Volume 7, Issue 3, March 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancing Data Encryption using Elliptic Curve Cryptography (ECC) Algorithm in 4G Networks

Abdu Ahmed Osman*
Science Department, Abdulrahman Al Sumait Memorial University- Zanzibar, Tanzania

DOI: 10.23956/ijarcsse/V7I3/01308

Abstract: ***Security advances and challenges associated with 4G wireless technologies have been presented in this paper. The contribution of the paper in the area of 4G security represented in the study of data encryption issues and the potential threats and risks across the 4G networks. Another contribution was the study of the major cryptography methods in 4G networks. To enhance the data encryption process in the 4G networks, Elliptic curve cryptosystem (ECC) for data encryption algorithm is proposed. The Strength of the proposed ECC algorithm depends on the complexity of computing discrete logarithm in a large prime modulus. ECC needs a less storage space due to the shorter key length and faster arithmetic operations. These ECC advantages are important for mobile devices, because they are constrained devices. The evaluation focuses on: Key generation time and Encryption- Decryption time. Results show that the performance of ECC, in three area of evaluation, was better than the RSA algorithm which is used for comparison purpose.***

Keywords: 4G Networks, Data Encryption, Elliptic curve cryptography.

I. INTRODUCTION

'3G' and '4G' are the terminologies used in abundance in the market of mobiles and tablets, while they are one of the most ambiguous terms in the mobile technology dictionaries. The third generation or 3G is considered as a modern technology in the field of telecommunications, with minimum reliable Internet speeds of 384 Kbps, and 2 MB in HSDPA (High-Speed Downlink Packet Access) technology [1]. This technology provides some services were not available on the earlier generations, such as video calling and watch TV channels and other services via the mobile phone. The fourth generation or 4G is wireless mobile telecommunications technology, succeeding 3G. The first improvement that offered by 4G networks is the speed, this new technology is will providing data transfer speed faster by 4 to 10 times [2] than that of the 3G. Speed is what matters most to the average user, but the new technology is providing a number of other improvements, such as more security and protection, better switch between the towers and networks, better international roaming, higher data rate, and other improvements.

II. KEY FEATURES OF 4G NETWORKS

2.1 Evolution of Mobile Technologies

Innovation is a cornerstone of Technology. Ten years ago today, it was enough simply sending a small text message, or a fun game of Snake on a screen of two colours. Today, we have portable devices that can surface and process like any other desktop computers, and at the same time period. Following is the review of the most important stages of the evolution of Mobile Technologies.

2.1.1 1G (First Generation):-

The first generation of communications came out in 1980's [3] and powered by Frequency Division Multiplexing (FDM) and relies on analog waves. This has been dealing with all the calls in where the local area is divided in to cells around limited distance each served as base station, "There are no short messages or Internet." Because of that the network relies on analog signals and did not use encryption techniques, it was hunting for penetrating and spying easy and who was one of the reasons why experts to develop a new generation of networks.

2.1.2 2G (Second Generation):-

This generation is considered the most famous in the world of communications, who was known as GSM, or Global System of Mobility. This generation is relied on new techniques based on digital signals to be the first generation based on digital signals [4], using techniques such as TDMA and CDMA. This opened the door for new services such as short messaging services (SMS) and E-mails. The Development continues in this generation of communications until 2.5G or GPRS technology emerged, which has reached the data speed of 144 Kbps. After that 2.75G EDGE technology emerged and reached a speed of 1 megabit per second, and new services have been added such as multimedia messaging (MMS) and wireless Internet WAP.

2.1.3 3G (Third Generation):-

This generation was based on UMTS technology which allowed larger data processing and greater speed of up to 2 megabits per second [5], or a little beyond. It added other new services such as video calls and Global Positioning

System GPS. Despite the great features that have emerged with this generation, however, it is considered expensive and consumes the largest energy. The network has evolved to 3.5G by adding HSDPA & HSUPA technology, which raised speed limits to 14.4 Mbps for download and 5.88 Mbps for upload. The speed has been raise to 56 Mbps for download and 22 Mbps for upload after the network evolved to 3.75G with the presence of HSPA+ technology.

2.1.4 4G (Fourth Generation):-

This generation depends on the Long-Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (Wimax) standards and offering high speeds of up to 173 Mbps [6], which have been developed until it reached 225 Mbps using the new standards for LTE-A, which enables you to download a movie in the range of 800 MB in less than half a minute.

