International Journal of Computer Applications (0975 – 8887)
Volume 179 – No.46, June 2018

Securing VoIP Communication using ECC

Amar S. Gosavi
Department of Master of Computer Appplication,
Veermata Jijabai Technological Institute (V.J.T.I)
Matunga, Mumbai, Maharashtra, India

Nikhil B. Khandare
Visvesvaraya National Institute of Technology
Nagpur, Maharashtra, India

ABSTRACT
This paper highlights the enhancement in security in VoIP by using ECC. The proposed protocol to enhance security comprises of two phases key generation, Secure transmission. Both phases included ECC which can be proved to be practically secure against most of the popular attacks. The security analysis of the proposed protocol is also given and protocol mathematically to be secure.

Keywords
Elliptic Curve Cryptography(ECC), Mobile Station International Subscriber Directory Number(MSISDN), Voice over Internet Protocol(VoIP), Session Initialization Protocol(SIP), Real-time Transport Protocol(RTP), Elliptic curve Diffie Hellman Problem(ECDHP), Diffie Hellman Problem(DHP).

1. INTRODUCTION
ECC (Elliptic curve cryptography) this method based on DLP(Discrete logarithm problem). ECC is trapdoor function for key generation and difficult crack this function. The standard equation for curve E is had equation $Y^2 = X^3 + aX^2 + b$ on field F. ECC consists of point addition, point doubling and scalar point multiplication.

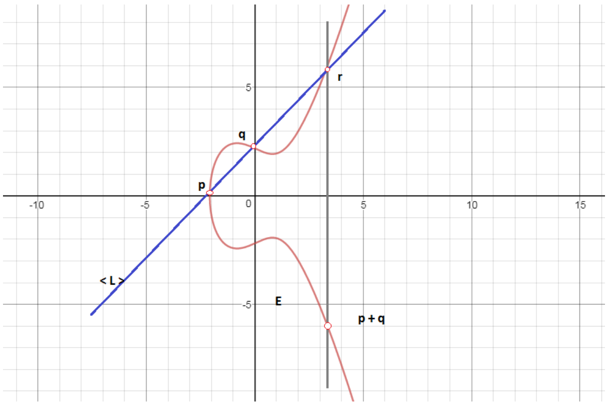

Figure 1: Point Addition

Point Addition is slope of line L is $\Lambda = \frac{(Y2 - Y1)}{(X2 - X1)}$ for X1 !=X2 or $= \frac{(3Xa\,2 + a)}{(2Y1)}$ for X1 = X2. Then third point on curve is X3 = Λ – (X1 + X2), Y3 = Λ (X3 - X1) + Y1 = R(X3, Y3)

In the point doubling are P + P = 2P for Line L is tangent to curve at point P and touch on point R on single point R then the value of R is = 2P.

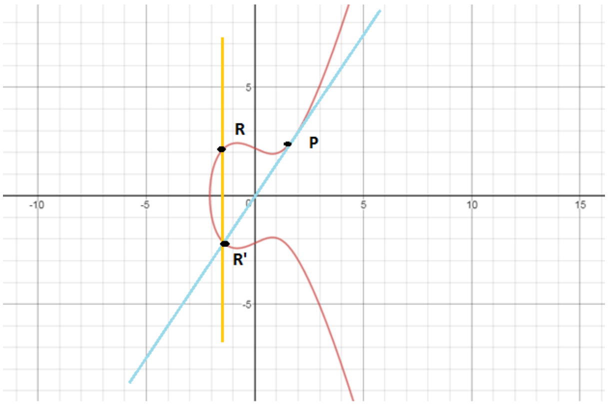

Figure 2: Point Doubling

Point coordinate can be calculated and slope as follows

$$s = \frac{3x\text{^}2 + a}{2Yp}$$

$$Rx = s^2 - 2xp \;\&\; Ry = s(xp - xr) - yp$$

Point coordinate can be calculated and slope as follows

$$s = \frac{3x\text{^}2 + a}{2Yp}$$

$$Rx = s^2 - 2xp \;\&\; Ry = s(xp - xr) - yp$$

In the scalar point multiplication generated by group generator G_q where Q = n **.** P, where n number of time addition of P. n is integer which belong to group generator Gq. That belongs to DLP which makes power full public key cryptography algorithm.

