Indian Journal of Science and Technology, Vol 9(45), DOI: 10.17485/ijst/2016/v9i45/106147, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Security Architecture for the Cloud Integrated Internet of Things

V. Kamalakannan* and S. Tamilselvan

Department of Electronics and Communication Engineering, Pondicherry Engineering College, Pillaichavadi, Puducherry – 605014, India; vkamalakannan@pec.edu

Abstract

Objectives: To design efficient hybrid architecture for data security is applied for securing communication link between two user/senders by considering symmetric key algorithm and asymmetric key algorithm. **Methods/ Analysis:** A highly efficient architectures for data security is applied for securing communication link between two user/senders in cloud integrated Internet of Things (IoT). Data is encrypted with Advanced Encryption Standard (AES) algorithm and Elliptical Curve Cryptography (ECC) concept is used for securing the secret key between user/ sender and system/receiver. In this architecture authentication is provided by Elliptic Curve Diffie Hellman algorithm between user/sender and system/receiver. The efficient hybrid architecture is implemented on Field Programmable Gate Array (FPGA) and is scripted in verilog Hardware Description language (HDL).**Findings:** According to the IoT concept, Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) meet new challenges related to large volume of data. The physical things in an IoT are generally identified by WSN or RFID before connecting with each other. Once identified, they can interchange data between them. Cloud computing provides virtual infrastructure for storing, analyzing, and virtualization large data in client delivery. Data transferring like storing and retrieving from cloud by different user/senders should be secure from Men in the Middle (MIM) attack of information. The outcomes obtained shows that the efficient cryptosystem with encryption and decryption has a minimum period of 18.060ns with the maximum achievable frequency of 55.371MHz on Xilinx Virtex-5 (XC5VLX50T-1FF1136).**Novelty/ Improvement:** In this paper ECC algorithm is for providing security communication between user/senders and system/receiver. ECC encryption is used for encrypting the request of user/senders connected to the receiver. The file in the system/receiver is accessed by the user/sender and the file is encrypted by system/receiver using user/ sender's public key. When uploading the files system/receiver encrypts the file using AES encryption algorithm or while downloading the file from data storage the system/receiver decrypts the data or file using AES algorithm.

Keywords: Advanced Encryption Standard (AES), Cloud Computing, Elliptic Curve Cryptography (ECC), Elliptic Curve Diffie-Hellman-Merkle, Internet of Things (IoT), Key Exchange

1. Introduction

The IoT was introduced by Kenn Ashton in 1999 based on principle of internet evolution of the idea of IoT evolved[1]. It is assumed by the end of 2020 about billions of devices would be connected among each other[2]. IoT is an intelligent network present over the internet. In future people will be having different types of devices and there have to be connected in IoT infrastructure[3]. The impact of IoT is generally visioned as network centric or internet centric and things centric or object centric having their own architectures. Network architecture in IoT is generally the identity of the object, whereas object architecture is nothing but objects allotted to networks. The intelligence present in the devices should perform their responsibilities to counteract threats. Instead of searching for a solution, proposing an approach to security for IoT[4]. In cloud computing authenticating the user/senders is also very much needed apart from encryption of data[26,28]. Considering the threats, some improved techniques

*Author for correspondence

are applicable for the performance enhancement in the security architecture related to cloud computing. In this paper data to be transferred in cloud integrated IoT are encrypted with AES algorithm. ECC concept is used for securing the secret key between user/sender and system/receiver[29]. In this architecture authentication is provided by Elliptic Curve Diffie Hellman algorithm between user/sender and system/receiver. Section II gives an overview of IoT Characteristics, a brief description about the IoT elements is provided in section III and application areas of IoT provided in section IV. Supporting technologies of IoT is explained in section V with security threats and challenges in Cloud and IoT in section VI. The IoT architecture is illustrated in section VII and security architecture is illustrated in Section VIII. Based on the security architecture a model is proposed in section IX,cryptographic algorithms are discussed in section X. An implementation example is considered in section XI. Finally summary and conclusions arrived in section XII and section XIII. Section XIV discusses the future work and are followed by references.

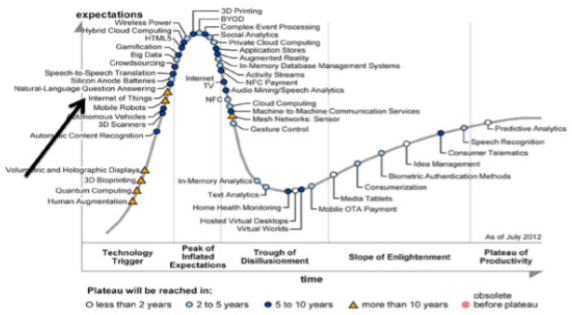

Figure 1. Gartner's hype cycle.

2. IoT Characteristics

The IoT concept is derived from sensor network and RFID where long distance identification and process of data is performed. In 2005, International Telecommunication Union released report on "IoT"[5]. It is a global network connecting physical and virtual objects using object identifier sensors as the basis. I future it challenges security and privacy of end user/senders[6]. Basically partial techniques of IoT such as RFID, sensor technology are referred for security issues. The IoT definition is not defined properly and is difficult to arrive with a standard definition[7]. IoT is one of the technology emerging in IT which is given in Gartner's IT hype cycle in the Figure 1[8].Due to limitations related to connectivity, IoT is significantly different from the present distributed system. As the number of devices integrated are increasing in the network, monitoring becomes difficult[9]. In IoT simple devices also have to be managed due to different computational capabilities. A wide wireless network has to be developed such as Wi-Fi, ZigBee, and WiMAX etc[10].

3. IoT Elements

All the integral parts of IoT are generally referred as IoT elements. The IoT technology or elements used are RFID, Near Field Communication (NFC) and Wireless Local Area Network (WLAN). Basically there are three IoT elements, which are hardware, middleware and presentation tools. Identifying 'things" is very important for the IoT success as unique identity of billions of devices in internet is necessary and firstly the RFID was being used to determine the objects at a distance and communicate with it, later NFC was considered due to limitations in RFID[11]. In NFC there is no limitations in distance. Nowadays for IoT technology WLAN with object identity is used for communication. The data are to be stored and intelligently used for smart devices using artificial intelligence algorithms to show interoperability, integration and adaptive communication, which presents the middleware of the IoT[12]. Visualization is also very important element for the interaction of user/senders. It is known that IPv4 supports limited no of computers with IP address but in IoT this is not recommended due to large no of IP address allotment for objects is required. IPv6 having 128 bit address scheme is used in IoT techniques as it can generate billions of IP address for objects to be connected in a network, IPv6 also provides end to end encryption to the communication link[13]. The advancement in technology has resulted in development of devices with ability to sense, compute and communicate wirelessly, which are known as WSN.