2.2 What is 4G?

4G refers to the fourth generation of cellular wireless communication generations, which is the latest technology in the field of mobile phone networks, allowing wireless Internet access at a much higher speed. LTE technology (Long Term Evolution) is a new standard for fourth generation networks, provides very high speeds for data transmission compared with 3G networks.

2.2.1 How does LTE work?

Unlike CDMA and GSM, which were transfers small amounts of data, the new technology LTE changes the current method of moving data to an internet protocol system [7], which means that the large packets of data can move through the system.

LTE uses Orthogonal Frequency Division Multiplexing (OFDM) for downlink, OFDM is a method of encoding digital data on multiple carrier frequencies, and for uplink it uses Single Carrier Frequency Division Multiple Access (SC-FDMA), SC-FDMA deals with the assignment of multiple users to a shared communication resource. To enhance the throughput, LTE uses Multi-input Multi-output (MIMO) technique. The major benefit to LTE is that in reduces the latency in data transfer and in reduces the power consumption.

2.2.2 LTE Architecture

The high-level network architecture of LTE is comprised of following three main components [8]:

The User Equipment (UE): This part contains the following modules: Mobile Termination (MT): This handles all the communication functions. Terminal Equipment (TE): This terminates the data streams. Universal Integrated Circuit Card (UICC) or LTE SIM card it runs an application known as the Universal Subscriber Identity Module (USIM).

The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN): The E-UTRAN switches the radio communications between the mobile and the evolved packet core with one component, called eNodeB or eNB (base station).

The Evolved Packet Core (EPC), comprised: The Home Subscriber Server (HSS) which is a central database that contains the entire network operator's subscribers information. The Packet Data Network (PDN) Gateway (P-GW) this is the part that is responsible to communicate with the outside world with specific interface known as Sgi (Silicon Graphics). The serving gateway (S-GW) it looks like a router, and switches data between the base station and the PDN gateway. The mobility management entity (MME) the high-level operation of the mobile is controlled by this part.

2.3 4G benefits

The most important benefit of using the fourth-generation technology 4G is the speed of data transfer, offering the user high speed data transfer to do things faster with the possibility of doubling the Internet access speed, which is one of the most important features of interest to the user, but it must be said that the speed will vary from company to another according to the network infrastructure of the company. Another benefit of 4G is the consuming more media on user device and work harder as well as the highest quality in the sound.

Among the benefits of using the fourth-generation technology is also the possibility of obtaining a higher degree of security and protection for data, video streaming services, as well as better international roaming.

2.4 Types of 4G

4G+ or LTE-A

In October 2010 the International Telecommunication Union Radiocommunication Sector (ITU-R) adopted six new technologies [9], which is what would be called the fourth generation, one among them is LTE Advanced (LTE-A / 4G +) technology for mobile phones networks.

You must know that LTE Advanced technology is not just high-speed data upload rats only, but LTE-A / 4G + is in fact a combination of several different techniques. The largest of these is called "carrier aggregation." This allows mobile phones to collect different wave frequencies, which may also be contiguous, and then receives the data at once from each carrier wavelength, thus imagination speeds have been achieved.

Fourth-generation technology features they rely on the technology of MIMO which means Multiple Input Multiple Output, and this is done by using several Antennas, so that you can meet a huge amount of users and provide them with this tremendous amount of speed in transport.

4GX

Telstra, in Australia, officially revealed its new 4GX technology for mobile networks, which is really the new Next-G network for 4G technology. 4GX is a imagine name for its new 700 MHz 4G network. It means higher speeds and better coverage, both in buildings and in pastoral areas. It can do this due to the lower frequency, which allows the

signal to travel farther. It's also faster; due to the current frequency of the network is half to the frequency of the proposed network, which means they can afford theoretically twice the amount of data.

XLTE

XLTE is basically a Verizon version of 4GX. It's just a way to describe how they open up more LTE spectrum. LTE bands, named by AWS (Advanced Wireless Service), are only numbered, and this one gets name (spectrum) because has two frequencies 1700MHz spectrum for uploads, and 2100MHz spectrum for downloads, whereas the others are using the same frequency for uploading and downloading.