Proposed system are based on mathematical hard problem like DLP and DDHP.

DLP(Discrete Logarithm problem)this is defined as Logarithmic multiplicative cyclic group. Its based-on Logarithm and multiplicative function. If cyclic group G and g is generator then his element in G so it can write as g^x for some x. If we mode g^x this will give h. Finding x from value of n not possible and probability of finding same x is negligible.

DDHP(Decisional Diffie-Hellman Problem) it having G in member with $(g,g^{a,} g^b, g^{ab)}$ the G called collection tuples G^4. For any value of a & b you are not able to find weather $g^{ab} = g^c$ or (a*b) = c mod by g. Finding the processed final value is not possible.

VoIP is popular technique that transfer telephonic system audio on internet. It has 2 way data transfer enable on broadband network combination of VoIP + LTE (Long-term Evolution) = VoLTE (Voice over Long-term Evolution) which benefit mobile cellular network provider giving cheapest option transfer voice data. VoIP has two SIP and RTP

2. LIRATURE REVIEW

2.1 Secure Multi-Purpose Mobile-Banking Using Elliptic

Ray.et al. [1] built system for mobile to provide security in mobile banking system using ECC. In this system, there are two major components which are CPU (Client Processing Unit) and SPU (Server Processing Unit) that help to achieve the secure and robust system. Different types of the task can be given following manner

2.1.1 Session key generation and Authentication.

Step1 CPU to SPU : ID_U ,V_U,$EK_X(C||h(ID_U ,V_U,B_U))$

In this step, CPU has ID_U, V_U (generated public key), B_U (Captured Biometric). Where B_U helps to avoid the replay attack. Hash digests are calculated to avoid modification during the transfer. A is the secret key of Client and V_U is a public key of the client. X is symmetric key and X = xi.P where xi = x + i for i=1,2,3…up to bank limit. The operation will continue until 3 wrong attempts.

.Step2 SPU to CPU $EK_X(C)$ /No[Terminate]

SPU verifies that if ID_U is matching then it generates a key with respect to their ID_U. SPU decrypt packet and from that get C and $h(ID_U ||V_U||B_U)$. SPU checks that h $(ID_U ||V_U||B_U)$ is matches or not. If all conditions are satisfied then SPU sends packet $EK_X(C)$.

Step3

CPU calculates the key K= a.V_U = a.b.P = (K_X,K_Y) using key decrypt the message $DK_X(EK_X(c))$ and check is Equal if yes then authenticate. Else process is repeated from the start.