4. Application Areas of IoT

Recently IoT is being implemented in so many fields or sectors in support to the life of the human beings. IoT assists number of applications applicable to the existence of humans but only few of them are currently applied as shown in the Figure 2. Few of the implementation fields are health care, agriculture services, weather monitoring, etc.

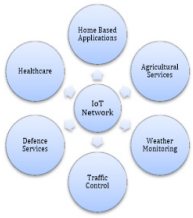

Figure 2. Application of IoT.

The IoT concept target is in the formation of smart items, smart cities, smart living by forming smart autonomous devices[14,15]. Few examples of applications being categorized as personal, social, enterprises, industry and transportation. The next era of application in communication is IOT technology which will be working beyond its domain. The IoT will interconnect and exchange between the devices information and data. For its efficiency lots of effective security should be ensured with confidentiality, integrity, authentication and access control. As IoT is developing, sensor networks and RFIDs are becoming important part or feature of the IoT architecture. RFID is a technology to identify an object through RF signal. It is highly efficient in identifying objects or things, thereby it is a necessity for IoT[16]. The sensor network in the IoT is generally Wireless Sensor Network and is usually used for finding the changes in the things connected to the IoT. It converts the analog data to specific location by applying techniques related to wireless communications.

5. Supporting Technologies of IoT

With the development of advanced technologies such as smart phone, sensors, cloud computing, networking, devices can connect with one another anywhere, anytime and with anything. The technologies supporting IoT are wireless technologies like WSN and RFID with network and communication technologies like wireless and wired technologies related to ZigBee, GSM, UMTS, Wi-Fi and Bluetooth. The IoT concept consist of individual devices and services interconnecting these devices to exchange information with the innovation in RFID and WSNs. The mechanisms involving these in IOT can connect with each other anytime, anywhere and in every form. As the application of IoT increases, several security issues arises due to connection of everything with each other which literally increases security weakness. Thus intruders exploit this weakness. Apart from these various restrictions on capability of the devices connected makes the security protocols like cryptography mechanisms insufficient. Therefore security must be very robust for >20 years of life cycle. Thus new technologies should be developed in terms of security and reliability in IoT architecture[18].In IoT user/senders and their environment are also connected with connection between the devices and connection between the user/senders.

6. Security Threats and Challenges in Cloud and IoT

In IoT people, objects, software and hardware all are interconnected to communicate in trusted network. Therefore issues like user/sender privacy, business processes, confidentiality and third party dependability arises and are generally bounded with problems[24] and has to be secured. Based on these vulnerabilities IoT faces both active and passive attacks which can originate externally or internally. The main threat IoT faces are Denial of Service (DoS)attacks where network resources is made unavailable to the user/senders by jamming channels and stopping distribution of node information. In IoT huge number of devices are connected together to exchange information. Here each and every device has its own security and privacy requirements and few challenges related to security of the devices connected in IoT are specified assure/sender privacy, data protection, identity management, trust management, Policy integration, access control, authentication, authorization and end-to-end security. The main concept in cloud computing is for user/senders concern in reducing complexity and enhancing handling capability of cloud[28,29]. But there are many problems related to data security and connections as there are different models like public, private and hybrid clouds having various characteristics of on demand service with ubiquitous access of network. Cloud computing has several challenges and risks such as data segregation, recovery with long term viability[30]. In cloud computing one should ensure confidentiality, authentication, integrity and availability and for these the encryption of data, authentication, and intrusion prevention with detection and physical security solutions should be provided for secure data transmission[26].

7. IoT Architecture

IoT architecture depends on interoperability of heterogeneous systems. Security architecture is built for IoT based on the security deficiency. Well defined architec-

ture influences sustainable development of IoT. In this paper analysis on the security of the layers of IoT is performed. IoT is generally seen as three layer architecture consists of perception layer, network layer and application layer shown in the Figure 3[19]. The lowest layer in the IoT, perception layer captures and identifies the device's information with the help of RFID tags and sensors and passes the information to the network layer. In the network layer processing and transmission of the information is done. The information is available from the perception layer. This layer also supports the application layer.

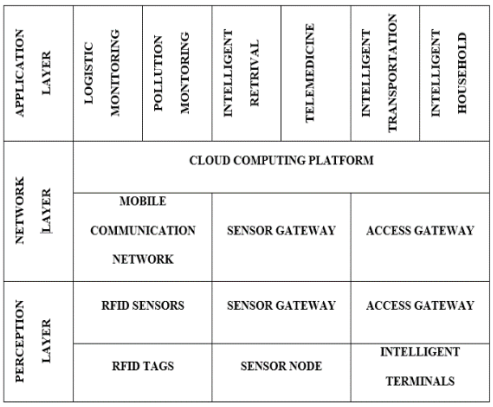

Figure 3. IoT architecture.

Application layer processes huge data by segregating it as it is available from different types of sources. In this layer information is being managed by cloud computing and data mining. In IoT realization of intelligent sense based on information acquisition, capture and identification is preferred under acquisition hierarchy which consists of sensors, RFIDs, wireless communications, etc. the acquisition hierarchy security issues relates to confidentiality and integrity of data information. The security in the network hierarchy plays an important role in the data transmission in IoT. The role network hierarchy plays is transmission of data in access layer and core layer (two parts of the network layer). The core problem in the network hierarchy is the identity allocation to the devices which is being solved by using IPv6 technology. The application hierarchy applies the security in the data processing in IoT. This hierarchy realizes communication between network hierarchy and application services in IoT. The application hierarchy mainly consists of different applications which generates restricted access in security of information processing and are very difficult to overcome.

8. Security Architecture of IoT

IoT is considered as an extension of internet, therefore security concept of internet are applicable to the IoT also[20, 21]. But the problem is in applying the internet security to the IoT is that the devices are of different environment with different computational power, thereby a uniform security approach is not possible in IoT. Hence security architecture is generally used for security problems in the layers such as physical security, information transmission security, information acquisition security, information processing security[22]. Therefore security architecture is divided into four layers shown in Figure 4 where equipment's in the perception layer's physical security is considered with sensor networks security in the network layer and data support security in the application layer.

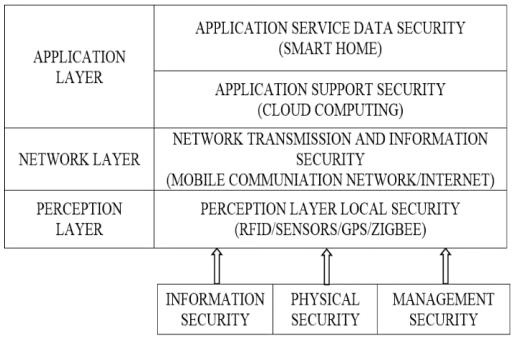

Figure 4. Security architecture.