VoLTE

VoLTE is sound transfer protocol through the fourth generation networks, where from which we can make high-definition video and voice calls in the case of higher bandwidth availability. It is also provides a wider range of audio with noise cancellation which helps to make more productive work sessions.

- VOLTE technology allows you to browse the Internet, complete your download, and running other applications while continuing to call on the phone, as you can move smoothly from voice call to a video call during the call. You can also, through VOLTE, collect voice calls up to 7 people together, and group video calls for up to 4 individuals.

III. LITERATURE SURVEY

To address the data encryption issues in 4G Networks, numbers of data security models have been developed. In paper [10] some challenges in terms of Security, Bandwidth, Multiple Frequencies, etc. have been discussed without presenting proposals or naming algorithms for how to solve the security problems in 4G Networks. Paper [11] proposed a dynamic S-box to enhance AES algorithm. The performance evaluation shows that the enhanced AES is a good alternative to the traditional AES with more confusion. To increase the complexity of the encryption, the paper proposed the number of rounds must be increased, but this will increase the processing time. Paper [12] introduced a theoretical background about the physical layer security in wireless networks. The authors argue that there is difficulty in securing the physical layer, in some aspects, lies in the implementation complexity and energy consumption. A novel key valid by time instant scheme, using AES (advanced encryption standard) algorithm, is proposed in paper [13] to enhance security in cloud computing. With The application of the proposed system, the data on the cloud can be accessed or downloaded when appropriate incorporation of various conditions is achieved. The main shortage in this proposal is that limited types of data and files can be exchanged over clouds. Senthilkumar Mathi∗ and Lavanya Dharuman [14] are proposed scheme to overcome the desynchronization problem in 4G LTE network using Double Authentication technique. The scheme shows efficiency in terms of communication cost. But the main drawback of like this technique is that, it cannot prevent identity theft, and cannot apply online security to prevent accounts from fraudulent transactions. Kire Jakimoski in his paper [15] analyzed and evaluated the security techniques for data protection in the cloud computing. The paper suggested a two-factor authentication as boundary defense of the data in the cloud. But the two-factor authentication solves the security problems we had ten years ago, not the security problems we have today. Krishna Prakash and Balachandra in their paper [16] provided general overview of mobile computing and m-commerce security issues and challenges. They addressed in details the wireless networks concepts and the techniques that have been used in this type of networks; also they mentioned the security vulnerabilities and the main drawbacks of each security technique without going into security algorithms and protocols. In paper [17] the authors have proposed a scheme of user authentication and data confidentiality using public key infrastructure (PKI). But, the PKI is more complicated, and complexity is the opponent of good computer security and PKI doesn't solve the biggest security problems.

IV. DATA ENCRYPTION ISSUES IN 4G NETWORKS

4.1 What is data encryption?

Data encryption is the process of changing the plaintext into cipher text using specific cryptographic key to provide confidentiality protection for data [18].

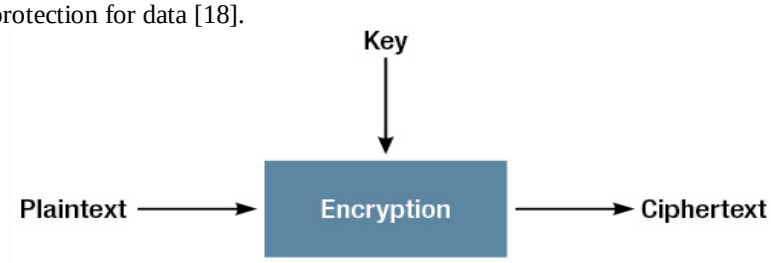

Fig.1depicts the concept of encryption

4.2 Security issues to be addressed before starting the encryption process

Data encryption process is an important, but it’s not everything in the Data Protection field. There is a number of issues, such as data security plan and data privacy, should be taking into account before encrypting the data. Complacency in such things leads to add cost and complexity of the security systems.

Security plan should point to the data classification clearly, because not all data requires equal protection. Another issue to pay attention is that the encryption process will applied for data in motion rather than stored data. The issue of encryption key management is the entrance to the disputes between the company owners and users, so preferably administered by a third party [19].

4.3 Data security issues in 4G networks

There are several security issues that have to be taken into consideration when deploying 4G networks. Security issues can be classified as data integrity, confidentiality, Authentication, Access Control, Operating Systems, and Downloading Contents as show below [20].