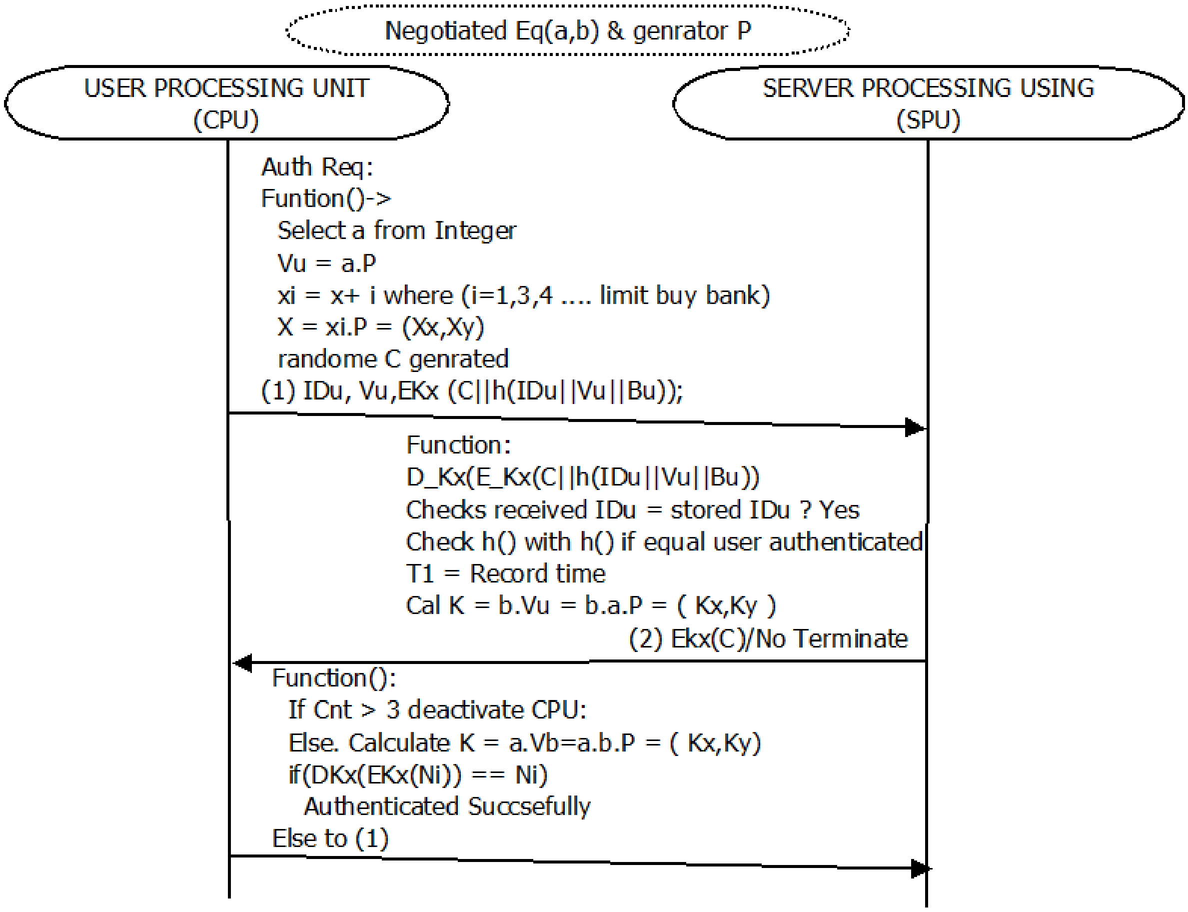

Figure 3: Session key generation and Authentication

2.1.2 Money Transfer

Step1 CPU to SPU: $EK_X(ID_J||y||h(y))$:

User provide ID_J (receiver A/c No), FUND to CPU. CPU generates y = A/c number || FUND then calculate h(y) then concatenates h(y) as $ID_J||y||h(y)$ and encrypts using K_X and sends to SPU.

Step2 SPU to CPU Ch2 [through SMS]:

CPU decrypt the data packet using K_X and checks time limit exceeds. If not Then calculate h(y) and checks that if equal then generate the 2nd challenge to SMS.

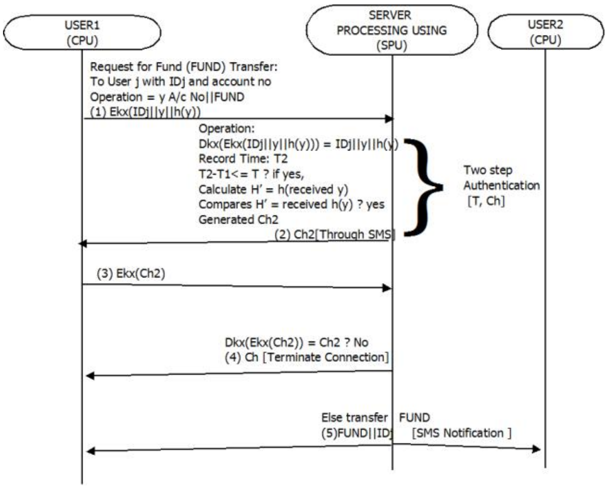

Figure 4: Money Transfer

Step3 CPU to SPU: $EK_X(Ch_2)$:

The user sends received Ch2 to SPU in an encrypted format.

Step 4

Decrypts the data and check whether is equal or not if not then terminate else transfer fund at ID_J account number.

Step 5

Send notification to ID_J, ID_U ,and FUND transfer successfully.