Due to security threats in the perception layer a secure cryptography algorithm is applied for the security of data, authentication of nodes with secured routing. Network layer is divided into two as access layer and core layer. Access layer may be wired or wireless having multiple access methods accessing heterogeneity. Due to this the switching technology in the open interface it is possible to capture, modify, detect, and retransmit information through radio interface. Core access vulnerabilities is large number of nodes present in IoT is exploited by intruder generating denial of service attack and thereby blocking the network. In the application layer different applications are integrated and requirement differs for a particular data causing data leakage with unwanted access of information. The IoT should consider these three layers to improve security. ECC algorithm prevents data from untrusted access in the perception layer, combined public key and private key provides data integrity and confidentiality of the encrypted data in the network layer. At the

application layer user/senders are ensured they log to the specific services by ensuring non repudiation.

9. Proposed Model for Cloud Security in the Network Layer of Iot

In the proposed model ECC encryption decryption is applied for securing communication[31] and AES for securing file[32] and authentication[33] is provided by using Diffie Hellman (DH) Key Exchange concept. In cloud computing user/senders have to exchange information through a secured communication connection between the main system/receiver and user/senders[21]. Data storage devices are also referred as servers therefore servers are not dedicated separately and are present in cloud computing[22,28]. Access the data from the servers by different user/senders are through system/receiver are represented in Figure 5.In this model ECC algorithm is for providing security communication between user/senders and system/receiver. ECC encryption is used for encrypting the request of user/senders connected to the receiver. The receiver's general public key is applied for encrypting the request. The request is decrypted by system/receiver using its private key[32,34].

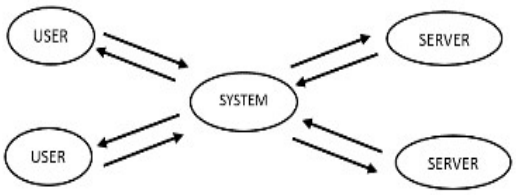

Figure 5. Communication model of cloud.

The file in the system/receiver is accessed by the user/sender and the file is encrypted by system/receiver using user/sender's public key. The user/senders can transmit or receive data files once connected with the system/receiver. When uploading the files system/receiver encrypts the file using AES encryption algorithm or while downloading the file from data storage the system/receiver decrypts the data or file using AES algorithm. In this model 128 bit key is applied for AES to perform encryption. The key is generated randomly. This paper ECC algorithm is applied for key management by encrypting and sharing the AES key with the sender and receiver.

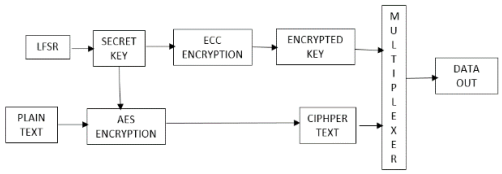

Figure 6. Block diagram of the user/sender.

The AES performs the encryption/decryption of the data. These algorithms combined guarantees data security and is shown in the Figure 6 for transmission of data after performing encryptions and the reverse process after receiving the data in receiver is shown in Figure 7.

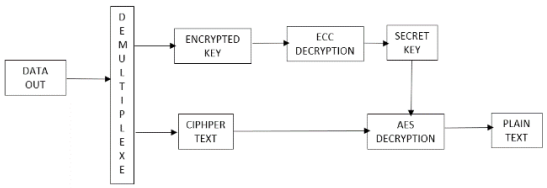

Figure 7. Block diagram of the system/receiver.

The AES encrypts the plain text to cipher text using Key. This is shared between the sender and receiver using Elliptic Curve ElGamal algorithm. The cipher text and key data and are transmitted to the receiver. The receiver performs the inverse operation of decryption of cipher text and Key.

10. Cryptography Algorithm

Cryptographic algorithm are used to achieve security, and are generally of two types i.e., symmetric key encryption using private key for cryptography and asymmetric key encryption using public and private key for cryptography. Symmetric key cryptographic algorithm are generally having speed of execution faster than asymmetric key encryption methods. Asymmetric keys are known as public key and are used in session key exchanges or authentication between user/sender and system/receiver whereas symmetric key are known as private key and are used for encrypting data in communication.

10.1 ECC

ECC is a public key encryption scheme introduced by Neil Koblitz[35] and victor Miller[36] in 1985. This cryptosystem is alternate to RSA[25,26]. The security provided by RSA can be provided by ECC with much smaller key size. Elliptic

Curves have been used in integer factorization and have played an important role in solving the famous problem known as Fermat's last theorem. ECC is now accepted commercially by ANSI, IEEE and NIST and ISO. Lots of research is done on security strength and implementation of Elliptic Curve Cryptography. Cryptosystems using EC are generally depending on the complexity of ECDLP[17]. The asymmetric encryption system based on ECC are Elliptical Curve ElGamal Algorithm and Elliptical Curve Menezes-Vanstone Algorithm[23]. The finite fields in Elliptical Curve are prime field GF (p) and GF (2^m). An Elliptical Curve E over the finite field GF (p) satisfies the equation 2 where a, b ∈ GF (p) and over the binary field GF (2^m) satisfy the equation 3 where a, b ∈ GF (2^m) and b≠0.

$$4a^3 + 27b^2 \neq 0 \quad (1)$$

$$y^2 = x^3 + ax + b \bmod p \quad (2)$$

$$y^2 + xy = x^3 + ax + b \bmod p \quad (3)$$

There are several arithmetic operations in finite field and affine coordinates system in EC are given by point addition and point doubling where

$$P = (x_1, y_1) \epsilon E \quad (4)$$

$$Q = (x_2, y_2) \epsilon E \quad (5)$$

$$-P = (x_1, x_1 + y_1) \epsilon E \quad (6)$$

If $P = Q$ Elliptical Curve point doubling happens and if $P \neq Q$ Elliptical Curve point addition happens. Scalar multiplication in ECC is very important operation and is generally specified by equation 7 where k is a random number generally an integer and p is point on the elliptic curve.