1. Authentication: the main target of 4G networks (huge number of subscribers) is to allow users to communicate from different regions in the world, so the processes of connecting subscribers and authentication of users become an issue.
2. Confidentiality: today users' devices depending upon 4G technology to send and receive sensitive information, so secure channels compulsory to achieve the confidentiality.
3. Integrity: Services provided by this technology, such as SMS, chat and file transfer, it is necessary to be delivered complete without any modification or distortion, shortages or increased.
4. Access Control: Access control to some sensitive files is an important issue, so to put policy for restricted access to the database is an effective protection way.
5. Operating Systems: As a result of the diversity of operating systems in devices that support fourth-generation technology, there is the possibility of the existence of security vulnerabilities that can be exploited by others.
6. Web Services: these services open the door to a large number of security issues and risks. These risks arise when the user browses unguarded websites which are depends on standard HTTP Protocol.
7. Downloading Contents: With no digital rights management, the scope is wide for illegal downloads, which brings with it the possibility to download spyware and eavesdropping software.

4.4 Threats and risks in 4G networks

We are required to understand the main threats and risks in 4G networks to mitigate them. According to McAfee [21], there are 7 deadly Threats to 4G.

1- Wireless Access Point Name (APN) flooding:
The great bandwidth provided by the fourth generation technology is a feature of these networks, but at the same time is a platform for cybercriminals to attack. The bandwidth of 4G LTE is 10 times faster than 3G— has peak download speeds approaching 50 Mbps, 5 to 12 Mbps for download 2 to 5 Mbps for upload. Cable speeds vary, but 4 to 12 Mbps are common. Unless preventive measures against offensive operations, the criminal activities will consume half of the bandwidth that is supposed to go to the users.

2- Peer To Peer (P2P) Communication Attacks:
Traffic in the 4G networks based on IP Protocol, which allow the transition from one device to another without going directly to the core network, unlike the case of the third-generation networks. This flexibility in motion produced what is known mobile-to-mobile (Mob2Mob) attacks. This type of attacks consuming huge amounts of spectrum consumes, drains the battery on the victim's device by maintaining a network connection, and can also cause a denial-of-service (DoS) situation due to signalling congestion.

3- virtualization:
In order to reduce operating costs many companies adopting virtualization technology. But virtualization has many security vulnerabilities which can be exploited by attackers. Implementing some kind of virtual machine monitor like hypervisors can mitigate the risks of attack.

4- Machine to machine fragility:
Machine to machine (M2M) is used to describe any technology that allows networked devices to switch information and carry out actions without the manual assistance of humans. The main drawback of M2M system is that it's intended to work within hostile environment of the internet. When devices- in these systems- have been attacked, they will stop immediately without easily recovering. 4G technology providers who are looking to provide M2M service, a degree of security standards and awareness about mobile security attacks will be useful.

5- Lawful intercept compliance:
Development, which is in the fourth generation technology, allows you to track or intercept some of the traffic in the network orders hat come from the judiciary, through improvements to the system, such as the better designing for the interception, monitoring, and collection capability into the relevant points of the network.

6- VOLTE service assurance:
Voice services and media services are adding a quality to user devices. Voice over long-term evolution (Voice over LTE/VoLTE) is a technology that defines the principles and measures for sending voice signals and data over 4G LTE networks. Strategies and tactics that have been used to attack VOIP can be used to attack VoLTE effectively, because VOLTE infrastructure sometimes can be accessed even if it's not connected to the Internet. To detect attacks and threats in such networks (4G) characterized by the movement of high data traffic, different monitoring equipment is needed.

7- Content and media delivery:
Video and music are representing the more of the data travelling over the Internet, and thus are vulnerable to attack than others. Attackers attempt to disrupt content delivery systems In order to prevent the arrival of materials to the user or reached with a damaged or distorted case, this damage the company's reputation.

V. CRYPTOGRAPHY METHODS IN 4G NETWORKS

In the field of 4G network security there are two standardized algorithms required for the radio interface, namely:

- EEA = EPS Encryption Algorithm (EPS = Evolved Packet System)
- EIA: EPS Integrity Algorithm

We can classify the cryptographic algorithms of 4G into three sets [22] for confidentiality and integrity.

