPA.

This section explains in detail about the proposed model which consists of three major phases such as key generation phase, encryption phase and decryption phase for performing effective and secured data communication in 5G networks. In the key generation phase, a new key generation technique based on Polynomial operations and the Differential Calculus method and the Cathode Ray Tube (CRT) based Key Generation process is proposed for performing encryption and decryption processes. Here, the polynomial equations are used for generating a public key which is considered a symmetric key that is useful for the encryption and decryption process. In the encryption phase, a new binomial theorem concept is applied for encrypting the input text or document. In the decryption phase, the nth root operation is applied over the symmetric key to decrypt the encrypted text.

4. PROPOSED MODEL

This section explains in detail about the proposed model which contains three major phases such as key generation phase, encryption phase and decryption phase for performing effective data communication in cloud networks. In key generation phase, a new Polynomial and Differential Calculus and CRT based Key Generation Algorithm (PDC-KGA) is proposed in this work for performing encryption and decryption processes. Here, the polynomial equations are used for generating a public key which is considered a symmetric key which is useful for encryption and decryption process. In encryption phase, New Binomial Theorem (Pascal triangle) concept is applied for encrypting the input text or document. In decryption phase, nth root operation is applied over the symmetric key for decrypting the encrypted text.
4.1 Key Generation Phase

This subsection discusses about the key generation process in the proposed model. This phase contributes for this model by providing a common key for performing encryption and decryption processes in the form of symmetric key. This phase applied the newly proposed algorithm namely PDC-KGA for generating a public key. In the proposed Polynomial and Differential Calculus and CRT based Key Generation Algorithm called PDC-KGA, the key generation module selects two large prime numbers ‘p’ and ‘q’, initially where p>q. The value ‘p’ helps in defining a multiplicative group $\mathbb{Z}_p^*$ and ‘q’ is used to fix a threshold value to select the Group Key values. Now, the Key Server selects secret keys/private keys $k_i$ (user id / entry position / random number) from the multiplicative group $\mathbb{Z}_n^*$ for ‘n’ number of users which will be given to users as they join into the multicast group. It calculates the value of $\partial g$ using the following equation (4.1).

$$\partial g = \prod_{i=1}^{n} n$$

(4.1)

After this, it calculates the value of $x$ using the following equation (4.2).

$$x = \frac{\partial g}{k_i}$$

(4.2)

The value of equation (4.2) is used to find the value of the polynomial ($U_i$) equation (4.3) given below if we consider $U_i$ as an Integral function.

$$U_i = x^3 + x^2 - x$$

(4.3)

Moreover, the integration is the reverse of diversity operation. Therefore, it can be shown that the equation (4.4) is the inverse of equation (4.3).

$$V_i = 3x^2 + 2x - 1$$

(4.4)
Using the following CRT equation (4.5) it is confirmed that equation (4.4) is the additive inverse of equation (4.3).

\[ U_i + V_i \equiv 1 \mod k_i \]  \hspace{1cm} (4.5)

Finally, the proposed algorithm stores the value of “\( U_i + V_i \)” in “\( \text{Var}_i \)” using equation (4.6) and save the value of “\( \text{Var}_i \)” in equation \( \mu \) (4.7).

\[ \text{Var}_i = U_i + V_i \]  \hspace{1cm} (4.6)

\[ \mu = \sum_{i=1}^{n} \text{Var}_i \]  \hspace{1cm} (4.7)

Whenever a new user ‘\( i \)’ is authorized to join the dynamic multicast group for the first time, the Key Server sends a secret key ‘\( k_i \)’ using a secure unicast which is known only to the user ‘\( u_i \)’ and Key Server. Next, Key Server computes the Group Key in the following way and broadcast it to the users of the multicast group. Initially, the Key Server selects a random element ‘\( k_g \)’ as a new Group Key within the range ‘\( q \)’. Now, it multiplies the newly generated Group Key with the value of ‘\( \mu \)’ to get Y as shown in equation (4.8).

\[ Y = k_g \times \mu \]  \hspace{1cm} (4.8)

Now, the Key Server broadcasts a single message ‘\( Y \)’ to the multicast group members. On receiving ‘\( Y \)’ value from the Key Server, an authorized user ‘\( u_i \)’ of the current group can obtain the new Group Key ‘\( k_g \)’ by doing only one mod operation,

\[ Y \mod k_i = k_g. \]  \hspace{1cm} (4.9)