$$kP = P + P \ldots\ldots\ldots + P \ (k \ times) \quad (7)$$

10.2 Elliptic Curve Diffie–Hellman–Merkle Key Exchange Scheme

The method is applied for user/senders, system/receiver and servers present in Cloud Computing architecture by considering prime field in the Elliptic Curve. Here the user/sender and system/receiver in the cloud select a finite prime field F_q by considering $q = p^r$ and a base point or generator point (G). All the three base point G, p and q are publicized by the Certificate Authority and is shown in Figure 8. The user/sender/sender generates a secret number R_S randomly and calculates $P_S = R_S G \epsilon$ E and transmits it to the system/receiver. System/receiver generates secret number R_R randomly and calculates $P_R = R_{R^*} G \epsilon$ E and transmits it to the user/sender. The user/sender receives P_R from system/receiver and multiplies with its secret number to generate $K_S = R_S * P_R$. The system/receiver receives P_S from user/sender and multiplies with its secret number to generate $K_R = R_R * P_S$. Comparison of K_S and K_R are performed and specified in equation 8.

$$K_S = R_S{}^* P_R = R_S{}^* (R_R{}^* G) = (R_S{}^* G)^* R_R = R_R{}^* P_S = K_R \quad (8)$$

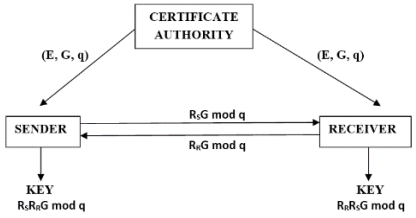

Figure 8. Elliptic curve diffie-hellman-merkle key exchange scheme.

From the comparison a common key K is used for securing the information in the unsecured communication link.

10.3 Elliptic Curve ElGamal Encryption Scheme

The well-known ElGamal cryptosystem has a conventional Elliptic Curve analog. The cryptosystem's issues are related to information exchange between system/receiver and user/sender but have previous Elliptic Curve generator point and public keys of each other[40]. Referring to the generator point P=G=(x, y) generating by the Elliptic Curve Diffie–Hellman–Merkle Key Exchange, the scalar multiplication is performed to generate 2P, 3P....., 233P. The scalar multiplication is performed by point addition and point doubling process[27]. The ASCII characters are mapped to the scalar multiplied points which is specified in Table 2[42,43]. The message from user/sender is mapped with the elliptic curve generated points and encrypted using the Elliptic Curve ElGamal Encryption Scheme shown in the Figure 9.As shown in the Figure 9 the user/sender computes $(M+R_S{}^*(R_R{}^*G))$ and the encrypted message from user/sender is represented as $(R_S{}^*G, M+R_S{}^*(R_R{}^*G))$[42].

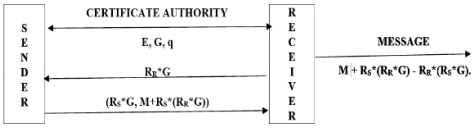

Figure 9. Elliptic curve elgamal cryptosystem.

The system/receiver considering its secret key R_R computes $R_R*(R_S*G)$. The encrypted message received from user/sender is decrypted by the system/receiver to get the original key M as $M+ R_S*(R_R*G)-R_R*(R_S*G)$. The intruders can access the key only when they solve ECDLP.

10.4 AES

The AES is referred as US.FIPSPUB 197 by National Institute of Standards and Technology (NIST)[38] and has become popular and standard specifying Rjindael algorithm[37]. The standard AES processes encrypts 128 bits of data using different key sizes[41]. The basic operation is represented in Figure 10 for encryption and decryption of data. The sequence are shown as Blocks. A sequence of 8 bits are single entity which is basic for processing AES[39]. In the AES input and output blocks with state is 128 bits. The size of the cipher key is 128 bits and is denoted by NK-8 and performs 10 rounds for 128 bits key. For encrypting and decrypting process in this standard 4 byte oriented transformation steps are followed namely Byte Substitution, Shift Rows, Mix Column and Add Round Key. It also has an important function named Key Expansion

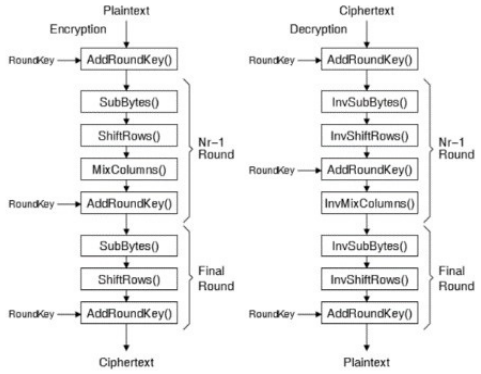

Figure 10. Encryption and decryption of AES.

Byte Substitution: This process is generally based on the concept of dividing the 128 bits of data into 4 by 4 array consisting 16 bytes. Here each and every byte is substituted by corresponding S-Box values.

Shift Rows: It is a simple process of shifting the rows of the 4 by 4 array. Here no shift operation is performed for the first row whereas the second row is shifted by 1 byte towards left, third row of the array is shifted two bytes toward left and the fourth row is shifted by 3 bytes towards left.

Mix Column: In this process an array (x^3+x^2+x for example) is selected for multiplying using modulo $x^4 + 1$ with respect to each column. Generally this process is executed in the last stage.

Add Round Key: Generally here an ex-or operation is performed bit wise for the block and the round key.

The 4 byte oriented transformation steps are repeated 10 number of times for a 128 bits key size. Key expansion process is performed on the initial key of 128 bits and expands the key a 16 bytes to generate 160 bytes for 10 rounds with 16 bytes round key depending on values of keys generated in preceding step. AES decryption is the reverse operation of each of transformation. The decryption process is similar to encryption process with changes in the key schedule. In the process inverse-shift row, inverse-byte sub are interchanged with add round key and inverse mix column interchange. Hence from the cipher text the information is obtained.

11. Implementation Example

An example of the proposed model is implemented on FPGA by coding the process in Verilog HDL. A Linear Feedback Shift Register (LFSR) is designed to generate a random number of 128 bits to be used as the secret key for encryption and decryption in AES. The value generated by LFSR is represented by ASCII equivalent characters. The 128 bits of data to be encrypted is represented in the hexadecimal form as 35 7E 22 CD 4B F0 99 00 AD DD 4F 37 0A 56 3D 01. The Key is divided into 16 blocks of ASCII values and is provided in equation 9.

K=M&0[1A4+f6@l196E (9)

Considering the ECDHM key exchange concept an elliptic curve E is selected as

E\F$_{233}$: $y^2 = x^3 + x + 17 \ mod \ 233$ by considering a=1, b=17 and p =233.

It is also found the $4a^3 + 27b^2 \neq 0$ i.e., $4(1)^3 + 27(17)^2 \neq 0$

Thus for the selected elliptic curve the points on the curve are found and is specified in the Table 1

The secret key of the sender/user is generated randomly i.e., $R_S = 13$.

The secret key of the receiver/system is generated randomly i.e., $R_R = 25$.