Set 1 includes (128-EEA1/128-EIA1) and they are stream cipher integrity algorithms based on SNOW 3G in producing the keystream. Set 2 includes (128-EEA2/128-EIA2) and this also is stream cipher algorithm for confidentiality in its first portion basing on the block cipher of 128-bit AES (Advanced Encryption

Standard) algorithm in CTR (Counter mode), and the second portion is based on Cipher-based MAC mode to insure the integrity. The third set of these algorithms is (128-EEA3/128-EIA3) based on ZUC as a keystream algorithm; 128-EEA3 is a stream cipher confidentiality algorithm to encrypt/decrypt blocks of data using a confidentiality key, while 128-EIA3 is an integrity algorithm to calculate a 32-bit MAC of the intended input [23].

The analytical evaluation of these sets has been applied [24] to test their efficiency during the execution by taking the time, space and data complexity as factors of the algorithms to measure the amount of security.

To achieve the space complexity AES algorithm executes message with 20, 000 bits length which is suitable for mobile equipments, and in terms of time complexity AES offers a high efficiency, While SNOW 3G and ZUC offer constant space complexity and linear time complexity.

To measure the resistance of each algorithm against specific kinds of attacks, some tests have been conducted, and the result was that the ZUC has a better resistance than SNOW 3G.

VI. PROPOSED ALGORITHM AND IMPLEMENTATION

From the previous analytical evaluation it became clear that AES has a potential advantage in terms of space and time complexity, while it is suffering from a lack of attacks resistance like linear and algebraic attacks, ZUC algorithm is characterized at this point. In order to overcome drawbacks of 4G cipher algorithms, Elliptic curve cryptosystem (ECC) for data encryption algorithm is used. The Strength of the proposed ECC algorithm depends on the complexity of computing discrete logarithm in a large prime modulus. ECC needs a less storage space due to the shorter key length and faster arithmetic operations. These ECC advantages are important for mobile devices, because they are constrained devices.

In 1985 Victor Miller (IBM) and Neil Koblitz (University of Washington) are proposed Elliptic Curve Cryptography (ECC) as an alternative mechanism for implementing public-key cryptography. In this scheme public key cryptography for data encryption is proposed to enhance the security level of 4G networks.

To demonstrate the power of ECC algorithm will be compared with RSA algorithm used in public key generation, by implementing each algorithm and comparing their experimental running-times in an attempt to measure the experimental time efficiencies of each.

6.1 Proposed Algorithm

As the other algorithms, public and private key generation in elliptic curve follows the same rules, the main difference being that the keys of elliptic curve exist only in the context of a particular elliptic curve and require having curve parameters associated with them to be of any use.

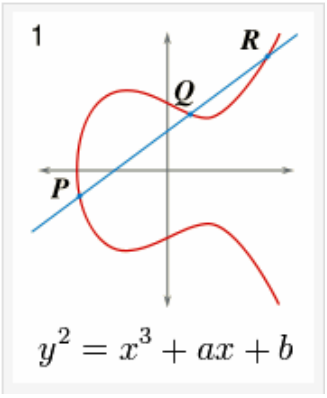

Fig. 2 shows simple elliptic curve.

The equation of an elliptic curve over a finite field considered in our work is given by Weierstrass equation as:

y2 (mod p) = (x3 + ax + b) mod p……. (1)

Where, x, y = coordinates, and a, b = are two integers.

Key generation

Step 1: select a random number **d**, within the range (**1 to n-1**), where **n** is Maximum limit (should be a prime number).
Step 2: from the elliptic curve determine **Q** and **P** points.
Step 3: Use the following equation to generate the public key

Q = d * P …… (2)

Step 4: '**Q**' is the public key and '**d**' is the private key, Operation '*' denotes the series of Point doubling and Point adding.

Encryption

Before the encryption process, the message that we want to send should be divided into small parts using hash function. Let "m" be the message that we want to send, and should be represented by the point 'M' into the curve 'E'. In the specified range (**1 to n-1**) select "k" randomly. The following equations will generate the cipher texts (**C1**, using the private key & **C2**, using Elliptic curve Algorithm with receiver's public key) after the encryption process.

$$C1 = k * p \quad (3)$$

$$C2 = M + k * Q \quad (4)$$

Decryption

From the (3 &4) **M** can be derived,
M = C2 – K * Q, from (2) Q = d * P
M = C2 – K * d * P, from (1) **k * p = C1**
So the message "M" that was sent is:

$$M = C2 - d * C1 \quad (5)$$

M is combining C2 and C1, so that means the decryption process is completed using the sender's public key and receiver's private key.

