AN IN-DEPTH ANALYSIS OF ADVANCED ENCRYPTION STANDARD (AES) AND ELLIPTICAL CURVE CRYPTOGRAPHY (ECC) ALGORITHM TO ENHANCE THE DATA SECURITY FEATURES AND SAFEGUARDS IN CLOUD COMPUTING, 2019

Drishti Arora

ABSTRACT

To structure effective half and half design for information security is applied for verifying correspondence interface between two clients/senders by thinking about symmetric key calculation and deviated key calculation. An exceptionally effective design for information security is applied for verifying correspondence connect between two clients/senders in cloud coordinated Internet of Things (IoT). Information is encoded with Advanced Encryption Standard (AES) calculation and Elliptical Curve Cryptography (ECC) idea is utilized for verifying the mystery key between client/sender and framework/recipient. In this engineering, verification is given by Elliptic Curve Diffie Hellman calculation between client/sender and framework/beneficiary. The productive crossbreed engineering is actualized on Field Programmable Gate Array (FPGA) and is scripted in Verilog Hardware Description Language (HDL). Discoveries: According to the IoT idea, Radio Frequency Identification (RFID) and Wireless Sensor Networks (WSN) address new difficulties identified with huge volume of information. The physical things in an IoT are commonly recognized by WSN or RFID before interfacing with one another. When distinguished, they can trade information between them. Distributed computing gives a virtual foundation for putting away, examining, and virtualization enormous information in customer conveyance. Information moving like putting away and recovering from the cloud by various client/senders ought to be secure from Men in the Middle (MIM) assault of data. The results acquired shows that the effective cryptosystem with encryption and decoding has a base time of 18.060ns with the most extreme attainable recurrence of 55.371MHz on Xilinx Virtex-5 (XC5VLX50T-1FF1136). In this paper, ECC calculation is for giving security correspondence between client/senders and framework/recipient. ECC encryption is utilized for encoding the solicitation of client/senders associated with the collector. The document in the framework/beneficiary is gotten to by the client/sender and the record is scrambled by framework/recipient utilizing client/sender's open key. While transferring the documents framework/collector encodes the record utilizing AES encryption calculation or while downloading the document from information stockpiling the framework/recipient unscrambles the information or record utilizing AES calculation.

1. INTRODUCTION

The IoT was introduced by Kenn Ashton in 1999 based on principle of internet evolution of the idea of IoT evolved1. It is assumed by the end of 2020 about billions of devices would be connected among each other2. 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 infrastructure3. The impact of IoT is generally vision 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 IoT4. In cloud computing authenticating the user/senders is also very much needed apart from encryption of data26,28. Considering the threats, some improved techniques 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/ receiver29. 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.