The steps of the proposed PDC-KGA are as follows:

Procedure pdc-kga(User_ID[ ], entry-position[ ], random_number[ ], Zn )

begin

choose-prime( p, q);  \hspace{1cm} // selects two large prime numbers ‘p’ and ‘q’, initially where p>q.


set $\partial g = 1$;
set $\mu = 0$;
for i:= 1 to n do
begin
  $k(i) = \text{key\_gen(user id(i), entry position(i), random number(i))}$;
  compute $\partial g = i \times \partial g$;
  compute $x = \frac{\partial g}{k_i}$;
  $U_i = \text{read (c1, p1, c2, p2, c3, p3)}$;  // from the polynomial $x^3 + x^2 - x$, coefficients
  c1=1, c2=1, c3=-1 and powers p1=3, p2=2 and p3=1.
  Compute $V_i = 3x^2 + 2x -1$  // Obtained by differentiating $U_i$.
  Check $(U_i + V_i \equiv 1 \mod k_i)$;
  Compute $\varpi_i = U_i + V_i$;
  Compute $\mu = \mu + \varpi(i)$;
  Compute $Y = kg \times \mu$;
  Broadcast $(Y)$;
End
Return Y;
End

4.2 Encryption Phase

This subsection discusses about the encryption process in the proposed model. This phase is useful to encrypt the original text by applying the newly proposed encryption algorithm called New Binomial Theorem (Pascal triangle) based Encryption Algorithm (BTEA).

In this work, the formula $C_i$ (4.10) given below is used to calculate the combinations of two variables $n$ and $k$.

$$C_i = \binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (4.10)$$

Where $n$ indicates the kg which is a public key and $k$ represents the number of iterations that
depends on n value in the encryption process. Here, the Alphanumeric value Table which is shown in Table 1 is used for assigning a value for the input text. Moreover, the public key will be considered as b.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

4.2.1 Encryption part

//Using New Binomial Theorem (Pascal triangle) to encryption//

//In fact there is a formula from Combinations for working out the value at any place in New Binomial Theorem (Pascal triangle): It is commonly called "n choose k" and written like this:

Encryption Text = \[ \sum_{i=0}^{n} C_i a^{n-i} b^i \]  \hspace{1cm} (4.11)

Where \[ C_i = \frac{n!}{i!(n-i)!} \]  \hspace{1cm} (4.12)

Encryption Text = Cipher Text (E)

The steps of the newly proposed Binomial Theorem based Encryption Algorithm (BTEA) are as follows:

*Binomial Theorem based Encryption Algorithm*
Step 1: Read a character/number from given content

Step 2: Find the combination $C_i$ using the formula which is given in Equation (4.12)

Step 3: Read the text and assign the values in $a_i$ by referring the table Alphanumeric value Table (4.1).

Step 4: The public key $k_g$ is assigned to $b$

Step 5: Apply the formula which is given in equation for getting encrypted text $M$ from input text

Step 6: Display the encrypted text

4.3 Decryption Phase

Decryption Part:

Cipher Text = $n\sqrt(M) - k_g$ = Original Decrypted Text.

4.4 EXAMPLE

1. Initially, select large prime numbers ‘$p = 5$’ and ‘$q = 3$’, where $5 > 3$. The value ‘$p$’ helps in defining a multiplicative group $Z_5^*$ and ‘$3$’ is used to fix a threshold value to select the Group Key values.

   $Z_5^* = \{1, 2, 3, 4\}$

2. Initially, the Key Server selects secret keys/private keys ‘$k_i$’ from the multiplicative group $Z_p^*$ for $n$ number of users which will be given to users as they join into the multicast group.

   $k_i = 4$

3. Calculate $\partial_g$,

   $$\partial_g = \prod_{i=1}^{n} n$$
4. Find ‘x’, \( x = \frac{\partial g}{k_i} \)

5. Calculate \( U_i = 63 + 62 - 6 \)
   \( U_i = 246 \)

6. Calculate \( V_i = 3(62) + 2(6) \)
   \( V_i = 119 \)

7. To check ‘\( V_i \)’ is the additive inverse of ‘\( U_i \)’,
   \( U_i + V_i \equiv 1 \mod k_i \)
   \( 246 + 119 \equiv 1 \mod 4 \)
   \( 365 \equiv 1 \mod 4 \)

8. Store ‘\( U_i + V_i \)’ in variable,
   \( \therefore \text{Var}_i = 365 = \mu \)

9. Whenever a new user ‘\( i \)’ is authorized to join the dynamic multicast group for the first time, the Key Server sends a secret key ‘\( k_i = 4 \)’ using a secure unicast which is known only to the user ‘\( u_i \)’ and Key Server. Next, Key Server computes the Group Key in the following way and broadcast it to the users of the multicast group.