2.2 ECC Based IKE Protocol Design for Internet Applications

This system developed by Ray et al [2] it consists 2 phases which are further classified as phase 1 in 2 modes and phase 2 in 1 mode. See Phase by phase explanation working of the system. requester and responder are the two members of communication in the system this where the requester is client and responder are Server.

2.2.1 PHASE 1

Step1

A client sends a request to the server. In that request client sends the supported cryptographical function, IP and ID know the client to a server.

Step2

Server select supported cryptographical suit and Generate X_{RES} where X_{RES} = Fun (IP_{RES}, ID_{RES}, PU_{RES}). The server sends X_{RES}, PU_{RES}, N_{RES} to the client. X_{RES} define the uniqueness of sender and receiver. Where N_{RES} is number given to packet which helps to avoid replay attacks. PU_{RES} key give helps achieve security.

Step3

Client computer calculates Fun(IP_{RES}, ID_{RES}, PU_{RES}) for X_{RES} if both, received and calculated are equal then go further processing else reject the packet. Calculated the secret key K = K_{REQ}. PU_{RES} =K_{RES}.K_{REQ}.P = ($SKEY_E$, K_Y) and generate X_{REQ} and send $HASH_{RES}$ = fun($SKEY_{ID}$, IP_{REQ}, IP_{RES}|SA_{OFF}|ID_{REQ}) where $SKEY_{ID}$=($SKEY_E$, N_{RES}|N_{REQ}) Session-key and encrypts with ID_{REQ}, IP_{REQ} using $SKEY_E$ and send with public key X_{REQ}, N_{REQ}

Step4

The server generates secrets key K = K_{RES}. PU_{REQ} = K_{RES}. K_{REQ}.P = (K_X, K_Y) = ($SKEY_E$, K_Y) then generates the $SKEY_{ID}$ = PRF($SKEY_E$, N_{REQ}, N_{RES})and decrypt the message using $SKEY_E$ now calculate X_{REQ} and verifies requester not Bogus. If all matched the calculated $HASH_{RES}$ and send to the client.

In phase I three keys are generated as given $SKEYID_E$ (Encryption), $SKEYID_A$(Authentication), $SKEYID_D$ (Decryption) used common key $SKEY_{ID}$ for phase II. Generation as follows $SKEYID_D$ = Fun(SKEYID, KY|0), $SKEYID_D$ = Fun($SKEY_{ID}$, SKEYIDD, K_Y|1), $SKEYID_E$ = Fun($SKEY_{ID}$, SKEYIDA, K_Y|2) all keys help to complete phase II.

Generate IPSec SA is in the last step of the system. Generation of public key P_{REQ}, P_{RES} is generated package exchange only in PFS (Perfect Forward Security) is desired. The details based on ECC-based IKE protocol are discussed.

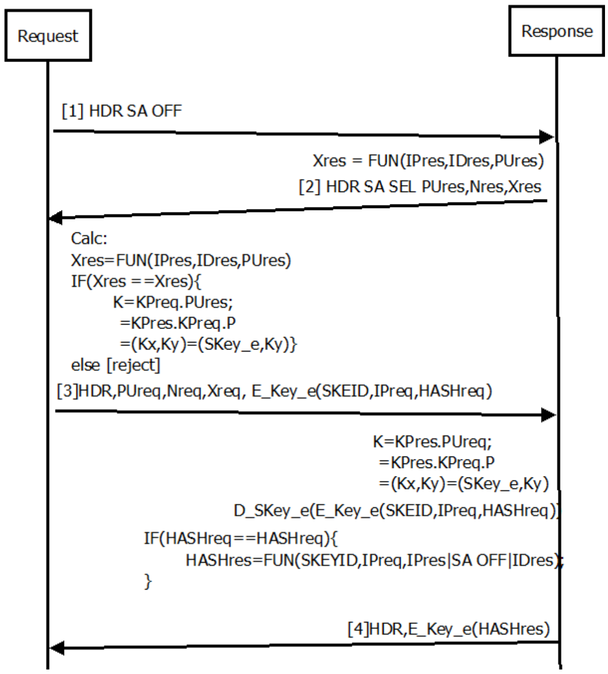

Figure 5: PHASE 1

2.2.2 PHASE II

Step 1

Generates HASH I = Fun (K_Y, Msg_{ID}, |SA|N_{REQ}) to authenticate received packet. Where K_Y generated in Phase I. SA = IKESA of phase I and N_{REQ}, the client sends HASH-I, SA, N_{REQ}, and some optional parameter's like P_{REQ}, ID_{REQ}, ID_{RES} which encrypted using $E_{SKEYIDE}$ to confidentiality of package.