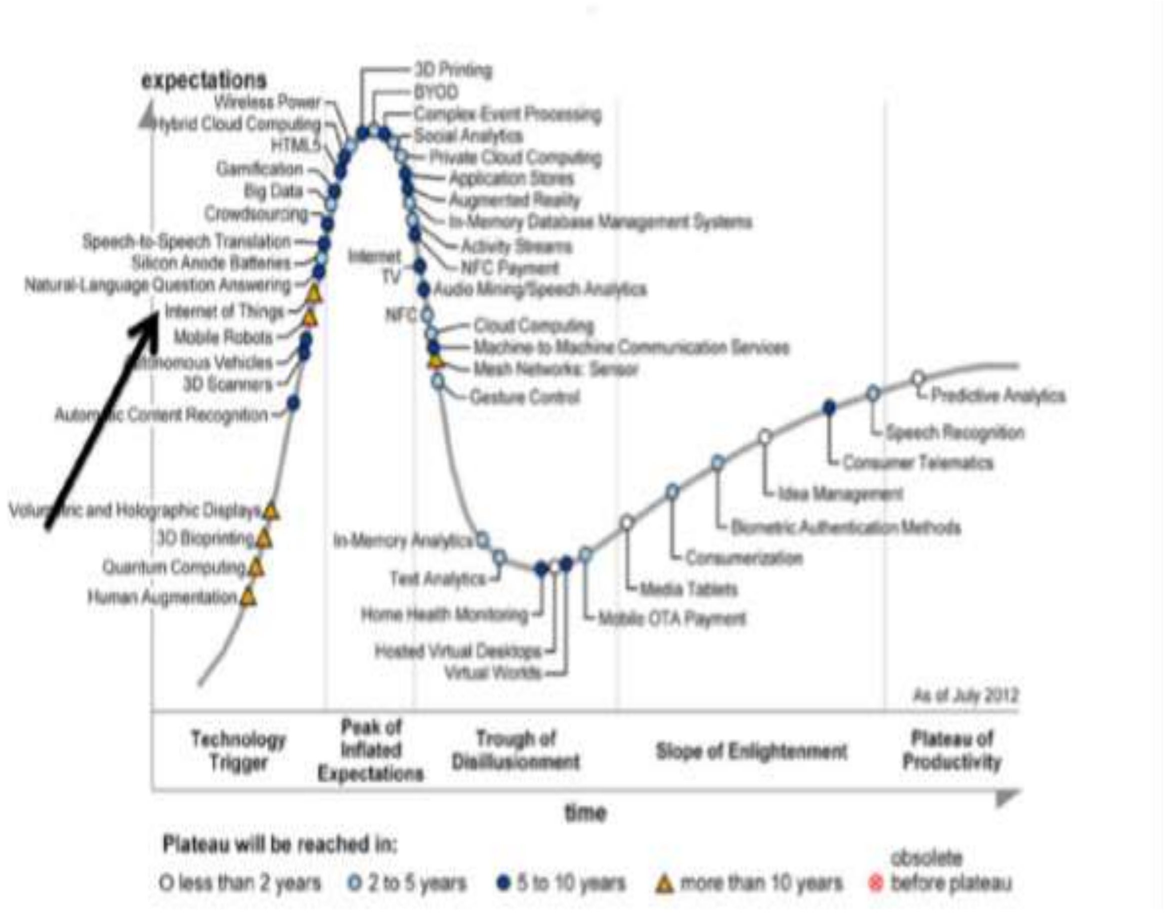


Figure 1. Gartner’s hype cycle.

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/senders6. 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 definition7. IoT is one of the technology emerging in IT which is given in Gartner's IT hype cycle in the Figure 18. 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 difficult9. 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 etc10.

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 RFID11. 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 IoT12. 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 link13. 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.

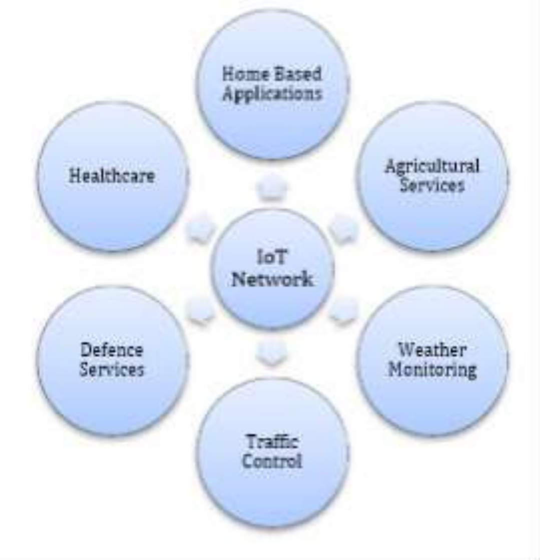


Figure 2. Application of IoT.

The IoT concept target is in the formation of smart items, smart cities, smart living by forming smart autonomous devices14,15. 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 IoT16. 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 analogy 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 arise 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 architecture18. In IoT user/senders and their environment are also connected with connection between the devices and connection between the user/senders.

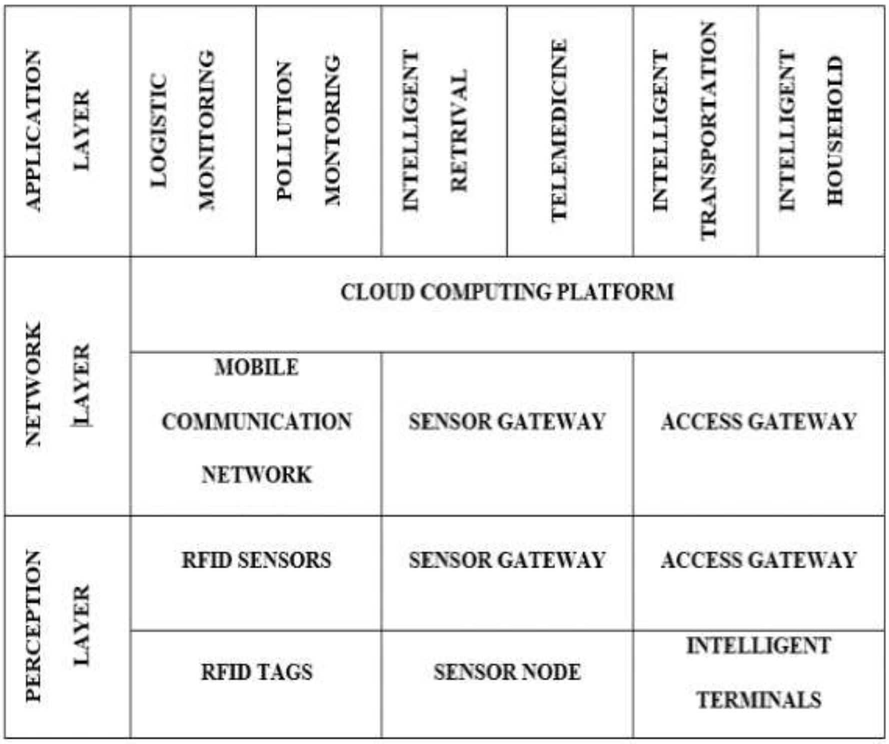
6. SECURITY THREATS AND CHALLENGES IN CLOUD AND IOT