10. Initially, Key Server selects a random element ‘\( k_g \)’ as a new Group Key within the range ‘\( q \)’.
    \( k_g = 2, \text{within the range } q = 3 \)

11. Multiply the newly generated Group Key with the value ‘\( \mu \)’, \( Y = k_g \times \mu \)
    \( Y = 2 \times 365 \)
    \( Y = 730 \)

12. The Key Server broadcast a single message ‘\( Y = 730 \)’ to the multicast group members. On receiving ‘\( Y \)’ value from the Key Server, an authorized user ‘\( u_i \)’ of the
current group can obtain the new Group Key ‘\(k_g\)’ by doing only one mod operation, \(Y \mod k_i = k_g\)

\[730 \mod 4 = 2\]

13. Symmetric Key Cryptography Algorithm Application: Symmetric Key = \(kg = 2 = n\).

14. Message: “H A I”

15. H A I = H→8=a1, A→1= a2, I→9= a3 using the Alphanumeric value Table.

### 4.4.1 Encryption Part

1. \(C_0 = \frac{2!}{0!(2-0)!} = 1\); \(C_1 = \frac{2!}{1!(2-1)!} = 2\); \(C_2 = \frac{2!}{2!(2-2)!} = 1\)

2. Encryption Text = \(1 \times (k_g^2a_1 = 1) + 2 \times (k_g^2a_1 = 2) + 1 \times (k_g^2a_1 = 1)\)

3. Encryption Text = \(1 \times (k_g^2) + 2 \times (k_g^2a_1) + 1 \times (k_g^2a_1)\)

4. \(H→8=a1 = (2)^2 + 2 \times (2) \times (8) + (8)^2 = 4 + 32 + 64 = 100\) First Cipher Text (E1)

\(A→1= a2\) = \((2)^2 + 2 \times (2) \times (1) + (1)^2 = 4 + 4 + 1 = 9\) First Cipher Text (E2)

\(I→9= a= (2)^2 + 2 \times (2) \times (9) + (9)^2 = 4 + 36 + 81 = 121\) First Cipher Text (E3)

### 4.4.2 Decryption Part

Cipher Text = \(n\sqrt{(M_i) - k_g} = \text{Decrypted Text}\)

\(DM_1→100\) = \(2\sqrt{(M_1) - k_g} = 2\sqrt{100 - 2}\) = \(10 - 2 = 8\) → H Decrypted Text

\(DM_2→9\) = \(2\sqrt{(M_2) - k_g} = 2\sqrt{9 - 2}\) = \(3 - 2 = 1\) → A Decrypted Text

\(DM_3→121\) = \(2\sqrt{(M_3) - k_g} = 2\sqrt{121 - 2}\) = \(11 - 2 = 9\) → I Decrypted Text

Message: “H A I”.

In this way, the message is decrypted to plain text form.
4.4.3 Cluster and Fuzzy Rule Based Secure Routing

In this work, a cluster and fuzzy logic based secure routing algorithm is proposed to route the data for either delivering to the receiver node or only to store the data in the cloud database. The data owner can request the trusted third party auditor and routing module to store the data with encryption. If there is a request for the data and the data owner provides permission to route and deliver the data to the requesting end user (client), then the data are routed to the end user. Since the data is to be stored in cloud database, it must be routed through the 5G network, in this case the cloud network. For this purpose, first the data are encrypted using the proposed encryption algorithm. The encrypted data are routed through the cluster head nodes to the destination. Therefore, a fuzzy rule based cluster head selection scheme is proposed in this work. Initially, the nodes with high energy, minimum distance from a set nodes and higher trusted past credentials are selected as the Cluster Heads (CHs). The cluster members are admitted to the clusters by the application fuzzy rules shown in Table 2. Here, the security level or sensitivity of data is also considered for effective selection of member nodes. The member nodes will become the cluster heads through cluster head rotation based on their current energy and distance of other nodes. After the formation of clusters, the data received by the member nodes are routed to the receiver using the cluster and fuzzy rule based secured routing algorithm proposed in this work. The member nodes can receive the data from the data owners and the CH nodes need not receive the data directly from the data owners. The secured routing algorithm uses five linguistic variables for selecting the next possible CH for routing. The secured routing algorithm checks the sensitivity of the encrypted data before it routes it to the next CH node.