Proof

To proof that the: cipher text = plain text
Cipher text = C2 - d * c1, and plain text = M
From equation (5):
RHS C2 - d * c1 = (M + k * Q) - d * (k * p)
But Q = d * P
So:
C2 - d * c1 = (M + k * d * p) - d * (k * p)
By cancelling out k * d * p,
C2 - d * c1 = M
M is the original message.

VII. SIMULATION

A. System Configuration

Tests were performed on an Intel(R) core(TM) i5-3337u CPU @ 1.80 GHz 1.80 GHz processor with installed memory (RAM) 4 GB and a 64-bit operating system Windows 8. 6534 KB block size is used for encryption and decryption processes.

B. Run-time Comparisons

To test and compare the performance characteristics of the RSA and ECC algorithms, we independently tested each of the three parameters: key generation, Encryption, and decryption.

The following table suggested by A. Lenstra, and E. Verheul [25] is used to test the performance of the two algorithms in terms of key size.

Table 7-1 Comparable key sizes (in bits)

ECC	RSA
163	**1024**
233	**2240**
283	**3072**
409	**7680**
571	**15360**

VIII. RESULTS

The following tables provide the performance of the key generation, as well as encryption and decryption times for ECC and RSA.

Table 8.1 ECC performance

Block Size (KB)	Key Length (bits)	Key Generation Time (sec)	Encryption Time (sec)	Decryption Time(sec)
6534	**163**	**0.258**	**2.480**	**1.487**
6534	**233**	**0.268**	**0.955**	**1.139**
6534	**283**	**0.276**	**1.047**	**1.070**
6534	**409**	**0.287**	**0.780**	**0.861**
6534	**571**	**0.321**	**0.706**	**0.804**

Table 8.2 RSA performance

Block Size (KB)	Key Length (bits)	Key Generation Time (sec)	Encryption Time (sec)	Decryption Time(sec)
6534	**1024**	**0.880**	**14.047**	**111.035**
6534	**2240**	**2.998**	**18.206**	**300.545**
6534	**3072**	**17.694**	**29.986**	**998.054**
6534	**7680**	**141.794**	**41.888**	**210.369**
6534	**15360**	**686.954**	**72.781**	**787.686**

IX. RESULTS ANALYSIS

A. Key Generation Time

ECC Key generation perform better than RSA at all key lengths, and is especially obvious when we increase the length of the key. Despite that the ECC does not have a dedicated resources to the computationally intensive generation of prime numbers, but it is superior RSA in speed to generate the private/public key using comparable lengths. ECC key generation time grows linearly with key size, while RSA grows exponentially.

B. Encryption/Decryption Time

Encryption and decryption time is depends on the processor speed, complexity of the algorithm etc. From the result tables, ECC with small key size gives much faster encryption/decryption as compared to RSA. The Time of encryption/decryption in RSA is growing exponentially with the given key size. ECC encryption time varies linearly depending on the input key size while in RSA it increases exponentially, also the decryption time remains in the exponential increase. The decryption time varies exponentially with key size for RSA and it remains linear for ECC as the case with encryption.

X. CONCLUSION AND FUTURE SCOPE

The main advantages of ECC are smaller keys and very fast key generation, which is required by the 4G networks that use limited sources Mobile devices. Results show that data is encrypted in inacceptable time in ECC algorithm which is the best algorithm of encryption technology and it is more secure than RSA.

The future is for ECC because of its inherent advantages such as moderately fast encryption and decryption. The research work can be extended with the use of further enhancements on ECC. One enhancement is that it can make use of good protocols for authenticated key exchange. Also the system can be modified and run on high end configurations to obtain more speed and security in 4G networks.

REFERENCES

[1] Obasi Miracle, *Difference Between Gprs, Edge, 3g, Hspa, Hspa+ & 4g Lte*, [Online]. Available: https://www.3ptechies.com/differences-between-gprs-edge-3g-hsdpa-hspa4g-lte.html, 2016.