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 problems24 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 are 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 endto- end security. The main concept in cloud computing is for user/senders concern in reducing complexity and enhancing handling capability of cloud28,29. 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 viability30. 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 transmission26.

7. IOT ARCHITECTURE

IoT architecture depends on interoperability of heterogeneous systems. Security architecture is built for IoT based on the security deficiency. Well defined architecture 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 layers' architecture consists of perception layer, network layer and application layer shown in the Figure 319. 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.



<table>
<tr><td>APPLICATION LAYER</td><td>LOGISTIC MONITORING</td><td>POLLUTION MONTORING</td><td>INTELLIGENT RETRIVAL</td><td>TELEMEDICINE</td><td>INTELLIGENT TRANSPORTATION</td><td>INTELLIGENT HOUSEHOLD</td></tr>
<tr><td rowspan="2">NETWORK LAYER</td><td colspan="6">CLOUD COMPUTING PLATFORM</td></tr>
<tr><td colspan="2">MOBILE COMMUNICATION NETWORK</td><td colspan="2">SENSOR GATEWAY</td><td colspan="2">ACCESS GATEWAY</td></tr>
<tr><td rowspan="2">PERCEPTION LAYER</td><td colspan="2">RFID SENSORS</td><td colspan="2">SENSOR GATEWAY</td><td colspan="2">ACCESS GATEWAY</td></tr>
<tr><td colspan="2">RFID TAGS</td><td colspan="2">SENSOR NODE</td><td colspan="2">INTELLIGENT TERMINALS</td></tr>
</table>

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 is applicable to the IoT also20, 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 security22. 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.

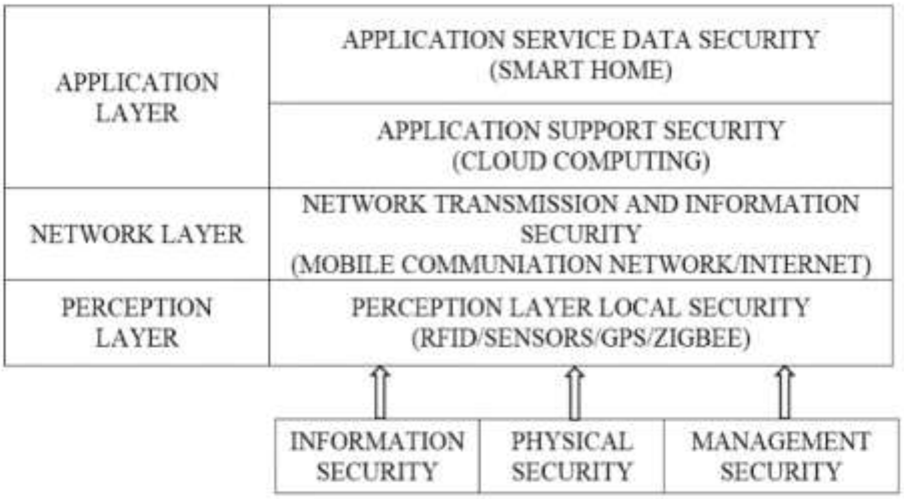

APPLICATION LAYER
APPLICATION SERVICE DATA SECURITY (SMART HOME)
APPLICATION SUPPORT SECURITY (CLOUD COMPUTING)
NETWORK LAYER
NETWORK TRANSMISSION AND INFORMATION SECURITY (MOBILE COMMUNIATION NETWORK/INTERNET)
PERCEPTION LAYER
PERCEPTION LAYER LOCAL SECURITY (RFID/SENSORS/GPS/ZIGBEE)
INFORMATION SECURITY
PHYSICAL SECURITY
MANAGEMENT SECURITY

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 communication31 and AES for securing file32 and authentication33 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/senders21. Data storage devices are also referred as servers therefore servers are not dedicated separately and are present in cloud computing22,28. Access the data from the servers by different user/senders are through system/receiver are represented in Figure 5.