From the points on the curve a particular base point P is selected as P= (18, 43) $\in$ E (F_{233})

Table 1. Points on the curve

Points	Points on the elliptic curve				
1-5	(66,0)	(113,1)	(104,2)	(81,3)	(101,6)
6-10	(196,8)	(91,10)	(52,11)	(111,15)	(96,18)
11-15	(57,21)	(98,23)	(169,24)	(228,23)	(168,26)
16-20	(156,27)	(51,28)	(60,31)	(126,33)	(170,32)
21-25	(149,33)	(191,33)	(62,34)	(61,35)	(114,37)
26-30	(125,37)	(227,37)	(77,39)	(78,40)	(79,41)
31-35	(18,43)	(130,42)	(127,45)	(74,49)	(10,51)
36-40	(195,51)	(147,52)	(42,55)	(67,57)	(106,59)
41-45	(116,60)	(150,60)	(210,60)	(90,61)	(186,63)
46-50	(211,63)	(16,64)	(183,65)	(137,67)	(204,70)
51-55	(134,70)	(20,72)	(12,73)	(54,73)	(177,73)
56-60	(132,74)	(155,76)	(56,79)	(179,79)	(231,79)
61-65	(58,80)	(171,85)	(25,89)	(199,89)	(176,90)
66-70	(148,95)	(85,99)	(108,101)	(119,101)	(120,102)
71-75	(36,103)	(4,107)	(181,107)	(8,108)	(72,108)
76-80	(35,109)	(219,109)	(1,112)	(30,112)	(46,114)
81-85	(46,119)	(1,121)	(30,121)	(219,124)	(72,125)
86-90	(4,126)	(181,126)	(36,127)	(120,131)	(108,132)
91-95	(119,132)	(85,134)	(148,138)	(176,143)	(25,144)
96-100	(199,144)	(73,147)	(171,148)	(58,153)	(179,154)
101-105	(231,154)	(132,159)	(2,160)	(54,160)	(177,160)
106-110	(20,161)	(128,163)	(204,163)	(37,166)	(183,168)
111-115	(16,169)	(186,170)	(211,170)	(90,172)	(116,173)
116-120	(150,173)	(200,173)	(106,174)	(147,181)	(10,182)
121-125	(195,182)	(35,84)	(74,184)	(122,188)	(214,189)
126-130	(18,190)	(130,191)	(79,192)	(78,193)	(77,194)
131-135	(114,196)	(62,199)	(126,200)	(149,200)	(191,200)
136-140	(168,201)	(170,201)	(51,205)	(159,206)	(169,209)
141-145	(228,210)	(57,212)	(127,213)	(96,215)	(111,218)
146-150	(152,221)	(52,222)	(91,223)	(19,224)	(196,225)
151-155	(101,227)	222,229)	(81,230)	(104,231)	(113,232)
156-157	(66,233)	(0,233)			

The user/sender then calculates (R_S*P) mod p = 13(18, 43) mod 233 = (41,162) and transmits it to the system/receiver.

The system/receiver then calculates (R_R*P) mod p = 25(18, 43) mod 233 = (123, 88) and transmits it to the user/sender.

The user/sender receives (R_R*P) mod p = (123, 88) and generates 13 (123, 88) = (56, 79)

The system/receiver receives (R_S*P) mod p = (41, 162) and generates 25 (41, 162) = (56, 79)

This base point generated by the concept of key exchange is shared between the user/sender and the system/receiver to encrypt and decrypt the secret key.

The shared base point P = (56, 79) = G is considered as the generator point and corresponding scalar multiplication is performed to obtain 2P, 3P…… up to 128P and the

Table 2. Mapping of ASCII characters

P=(56,79)=NULL	2P=(20,113)=SOH	3P=(68,10)=STX	4P=(11,70)=ETX	5P=(194,173)=EOT
6P=(113,43)=ENQ	7P=(36,31)=ACK	8P=(95,5)=BEL	9P=(100,118)=BS	10P=(85,167)=HT
11P=(117,226)= LF	12P=(43,144)=VT	13P=(159,203)=FF	14P=(52,219)=CR	15P=(185,9)=S0
16P=(71,93)=S1	17P=(198,37)=DLE	18P=(33,115)=DC1	19P=(98,7)=DC2	20P=(38,121)=DC3
21P=(15,136)=DC4	22P=(169,203)=NA	23P=(160,44)=SYN	24P=(154,8)=ETB	25P=(99,159)=CAN
26P=(29,20)=EM	27P=(132,126)=SUB	28P=(185,178)=ESL	29P=(116,144)=FS	30P=(211,91)=GS
31P=(97,232)=RS	32P=(75,166)=US	33P=(203,45)=space	34P=(142,37)=!	35P=(192,215)=“
36P=(225,195)=#	37P=(100,59)=$	38P=(158,32)= %	39P=(32,47)=&	40P=(157,112)=‘
41P=(122,54)=(	42P=(177,184)=)	43P=(182,10)=*	44P=(152,47)=+	45P=(51,230)=,
46P=(225,16)=-	47P=(28,167)=DOT	8P=(183,127)=/	49P=(110,7)=0	50P=(230,67)=1
51P=(203,132)=2	52P=(51,84)=3	53P=(127,225)=4	54P=(223,107)=5	55P=(25,42)= 6
56P=(34,58)=7	57P=(51,127)=8	58P=(226,70)=9	59P=(165,205)=:	60P=(165,33)=;
61P=(119,187)=<	62P=(163,42)= =	63P=(166,118)= >	64P=(188,90)=?	65P=(78,191)=@
66P=(196,45)=A	67P=(222,181)=B	68P=(173,198)=C	69P=(29,56)=D	70P=(124,152)=E
71P=(15,222)=F	72P=(68,12)=G	73P=(35,95)=H	74P=(230,160)=I	75P=(194,146)=J
76P=(109,30)=K	77P=(181,230)=L	78P=(28,58)=M	79P=(135,153)=N	80P=(190,116)=O
81P=(187,130)=P	82P=(19,166)=Q	83P=(130,95)=R	84P=(143,94)=S	85P=(3,131)=T
86P=(27,124)=U	87P=(202,19)=V	88P=(213,34)=W	89P=(227,117)=X	90P=(42,28)=Y
91P=(89,153)=Z	92P=(26,143)=[	93P=(23,37)=/	94P=(177,66)=]	95P=(63,226)=^
96P=(123,103)= _	97P=(62,9)=‘	98P=(113,196)=a	99P=(176,202)=b	100P=(190,230)=c
101P=(78,84)=d	102P=(157,164)=e	103P=(189,19)=f	104P=(39,74)=g	105P=(101,223)=h
106P=(79,227)=i	107P=(172,218)=j	108P=(57,113)=k	109P=(111,148)=l	110P=(146,21)=m
111P=(152,45)=n	112P=(164,95)=o	113P=(231,223)=p	4P=(131,106)=q	115P=(174,9)=r
116P=(87,37)=s	117P=(191,149)=t	118P=(21,143)=u	119P=(97,67)=v	120P=(187,18)=w
121P=(62,123)=x	122P=(10,49)=y	123P=(104,224)=z	124P=(15,141)={	125P=(155,173)=|
126P=(157,115)=}	127P=(22,60)=~	128P=(97,134)=DEL		