Table 2 Fuzzy Rules

| Current Energy of Cluster Head Node | Distance Between CH and the Base Station | Distance Between Sensor Node and the CH | Security Level of Data | Member Choice          |
|-------------------------------------|----------------------------------------|----------------------------------------|------------------------|------------------------|
| Lower                              | Far                                    | Far                                    | Higher                 | Very much weaker       |
| Lower                              | Far                                    | Far                                    | Higher Average         | Weaker                 |
| Lower                              | Far                                    | Far                                    | Average                | Lower weaker           |
| Lower                              | Far                                    | Far                                    | Lower Average          | Lower medium           |
The steps of the proposed secure routing algorithm are as follows:

**Algorithm cluster and fuzzy rule based secure routing**

**Input:** Data submitted by the data owner

**Output:** Stored data at cloud database or data to be delivered to the end user.

Step 1: Read the nodes N1, N2……Nm.
Step 2: Call fuzzy k-means clustering algorithm and form initial clusters.
Step 3: Measure the energy levels and distances of nodes and select initial CH nodes.
Step 4: Apply the fuzzy rules and Dijkstra’s shortest path algorithm for selecting the best secured and shortest path.
Step 5: Make the data owner side client node to initiate the encryption process and encrypt the data using the proposed symmetric key and polynomials based encryption algorithm
Step 6: Check the sensitivity of data and find a secured route for sending the data by applying fuzzy rules.
Step 7: If data-option == store then Route the data through the cluster heads to the cloud database
Step 8: At cloud database, store the encrypted data securely with the direction of TPA.
Step 9: If the data-option == serve-end-user-Id then
    Send data to end user node
Step 10: Decrypt the data with TPA and data owner permissions
Step 11: Deliver the plain text data to end –user.

5 RESULTS AND DISCUSSION

This system has been implemented using Java programming as well as simulations. The implementation was carried out to implement the key management techniques and to perform secured storage and retrieval of data in order to preserve the data owner’s sensitive data in a shared database. Therefore, we have used CloudSim and Network Simulator (NS-3) for analyzing the performance of the proposed key generation scheme by incorporating in a cloud environment and wireless.

Figure 5.1 shows the security level analysis for the proposed symmetric key and polynomial based key generation and encryption scheme and the existing symmetric key generation techniques namely DES, Triple DES and AES algorithms. Here, we have conducted five different experiments namely E1, E2, E3, E4 and E5.
From Figure 5.1, it can be observed that the security level of the proposed model for encrypted storage is higher when it is compared with the existing symmetric key algorithms namely DES, Triple DES and AES by 7%, 5% and 3% respectively. In the proposed algorithm, a polynomial is used to generate key in addition to the use of Galois field polynomial used in AES algorithm. It also uses new Binomial Theorem based approach for key computation and hence it increases the security level than the security provided by the other symmetric key algorithms.

The proposed model provides more power to the data owner rather than the key distribution centre. In this model, the key distribution centre which is the server for the system is responsible only for monitoring the security and transactions and is not provided with access permissions for accessing the data. Therefore, the server available in the cloud data centre is responsible for applying the proposed association rule mining algorithm along with key generation, encryption and decryption. This design enhances the security for more sensitive data and hence the private data is more secured for all data owners.

Figure 5.2 shows the encryption time analysis between the proposed encryption model and the existing symmetric key encryption models namely DES, Triple DES and AES. We have conducted five different experiments which were repeated with different size of data selected from the dataset.
From Figure 5.2, it can be observed that the encryption time is less by 10 ms, 8 ms and 4 ms for the proposed model when it is compared with the existing techniques namely DES, Triple DES and AES. This reduction in Encryption time is due the identification of the key using the required term of the Binomial Theorem expansion for key generation.