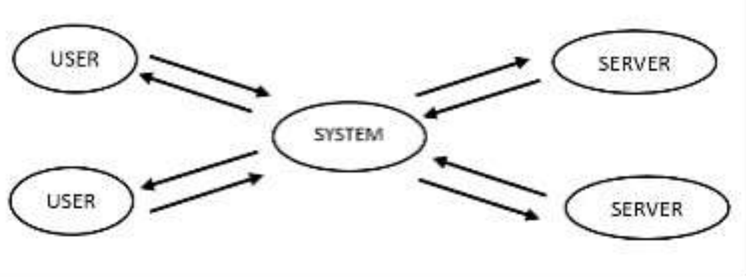


Figure 5. Communication model of cloud.

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 key32,34. 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.

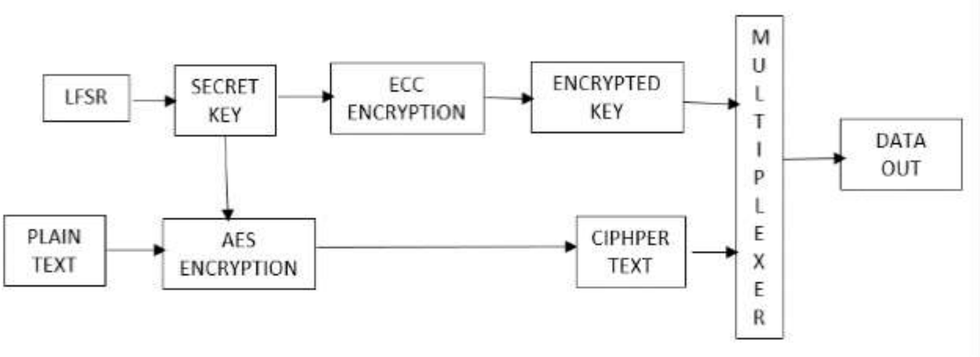


Figure 6. Block diagram of the user/sender.

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.

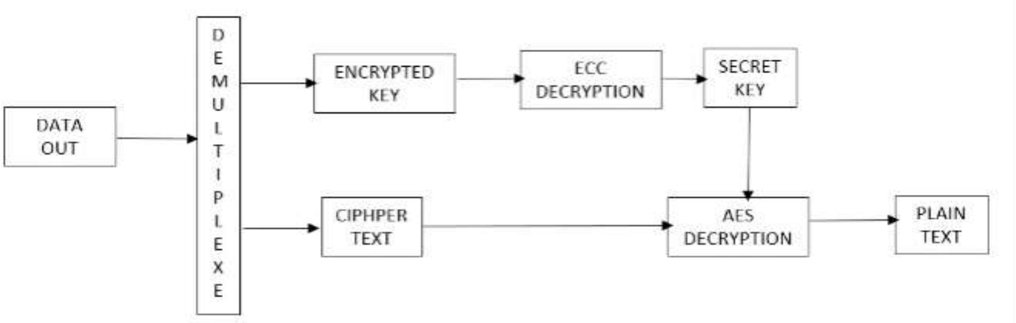


Figure 7. Block diagram of the system/receiver

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 is 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.

9.1 ECC

ECC is a public key encryption scheme introduced by Neil Koblitz35 and victor Miller36 in 1985. This cryptosystem is alternate to RSA25,26. 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 ECDLP17. The asymmetric encryption system based on ECC are Elliptical Curve ElGamal Algorithm and Elliptical Curve Menezes-Vanstone Algorithm23. The finite fields in Elliptical Curve are prime field GF (p) and GF (2m). 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 (2m) satisfy the equation 3 where a, b ∈ GF (2m) and b≠0.

If Elliptical Curve point doubling happens and if 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.

9.2 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 Fq by considering q = pr 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 RS randomly and calculates PS = RSG E and transmits it to the system/receiver. System/receiver generates secret number RR randomly and calculates PR = RR*G E and transmits it to the user/sender. The user/ sender receives PR from system/receiver and multiplies with its secret number to generate KS = RS * PR. The system/ receiver receives PS from user/sender and multiplies with its secret number to generate KR = RR * PS. Comparison of KS and KR are performed and specified in equation 8.