Step 2

This step finds HASH I (received)= HASH I (calculated) if equals then calculated HASH II = Fun(KY, MsgID, |SA|N_{RES}) to authenticate. N_R is message number to avoid the replay attack. HASH II encrypts using ESKEYIDE and send to the client.

Step 3

The same procedure of step 2 is repeated check HASH-II if equals proceed to calculate HASH III = Fun(K_Y, MsgID|SA|N_{REA}|N_{REQ}) packet encrypted using $E_{SKEYIDE}$ sends to the responder.

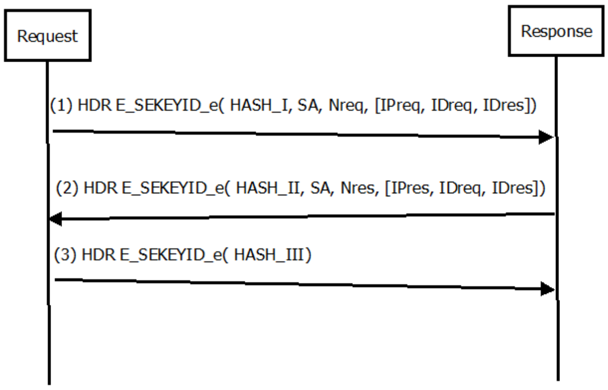

Figure 6: Phase II

2.3 Efficient and Secure Communication Architecture for E-Health System

This system developed by Ray et al.[4] based on Healthcare system which having multi-stage procedure to get treatment from DOC(doctor) who register with HOS(hospital). The user should have registered with RA (Register Authority) to getting treatment. RA is solely responsible for communication with USER and DOC. Steps give the user to accesses system for health care. In this MS_P is generated master secret key and store details of the user in RA database. Registration and Session key negotiation can explain as follows.

2.3.1 Registration

This step gives the user to accesses system to get the cure. In this process, MSP(master secret key) is generated and store details of the user in RA database.

Step1

The user sends his ID_U (identity), CA_U (certificate) and, N_U(nonce) to RA so that RA can Identify the user.

Step2

After receiving the Request validate the user, user data, and certificate then RA randomly generate MSp to ID_U respectively then RA generate is own NRA and process and concatenate as $X = MSp||N_{RA}$ and $Y = ID_U ||ID_{RA}||N_U||N_{RA}$ Which encrypted with public key of user and second part sign and encrypt with private key of RA.

Step3

Now user validate received data. First $D_{PRRA}(E_{PURA}(X))$ which gives MSp and N_{RA} to verify the message integrity and authentication and Decrypts $D_{PURA}(E_{PRRA}(h(y)))$ and calculate its own hash and checks $h(y) = D_{PURA}$ $(E_{PRRA}(h(y)))$ if fails then terminate connection else send $Z = N_{RA}$-1 by encrypting with E_{MSP}.

Step4

Now RA received data Decrypt that data $D_{MSP}(E_{MSP}$ (Z)) check is equal to N_{RA}-1 then yes else send no.

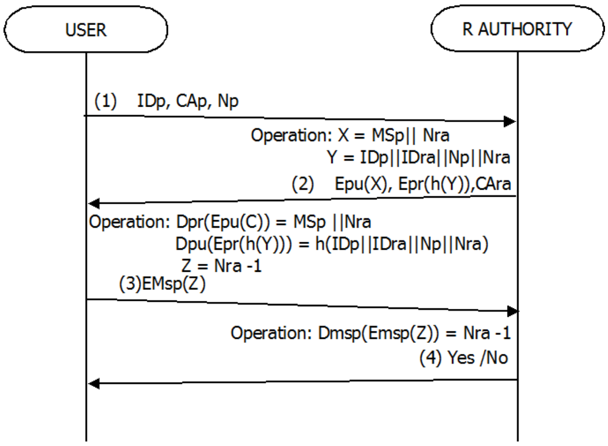

Figure 7: Registration

2.3.2 Session key negotiation

m This process three parties comes to generate the SKEY for secure communication between parties. By using Diffie Hellman key exchange problem.