[2] (2016) The Wikipedia website. [Online]. Available: https://en.wikipedia.org/wiki/4G.

[3] Evolution and Standardization of Mobile Communications Technology, *The 1G (First Generation) Mobile Communications Technology Standards* , international journal, EISBN13: 9781466640757, May, 2013.

[4] Seyed Hossein Ahmadpanah, et al, *4G Mobile Communication Systems: Key Technology and Evolution*, [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1606/1606.05477.pdf, 2016.

[5] Sharmila, *A Review of Wireless Mobile Technology*, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391.

[6] Subharthi Paul, *Long Term Evolution (LTE) & Ultra-Mobile Broadband (UMB) Technologies for Broadband Wireless Access*, A survey paper written under guidance of Prof. Raj Jain, [Online]. Available: http://www.cse.wustl.edu/~jain/cse574-08/ftp/lte.pdf, 2014.

[7] (2013) the androidauthority website. [Online]. Available: http://www.androidauthority.com/4g-lte-guide-146347/.

[8] (2013) Alcatel.Lucent website. [Online]. Available: http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf.

[9] Media Centre, *ITU paves way for next-generation 4G mobile technologies, ITU-R IMT-Advanced 4G standards to usher new era of mobile broadband communications*, ITU annual report, 2010.

[10] Hina Firdaus, *4G LTE Network Growth in India and Security Issue in Network*, B.Tech CSE, (M.Tech CSE) Jamia Hamdard University, New Delhi-62 7827261428, IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.11, November 2016.

[11] Vikas Kaula, et al, *Next Generation Encryption using Security Enhancement Algorithms for End to End Data Transmission in 3G/4G Networks*, 7th International Conference on Communication, Computing and Virtualization 2016.

[12] Weidong Fang, et al, *Information Security of PHY Layer in Wireless Networks*, Journal of Sensors, Volume 2016 (2016).

[13] Prof. D. G. Vyawahare, et al , *A Survey on Security Challenges and Solutions in Cloud Computing*, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 3, March 2016.

[14] Senthilkumar Mathi, et al, *Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme*, Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016).

[15] Kire Jakimoski, *Security Techniques for Data Protection in Cloud Computing*, International Journal of Grid and Distributed Computing, Vol. 9, No. 1 (2016).

[16] Krishna Prakash, et al, *SECURITY ISSUES AND CHALLENGES IN MOBILE COMPUTING AND M-COMMERCE*, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015.

[17] Kaleem Ullah, M.N.A. Khan, *Ensuring Data Confidentiality and Authentication through Encryption at Application Layer*, International Journal of Security and Its Applications Vol.9, No.11 (2015).

[18] (2013) Alcatel.Lucent website. [Online]. Available: http://library.ahima.org/doc?oid=104090#.WKe3Lm997IV.

[19] Warwick Ashford, *Six security issues to tackle before encrypting cloud data*, 22 Mar 2013 15:35 http://www.computerweekly.com/news/2240180087.

[20] Ali I. Gardezi, "Security in Wireless Cellular Networks", April 23, 2006, http://www.cs.wustl.edu/~jain/cse57406/ftp/.

[21] (2013) McAfee website. [Online]. Available: http://www.webtorials.com/main/resource/papers/McAfee/paper20/7-deadly-threats-4g.pdf.

[22] Alyaa Ghanim Sulaiman, et al, *Comparative Study on 4G/LTE Cryptographic Algorithms Based on Different Factors*, International Journal of Computer Science and Telecommunications [Volume 5, Issue 7, July 2014].

[23] 3GPP Task Force, ETSI/SAGE Specification, "*Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 1: 128-EEA3 and 128-EIA3 Specification*", Version: 1.7, Date: 30th Dec, 2011.

[24] Ghizlane Orhanou, et al, The New LTE Cryptographic Algorithms EEA3 and EIA3 Verification, Implementation and Analytical Evaluation, Applied Mathematics & Information Sciences. An International Journal, http://dx.doi.org/10.12785/amis/070631. Received: 22 Mar. 2013, Revised: 22 Jul. 2013, Accepted: 25 Jul. 2013 Published online: 1 Nov. 2013.

[25] A. Lenstra, and E. Verheul, Selecting Cryptographic Key Sizes, Journal of Cryptology 14 (2001) 255-293.