Figure 5.3 shows the decryption time analysis between the proposed decryption model and the existing decryption models namely DES, Triple DES, and AES. We have conducted five different experiments which were repeated with different size of data selected from the dataset.
From Figure 5.3, it can be observed that the decryption time is less by 10 ms, 8 ms and 4 ms for the proposed model when it is compared with the existing techniques namely DES, Triple DES, and AES. This reduction in Decryption time is due to the nth root operation is applied over the symmetric key for decrypting the encrypted text.

Figure 5.4 shows the performance of the proposed encryption and decryption algorithm and the existing decryption models namely DES, Triple DES, and AES. We have conducted five experiments for performing comparative analysis according to the packet delivery rate.
Figure 5.4 Packet Delivery Rate Analysis

From Figure 5.4, it can be seen that the performance of the proposed Encryption and Decryption algorithm performs well by more than 8%, 5% and 2% than the existing techniques namely DES, Triple DES, and AES. The reason for the enhancement is the introduction of the fuzzy rules and also due to the applied the application of the Binomial Theorem.

Figure 5.5 shows the delay analysis between the proposed Encryption and Decryption algorithm performs well than the existing techniques namely DES, Triple DES, and AES. Here, five experiments have been conducted for performing comparative analysis according to the delay.
From Figure 5.5, it can be observed that the performance of the proposed model performs well in terms of delay by 4 ms, 3 ms and 2 ms than the existing techniques namely DES, Triple DES, and AES. This is due to the fact that the introduction of new enhanced encryption and decryption techniques and the use of fuzzy and cluster based secured routing.

Figure 5.6 shows the energy consumption analysis between the proposed Encryption and Decryption algorithm performs well than the existing techniques namely DES, Triple DES, and AES. Here, five experiments have been conducted for performing comparative analysis according to energy consumption.
Figure 5.6 Energy Consumption Analysis

From Figure 5.6, it can be seen that the performance of the proposed Encryption and Decryption algorithm consumes less energy than the existing techniques namely DES, Triple DES, and AES by 6 Joules, 4 Joules and 2 Joules. The reason for the enhancement is the introduction of new enhanced encryption and decryption techniques and fuzzy rule based decision making.

Figure 5.7 shows the overall network performances between the proposed Encryption and Decryption algorithm performs well than the existing algorithms namely DES, Triple DES, and AES. Here, five experiments have been conducted for performing comparative analysis according to overall network performances.
From Figure 5.7, it can be seen that the performance of the proposed Encryption and Decryption algorithm performs well than the existing techniques namely DES, Triple DES, and AES by more than 5% on an average. The reason for the enhancement is the introduction of new enhanced encryption and decryption techniques. The overall observation from this work is that if the data are routed using the proposed algorithm, the packet delivery ratio and overall network performances are increased and the energy consumption and delay are reduced when the results when it is compared with the related secured routing algorithms that use the existing symmetric key cryptographic algorithms. Finally, the use of fuzzy rules in the clustering and routing process enhanced the decision accuracy and hence it provided increased overall network performance.

6. CONCLUSION AND FUTURE WORKS

This paper proposes a new key generation mechanism which is based on symmetric key cryptography and polynomial for effective data communication in 5G networks. Moreover, this work introduces a new concept called New Binomial Theorem (Pascal triangle) technique for performing the data encryption process along with a fuzzy rule and cluster based secure routing algorithm. Moreover, the two different polynomial equations namely three degree and two degree polynomials have been used in this work for performing the key generation process.
effectively. In addition, differential calculus has been applied in this work for finding the two degree polynomial mathematically. In the decryption part of the proposed mechanism, n-th root operation is applied which is able to reduce the number of steps that are available in single mode operation. Finally, an intelligent clustering and fuzzy rule based secure routing algorithm has been proposed in this work for secured data storage as well as secured data delivery to the end user. The experimental results of the proposed work have proved that the proposed system is better than other systems in terms of security level by more than 5%, reduction in encryption and decryption time by more than 10 ms and the efficiency of retrieval process by more than 8% which are obtained through simulations. Future works in this direction can be the introduction of new intrusion detection system for identifying the standard network attackers which is useful for enhancing the security level of the system with better efficiency.

REFERENCES

1. K. Biswas, V. Muthukkumarasamy and K. Singh, "An Encryption Scheme Using Chaotic Map and Genetic Operations for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 15, No. 5, pp. 2801-2809, May 2015. doi: 10.1109/JSEN.2014.