Step1

The user selects any random number which 0<=x<=p-1 and calculated $R1 = g^x \bmod p$ and concatenate with disease details and encrypt using his master key generated during registration. EMSP (R1|| DS) send with ID_U ,ID_{HSP} and $E_{PRUR}(h(Y))$ where Y is concatenation of $ID_U||ID_{HSP}||DS$ and E_{PRUR} is private key of User.

Step2

RA decrypt received data $D_{PUUR}(E_{PRUR}(h(Y)))$ also decrypt $D_{MSP}(E_{MSP}(R1||DS))$ and calculate h(Y). If $h(Y) = D_{PUUR}$ $(E_{PRUR}$ (h(Y))) fails then termination of process and request resend to user. After success, RA chose y has his secret key where y is (0<=y<=p-1) $P1= R1^y \bmod p$ and then data to the hospital which includes ID_U, ID_{RA}, $E_{MSPHSP}(R1||P1)$ to hospital.

Step3

Hospital decrypt all data using master secret key received from RA and select his secrete key z. By decrypting data and get R1 and P1 now select z where (0<=z<=p-1), Calculate $R2 = g^z \bmod p$ and $P2 = R1^z \bmod p$ now $SKEY = P1^z \bmod p = R1^{yz} \bmod p = g^{xyz} \bmod p$ now send ID_{HSP}, ID_U along with E_{MSPHSP} (R2||P2) and Nonce $E_{SKEY}(N_{HSP})$.

Step4

RA received data packets which decrypt using MSP and get R2 and P2 and calculate $P3 = P2^y \bmod p$, $SKEY = P2^y \bmod p = R2^{xz} \bmod p = g^{xyz} \bmod p$ now have SKEY decrypt the Nonce D_{SKEY} $(E_{SKEY}$ $(N_{HSP}))$ for user RA send ID_{HSP}, ID_U along with E_{MSP}(P3), E_{SKEY} $(N_{HSP}$-1).

Step5

The user first decrypts the message $D_{MSP}(E_{MSP}(P3))$ and calculate or generate the SKEY and now decrypt D_{SKEY} $(E_{SKEY}$ $(N_{HSP}$-1)) now calculate the $(N_{HSP}$-2) and E_{SKEY} $(N_{HSP}$-2) and send to Hospital.

Step6

Hospital calculate the NHSP-2 and checked with D_{SKEY} $(E_{SKEY}$ $(N_{HSP}$-2)) if equal the send's YES to RA else NO to RA

Step 7 & 8

RA received ACK for hospital this step generated token as $UT = E_{PRRA}(h(X||T))$ where $X = h(Y)$ which is received in step 1 and T is timestamp for validate UT generate the Z = UT||ID_U ||DS||T which encrypt using SKEY and E_{SKEY}(UT) to user and E_{SKEY} (Z) to hospital. UT will available for specific time T. which include ID_U and DS identity and disease.