ASCII characters are mapped to the corresponding points as provided in Table 2

Now considering the Elliptic Curve ElGamal algorithm the secret key of the AES is encrypted block by block. The secret key consists 16 blocks of ASCII values mapped as M:(28,58) ; &:(32,47) ; 0:(110,7) ; [:(26,143) ; 1:(230,167) ; A:(196,45) ; 4:(127,225) ; +:(152,47) ; f:(189,19) ; 6:(25,42) ; @:(78, 191) ; l:(111,148) ; 1:(230,67) ; 9(226,70) ; 6:(25,42) ; E:(124,152).

The secret key represented by points are encrypted by considering the secret key of the user/sender is generated randomly i.e., $R_S = 13$ and the secret key of the receiver/system is generated randomly i.e., $R_R = 25$. Encrypted points of the secret key for the generator point (56, 79) is split into K_i (I ranges from 1 to 16) and sent to the receiver.

$(C1, C2) = (R_S*G, M+R_S*(R_R*G)$

For K_1 = (28, 58) => [C1, C2] = [(143, 109), (174, 91)]

For K_2 = (32, 47) => [C1, C2] = [(143, 109), (101, 12)]

For K_3 = (110, 7) => [C1, C2] = [(143, 109), (93, 115)]

For K_4 = (26, 143) => [C1, C2] = [(143, 109), (218, 45)]

For K_5 = (230, 167) => [C1, C2] = [(143, 109), (207, 4)]

For K_6 = (196, 45) => [C1, C2] = [(143, 109), (93, 114)]

For K_7 = (127, 225) => [C1, C2] = [(143, 109), (12, 82)]

For K_8 = (152, 47) => [C1, C2] = [(143, 109), (231, 0)]

For K_9 = (189, 19) => [C1, C2] = [(143, 109), (101. 114)]

For K_{10} = (25, 42) => [C1, C2] = [(143, 109), (179, 212)]

For K_{11}= (78, 191) => [C1, C2] = [(143, 109), (130, 148)]

For K_{12} = (111, 148) => [C1, C2] = [(143, 109), (163, 34)]

For K_{13} = (230, 67) => [C1, C2] = [(143, 109), (2074)]

For K_{14} = (226, 70) => [C1, C2] = [(143, 109), (13, 27)]

For K_{15} = (25, 42) => [C1, C2] = [(143, 109), (179, 212)]

For K_{16} = (124, 152) => [C1, C2] = [(143, 109), (98, 48)]

The encrypted data obtained from the AES encryption block is represented in the hexadecimal form as 1A 87 2A DC 3E FF 45 70 01 25 9B 21 BF 00 AC 99. At the receiver the blocks of encrypted secret key is decrypted. The encrypted message [C1, C2] received from user/sender is decrypted by the system/receiver to get the original key M as

$M+ R_S*(R_R*G)-R_R*(R_S*G) = C2- R_R*C1$

For K_1 =>C2- R_R*C1 = [(174, 91)-25*(143, 109)] = (28, 58) = M

For K_2=>C2- R_R*C1 = [(101, 12) -25*(143, 109)] = (32, 47) = &

For K_3 =>C2- R_R*C1 = [(93, 115) -25*(143, 109)] = (110, 7) = 0

For K_4 =>C2- R_R*C1 = [(218, 45) -25*(143, 109)] = (26, 143) = [

For K_5 =>C2- R_R*C1 = [(207, 4) -25*(143, 109)] = (230, 167) = 1

For K_6 =>C2- R_R*C1 = [(93, 114) -25*(143, 109)] = (196, 45) = A

For K_7 => C2- R_R*C1 = [(12, 82) -25*(143, 109)] = (127, 225) = 4

For K_8 => C2- R_R*C1 = [(231, 0) -25*(143, 109)] = (152, 47) = +

For K_9 => C2- R_R*C1 = [(101. 114) -25*(143, 109)] = (189, 19) = f

For K_{10} => C2- R_R*C1 = [(179, 212) -25*(143, 109)] = (25, 42) = 6

For K_{11}=> C2- R_R*C1 = [(130, 148) -25*(143, 109)] = (78, 191) = @

For K_{12} => C2- R_R*C1= [(163, 34) -25*(143, 109)] = (111, 148) = l

For K_{13} => C2- R_R*C1 = [(207, 4) -25*(143, 109)] = (230, 67) = 1

For K_{14} => C2- R_R*C1 = [(13, 27) -25*(143, 109)] = (226, 70) = 9

For K_{15} =>C2- R_R*C1 = [(179, 212) -25*(143, 109)] = (25, 42) = 6

For K_{16} => C2- R_R*C1 = [(98, 48) -25*(143, 109)] = (124, 152) = E

The points are then de-mapped and all are combined together to build back the secret key, K= M&0[1A4+f6@ l196Ewhich is applied to AES decryption to get the original data. The decrypted data from the AES decryption block is represented in the hexadecimal form as 35 7E 22 CD 4B F0 99 00 AD DD 4F 37 0A 56 3D 01.

The block diagram of transmitter and receiver for cloud computing process in the network layer of IoT is shown in the Figure 11 and Figure 12. The architecture is simulated to the get the results for the designed algorithms in the IoT.

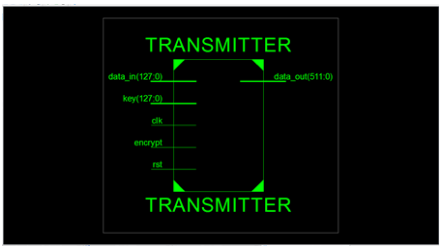

Figure 10. Block diagram of transmitter.

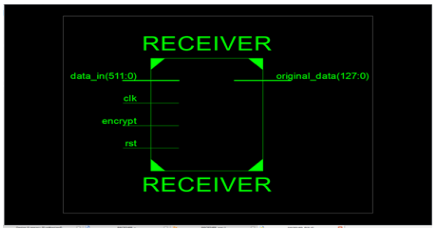

Figure 11. Block diagram of receiver.