2. Q. Wu, B. Qin, L. Zhang, J. Domingo-Ferrer, O. Farràs and J. A. Manjón, "Contributory Broadcast Encryption with Efficient Encryption and Short Ciphertexts", IEEE Transactions on Computers, Vol. 65, No. 2, pp. 466-479, 1 Feb. 2016.

3. R. Muradore and D. Quaglia, "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," in IEEE Transactions on Industrial Informatics, vol. 11, no. 3, pp. 830-840, June 2015.

4. G. Liu, B. Liu, X. Liu, F. Li and W. Guo, "Low-complexity secure network coding against wiretapping using intra/inter-generation coding", China Communications, Vol. 12, No. 6, pp. 116-125, June 2015.

5. S. Tan, X. Li and Q. Dong, "TrustR: An Integrated Router Security Framework for Protecting Computer Networks", IEEE Communications Letters, Vol. 20, No. 2, pp. 376-379, Feb. 2016.

6. H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang and D. Wang, "Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body
 Networks”, IEEE Transactions on Biomedical Circuits and Systems, Vol. 11, No. 3, pp. 558-573, June 2017.

7. T. Liu, J. Tian, Y. Gui, Y. Liu and P. Liu, “SEDEA: State Estimation-Based Dynamic Encryption and Authentication in Smart Grid”, IEEE Access, Vol. 5, pp. 15682-15693, 2017.

8. R. Tourani, S. Misra, T. Mick and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey", IEEE Communications Surveys & Tutorials, Vol. 20, No. 1, pp. 566-600, First quarter 2018.

9. Aguado A, Victor Lopez, Jesus Martinez-Mateo, Thomas Szyrkowiec, Achim Autenrieth, Momtchil Peev, Diego Lopez, "Hybrid conventional and quantum security for software defined and virtualized networks", IEEE/OSA Journal of Optical Communications and Networking, Vol. 9, No. 10, pp. 819-825, Oct. 2017.

10. D. Schinianakis, "Alternative Security Options in the 5G and IoT Era", IEEE Circuits and Systems Magazine, Vol. 17, No. 4, pp. 6-28, Fourth quarter 2017.

11. H. S. Gill, S. S. Gill and K. S. Bhatia, "A novel chaos-based encryption approach for future-generation passive optical networks using SHA-2", IEEE/OSA Journal of Optical Communications and Networking, Vol. 9, No. 12, pp. 1184-1190, Dec. 2017.

12. T. Szyrkowiec et al., "Automatic intent-based secure service creation through a multilayer SDN network orchestration”, IEEE/OSA Journal of Optical Communications and Networking, Vol. 10, No. 4, pp. 289-297, April 2018.

13. A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez and V. Martin, "Virtual network function deployment and service automation to provide end-to-end quantum encryption", IEEE/OSA Journal of Optical Communications and Networking, vol. 10, no. 4, pp. 421-430, April 2018.

14. H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense”, IEEE Access, Vol. 6, pp. 26059-26068, 2018.

15. Z. Hu and C. Chan, "A Real-Valued Chaotic Orthogonal Matrix Transform-Based Encryption for OFDM-PON", IEEE Photonics Technology Letters, Vol. 30, No. 16, pp. 1455-1458, 15 Aug.15, 2018.

16. B. Li, Q. Zhou, X. Si and J. Fu, "Mimic Encryption System for Network Security", IEEE
17. W. Wei, S. Liu, W. Li and D. Du, "Fractal Intelligent Privacy Protection in Online Social Network Using Attribute-Based Encryption Schemes", IEEE Transactions on Computational Social Systems, Vol. 5, No. 3, pp. 736-747, Sept. 2018.

18. X. Feng and L. Wang, "S2PD: A Selective Sharing Scheme for Privacy Data in Vehicular Social Networks", IEEE Access, Vol. 6, pp. 55139-55148, 2018.

19. A. Aichhorn, A. Unterweger, R. Mayrhofer and D. Engel, "Investigating the impact of network security on the line current differential protection system," in The Journal of Engineering, Vol. 2018, No. 15, pp. 1199-1203, 2018.

20. Sourabh Chandra, Bidisha Mandal, Sk. safikul Alam, Siddhartha Bhattacharyya, "Content Based Double Encryption Algorithm using Symmetric Key Cryptography", in Procedia Computer Science, Vol. 57, pp. 1228-1234, 2015.