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

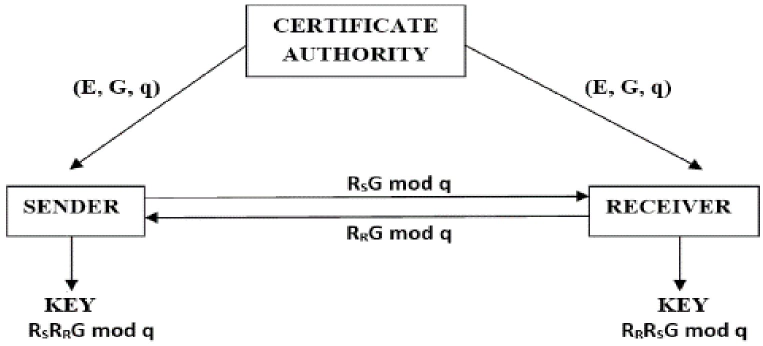


Figure 8. Elliptic curve diffie-hellman-merkle key exchange scheme.

9.3 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 other40. 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 process27. The ASCII characters are mapped to the scalar multiplied points which is specified in Table 242,43. 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+RS*(RR*G)) and the encrypted message from user/sender is represented as (RS*G, M+RS*(RR*G))42.

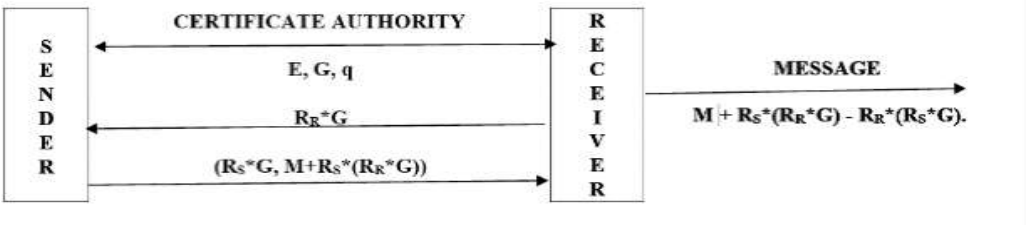

SENDER
CERTIFICATE AUTHORITY
E, G, q
R_R*G
(R_S*G, M+R_S*(R_R*G))
RECEIVER
MESSAGE
M + R_S*(R_R*G) - R_R*(R_S*G).

Figure 9. Elliptic curve elgamal cryptosystem.

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

9.4 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 algorithm37. The standard AES processes encrypts 128 bits of data using different key sizes41. The basic operation is represented in Figure 10 for encryption and decryption of data. The sequence is shown as Blocks. A sequence of 8 bits are single entity which is basic for processing AES39. 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 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.

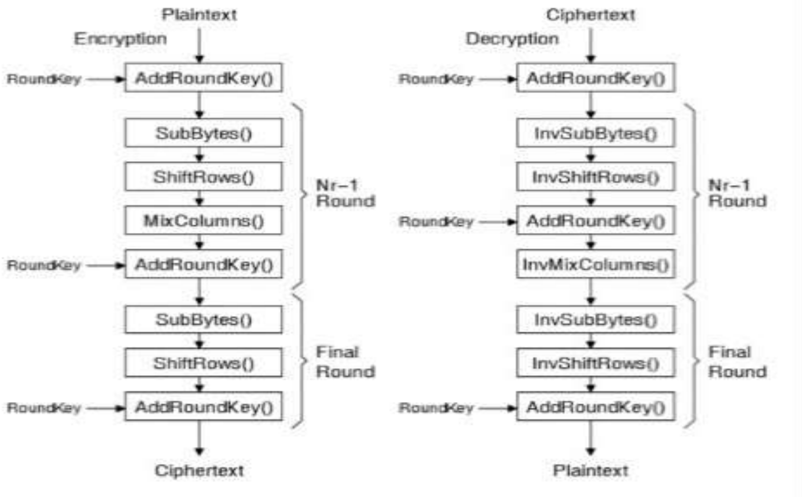


Figure 10. Encryption and decryption of AES.

Mix Column: In this process an array (x3+x2+x for example) is selected for multiplying using modulo x4 + 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 is interchanged with add round key and inverse mix column interchange. Hence from the cipher text the information is obtained.

10. 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 analysing, interpreting the data from sensors. These process of cloud computing are hidden from the user/senders.

11. 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 client/senders and framework/recipient by Elliptic Curve Diffie Hellman Key Exchange. Here basic leadership is simple as an individual has to need. In this paper IoT security challenges were considered and talked about. The results got to show that the cryptosystem with encryption and decoding over GF (p) has a base time of 18.060ns with the most extreme? feasible recurrence of 55.371MHz on Xilinx Virtex-5 (XC5VLX50T-1FF1136).

12. 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. The information is available from the perception layer. This layer also supports the application layer.