The security architecture implemented is shown in Figure 13. The RTL schematic of transmitter and receiver for is shown in the Figure 13 and Figure 14. The transmitter and receiver architecture are simulated to the get the results for the implemented algorithms in the IoT. The simulated results are shown in Figure 15 and Figure 16. The synthesis report is given in the Figure 17.

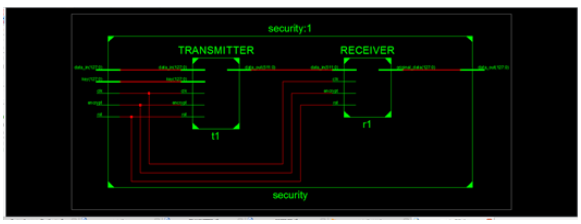

Figure 13. Architecture of security system.

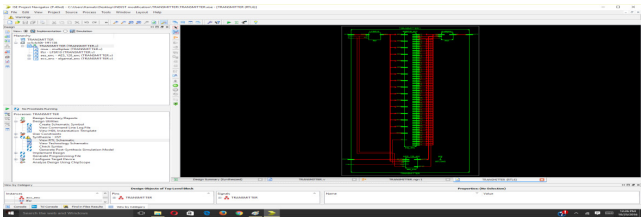

Figure 12. RTL schematic of transmitter.

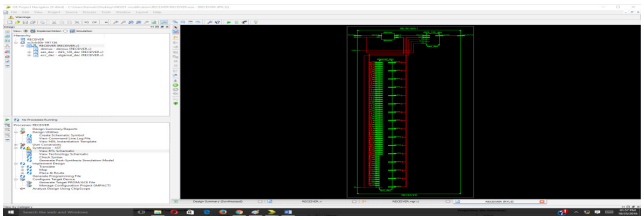

Figure 13. RTL schematic of transmitter.

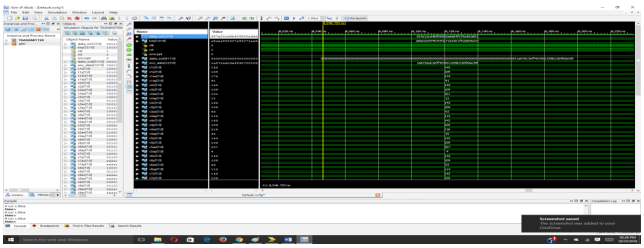

Figure 14. Simulation result of transmitter.

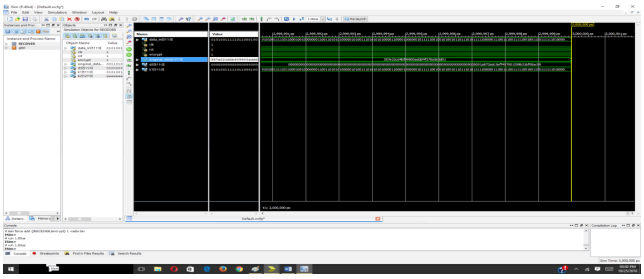

Figure15. Simulation result of receiver.

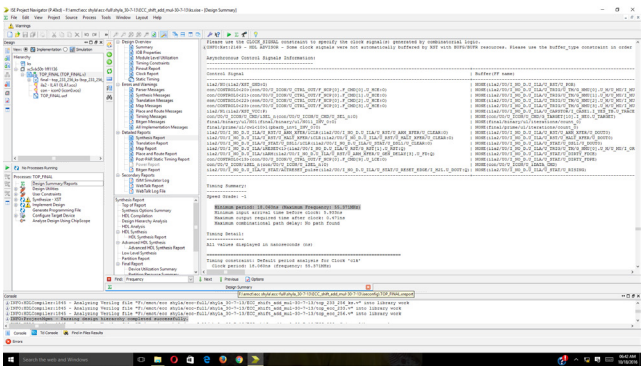

Figure 13. Synthesis report.

12. Summary

In the post – PC era devices are more informative and interactive. In IoT user/senders and things can be connected with anyone, anytime and anywhere. It is a network comprising autonomous devices with interoperable communication protocols. Interface of the devices and user/sender are integrated in network with a unique identity for each other, the IoT architecture makes it possible to be used in different applications applicable to the user/senders in different domains like personal, mobility, transportation etc. To make this possible challenges has to be overcome which are discussed. Therefore to implement IoT, a stronger security protocol should be developed. Lot of research has to be done on IoT to make it a reality. Security plays an important issue and must be considered seriously for personal and business data information being attacked by the intruders. IoT technologies should be identified and classified based on categories supporting IoT vision. Various identifier method should be developed addressing global schemes in identification, encoding and authentication. Challenges involving interoperability of autonomous devices in any network with security authentication and authorization were considered. WSN ability is critical in the IoT realization. Apart from these an efficient, secure computing and storage resources is necessary. Therefore cloud computing promises to deliver next generation services related to data storage. It also acts as receiver analyzing, interpreting the data from sensors. These process of cloud computing are hidden from the user/senders.

13. Conclusion

A security architecture for cloud computing is implemented on FPGA using Elliptical Curve Cryptosystem for securing 128 bits secret key and AES for encrypting files with authentication of user/senders and system/receiver by Elliptic Curve Diffie Hellman Key Exchange. Here decision taking is easy as individual have priority. In this paper IoT security challenges where considered and discussed. The outcomes obtained shows that the cryptosystem with encryption and decryption over GF (p) has a minimum period of 18.060ns with the maximum achievable frequency of 55.371MHz on Xilinx Virtex-5 (XC5VLX50T-1FF1136).

14. Future Work

In future, model can be enhanced by replacing the affine coordinates by projective coordinates in ECC such that the inversion operation in point doubling and point addition is eliminated. Further Elliptic Curve Digital Signature Analysis can be used for authentication of files, Elliptic Curve Diffie Hellman Key Exchange scheme for providing authorization and Elliptic Curve Menezes Vanstone Elliptical Curve scheme for sharing the key with between user/sender and system/receiver. Furthermore security can be improved between system/receiver and servers, servers and server user/sender and user/sender in the Cloud integrated IoT.