21. L. Harn and D. Huang, "A protocol for establishing secure communication channels in a large network", IEEE Transactions on Knowledge and Data Engineering, Vol. 6, No. 1, pp. 188-191, Feb. 1994.

22. H. Kouzehzar, M. N. Moghadam and P. Torkzadeh, "A High Data Rate Pipelined Architecture of AES Encryption/Decryption in Storage Area Networks," Iranian Conference on Electrical Engineering (ICEE), pp. 23-28, 2018.

23. S Ganapathy, K Kulothungan, S Muthurajkumar, M Vijayalakshmi, P.Yogesh, A.Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey", EURASIP Journal on Wireless Communications and Networking, Vol. 271, No.1, pp. 1-16, 2013.

24. R Logambigai, S Ganapathy, A Kannan, "Energy–Efficient Grid–Based Routing Algorithm using Intelligent Fuzzy Rules for Wireless Sensor Networks", Computers & Electrical Engineering, Vol.68, pp.62-75, 2018.

25. Ahmed A. Abd EL-Latif, Bassem Abd-El-Atty, Salvador E. Venegas-Andraca, Wojciech Mazurczyk, "Efficient quantum-based security protocols for information sharing and data protection in 5G networks", Future Generation Computer Systems, Elsevier, Vol.100, pp.893-906, 2019.

26. Bidi Ying, Amiya Nayak, "Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography", Journal of Network and
27. Dongfeng Fang, Yi Qian, Rose Qingyang Hu, "Security for 5G Mobile Wireless Networks", IEEE Access, Vol.6, pp.4850-4874, 2018.

28. Sooyeon Shin, Taekyoung Kwon, "Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks", IEEE Access, Vol.6, pp.11229-11241, 2018.

29. Marcus De Ree, Georgios Mantas, Ayman Radwan, Shahid Mumtaz, Jonathan Rodriguez, Ifiok E. Otung, "Key Management for Beyond 5G Mobile Small Cells: A Survey", IEEE Access, Vol.7, pp.59200 - 59236, 2019.

30. Md. Abdul Hamid, M. Abdullah-Al-Wadud, Mohammad Mehedi Hassan, Ahmad Almogren, Atif Alamri, Abu Raihan M. Kamal, Md. Mamun-Or-Rashid, "A key distribution scheme for secure communication in acoustic sensor networks", Future Generation Computer Systems, Elsevier, Vol.86, pp.1209-1217, 2018.

31. Jin Caoa, Maode Ma, Hui Li, Yulong Fu, Xuefeng Liu, "EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks", Journal of Network and Computer Applications, Elsevier, Vol.102, pp.1-16, 2018.

32. Pradeep, S, Muthurajkumar, S, Ganapathy, S& Kannan, Arputharaj, ‘Secured Data Storage and Retrieval using Elliptic Curve Cryptography in Cloud’, International Arab Journal of Information Technology, vol. 18, no.1, pp. 56-66, 2021.

33. Pradeep, S, Muthurajkumar, S, Ganapathy, S& Kannan, Arputharaj, ‘A Matrix Translation and Elliptic Curve Based Cryptosystem for Secured Data Communications in WSNs’, Wireless Personal Communications, https://doi.org/10.1007/s11277-021-08221-9, pp.1-20, 2021.

34. Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, Wojciech Mazurczyk, Carol Fung, Salvador E. Venegas-Andraca, “Secure data encryption based on quantum walks for 5G Internet of Things scenario”, IEEE Transactions on Network and Service Management, Vol.17, No.1, pp. 118-131, 2020.

35. Ahmed A.Abd El-Latif, BassemAbd-El-Atty, Irfan Mehmood, Khan Muhammad, Salvador E.Venegas-Andraca, Jialiang Peng, “Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities”, Information Processing & Management, Vol. 58, No.4, Article No. 102549, 2021.
36. Vijayakumar, P, Bose, S & Kannan, A, ‘Chinese remainder theorem based centralised group key management for secure multicast communication,’ IET Information Security, vol. 8, no. 3, pp. 179-187, 2014.

37. Vijayakumar, P, Bose, S & Kannan, A, ‘Centralized key distribution protocol using the greatest common divisor method’, Computers & Mathematics with Applications, vol. 65, no. 9, pp. 1360-1368, 2013.

38. Vijayakumar, P, Azees, M, Kannan, A & Jegatha Deborah, L, ‘Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks,’ in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, pp. 1015-1028, 2016.