15. References

1. Ashton K. IoT. RFID Journal. 2009.
2. Article Title [Internet]. 2016 [Cited 2016 Feb 23]. Available from: http://www.theinternetofthings.eu. Date accessed: 23/02/2016.
3. Buyya R, Gubbi J, Marusic S, Palaniswami M. IoT: A vision, architectural elements, and future directions. Journal of Future Generation computer systems. 2013 Feb; 24(29):1645–60.
4. Article Title [Internet]. 2016 [Cited 2016 Jan 12]. Available from: http://www.boston.com/business/technology/articles/2004/10/25/the_internet_of_things/. Date accessed: 12/01/2016
5. The IoT. International Telecommunication Union (ITU). ITU Internet Report; 2005.
6. Sundmaeker H, Guillemin P, Friess P, Woelfflé S. Vision and challenges for realizing the IoT. Cluster of European Research Projects on the IoT—CERP-IoT; 2010 Mar.
7. Floerkemeier C, Langheinrich M, Fleisch E, Mattern F. The IoT. Lecture notes in computer science. Springer. 2008; 49–52.
8. Rivera J. Gartner says 4.9 billion connected things will be in use in 2015, Gartner [Internet]. 2014 Nov 11[Cited 2016 Mar 01]. Available from: www .gartner.com/newsroom/id/2905717.
9. Buckley J. The IoT: From RFID to the next generation pervasive networked systems. Auerbach Publications: New York; 2006.
10. Aggarwal M, Singh M. Smart city based on NDNoT: The future of IoT. Indian Journal of Science and Technology. 2016 Sep; 9(36):1–8. DOI: 10.17485/ijst/2016/v9i36/89557.
11. Renold AP, Joshi RR. An internet based RFID library management system. Proceedings of International Conference of Information and Communication Technologies. Jeju Island; 2013. p. 932–6.
12. Pescatore J, Securing the IoT survey. White paper, SANS Institute[Internet]. 2014 Jan [Cited 2016 Mar 09]. Available from: www .sans.org/reading-room/white.
13. Roman R, Najera P, Lopez J. Securing the IoT, IEEE Computer. 2011; 44:51–8.
14. Gonzalez G, Organero M, Kloos C. Early in infrastructure of all IoT in space for learning. Proceedings of Eighth IEEE International Conference on Advance Learning Technologies; 2008. p.381–3.
15. Amardeo C, Sarma J. Identities in the future IoT. Journal of Wireless Communication. 2009; 49:353–63.
16. Enabling connected smart cities for a better tomorrow, Elitecore Wi-Fi Service Management Platform(SMP) [Internet]. 2015. Available from: http://www.elitecore.com/downloads/datasheets/wifioffload/Elitecore
17. Rajam STR, Kumar SBR. Enhanced elliptic curve cryptography. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–6. DOI: 10.17485/ijst/2015/v8i26/80444.
18. Wang C, Daneshmand M, Dohler M, Mao X, Hu RQ, Wang H. Special issue on IoT: Architecture, protocols and services. IEEE Sensors Journal. 2013; 13(10):3505–10.
19. Liu Y, Hu W, Du J. Network information security architecture based on IoT. ZTE Communication. 2011; 17(1):17–20.
20. Guo L, Yan B, Shen Y. Study on secure system architecture of IOT. Journal of Information Security and Communications Privacy. 2010; 73–5.
21. Kirubakaramoorthi R, Arivazhagan D, Helen D. Analysis of cloud computing technology. Indian Journal of Science and Technology. 2015 Sep; 8(21):1–3.
22. Shyamala K, Rani TS. An analysis on efficient resource allocation mechanisms in cloud computing. Indian Journal of Science and Technology. 2015 May; 8(9):814–21.
23. Nagaraj S, Raju GSVP. Image security using ECC approach. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–5. DOI: 10.17485/ijst/2015/v8i26/81185.
24. Raza S. Secure communication for the IoT - a comparison of link-layer security and IPSec for 6LoWPAN. Journal of Security and Communication Networks. 2014; 7(12):2654–68.
25. Miller VS. Use of elliptic curves in cryptography. Lecture notes in computer sciences; 218 on advances in cryptology - CRYPTO 85. Springer-Verlag New York, Inc.; 1986.
26. IEEE standard specifications for public-key cryptography. IEEE Std 1363-2000; 2000. p.1–228.
27. Stallings W. Cryptography and network security principles and practices. 5thedn, Pearson Publications; 2011.
28. Buyya R, Broberg J, Goscinski A. Cloud computing principles and paradigms, WILEY Publication; 2011.

29. Agrawal H, Sharma M. Implementation and analysis of various symmetric cryptosystems. Indian Journal of Science and Technology. 2010 Dec; 3(12):1173–6.
30. Miller VS. Use of elliptic curves in cryptography. Proceedings of Crypto85, Lecture note in Computer Science, v. 218, Springer Verlag; 1986. p. 417–26.
31. Shau PK, Chhotray RK, Jena G, Pattnaik S. An implementation of elliptic curve cryptography. International Journal of Engineering Research and Technology. 2013 Jan; 2(1). ISNN: 2278-0181.
32. Rajarajeswari S, Somasundaram K. Data confidentiality and privacy in cloud computing. Indian Journal of Science and Technology. 2016 Jan; 9(4):1–8.
33. Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory. 1976; 22:644–54.
34. Hiremath S, Suma MS. AES implemented on FPGA. Proceedings of Second International Conference on Computer and Electrical Engineering; 2009. p. 656–60.
35. Koblitz N. Elliptic curve cryptosystem. Mathematics of Computation. 1987; 48:203–9.
36. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Laboratory for Computer Science, Massachusetts Institute of Technology, Cam-bridge; 1977 Nov.
37. Ashwini R, Tonde A, Akshay P, Dhande A. Implementation of AES algorithm based on FPGA. International Journal of Current Engineering and Technology. 2014 Apr; 4(2):1048–50.
38. National Institute of Standards and Technology (NIST). Federal Information Processing Standards Publication 197(FIPS PUB 197); 2001.
39. Kamalakannan V, Tamilselvan S. Security enhancement of text message based on matrix approach using elliptical curve cryptosystem. Procedia Materials Science in 2nd International Conference on Nanomaterials and Technologies; 2015. p. 489–96.
40. Kamalakannan V, Tamilselvan S. An efficient crystography protocol using matrix mapping technique. Proceedings of International Conference on Communication and Signal Processing. Melmarvathur; 2015. p. 132–6.
41. Gandh DR, Kamalakannan V, Tamilselvan S, Balamurugan R. FPGA implementation of enhanced key expansion algorithm for advanced encryption standard.Proceedings of International Conference on Contemporary Computing and Informatics. Mysore; 2014. p. 409–13.
42. Balamurugan R, Kamalakannan V, Tamilselvan S, Gandh DR. Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography. Proceedings of International Conference on Contemporary Computing and Informatics. Mysore; 2014. p. 103–6.
43. Kamalakannan V, Tamilselvan S. Implementation of menezes vanstone ECC algorithm using matrix mapping method. Proceedings of International Conference on Communication and Security. Puducherry; 2016 Mar. p. 490–3.