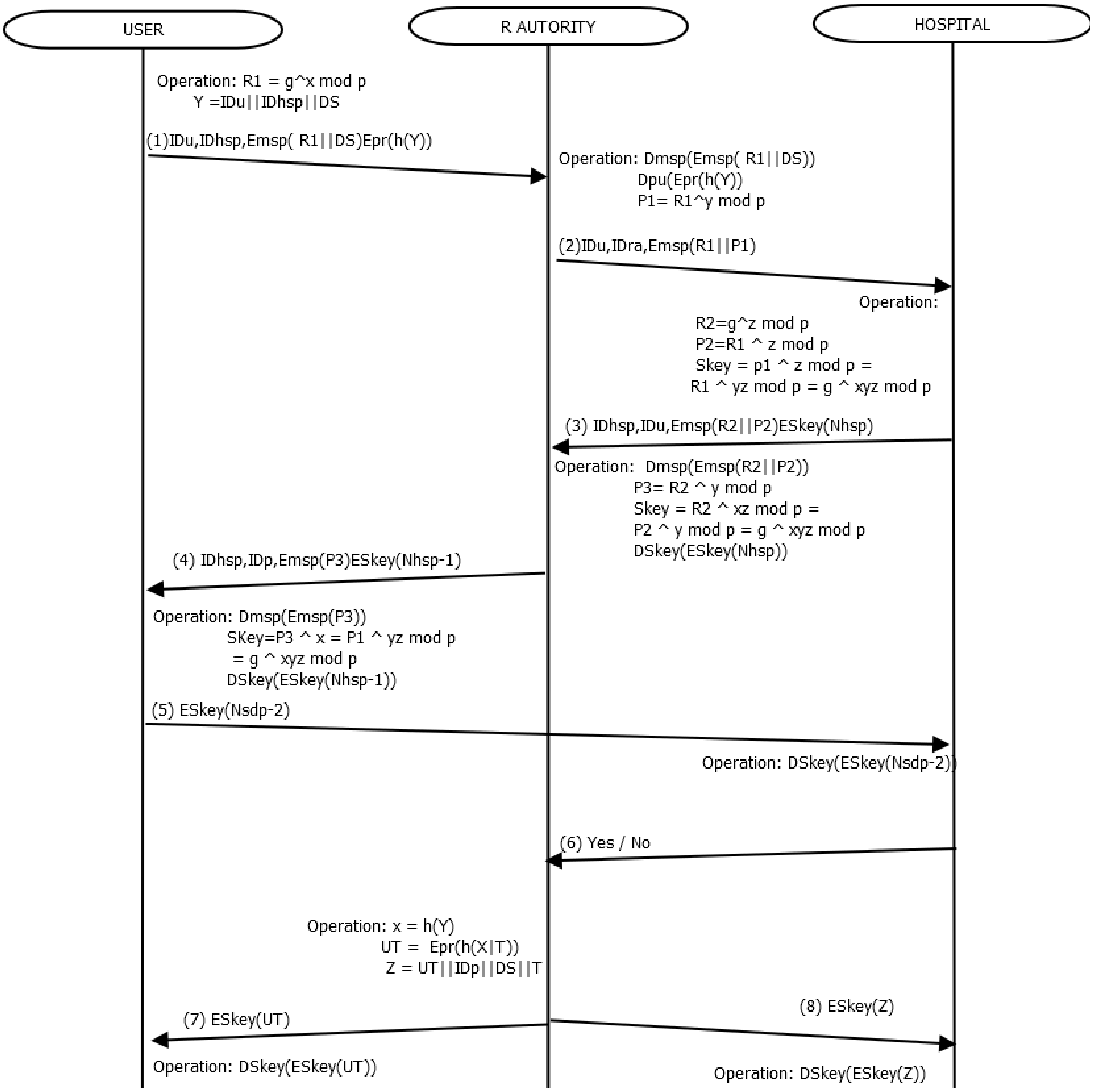

Figure 8: Session Key Negotiation

2.3.3 *Service and UT negotiation*

SERVID is generated with the help of SERVUT = E_{SKEY} (h(Y)) where y is in the first step of key generation. Generated SERVID uses to authenticate the user for treatment to any doctor until time T is finished. It can be explained as flows.

Step1

The user sent a request to a hospital with ID_U, E_{SKEY} (UT||DS) in this packet provide the identity of user = ID_U and provide security to communication by using SKEY for encryption.

Step2

Hospital first decrypt the data which come from user and verify data in database UT equal to stored UT if match generate the SERVID = (ID_U ||ID_{HSP}||DS||SlNo) where Sl No is the serial number of user after that create SERVUT by sighing with private key and Time stamp T. SERVID = E_{PRHSP}(h(SERVUT||T)). List of doctors is select from database send to user LOD which include IDDOC. Now HSP send data to USER E_{SKEY} (ID_{HSP}||SERVUT||LOD)

Step3

This phase hospital sends data to DOC the list in LOD with User id ID_U which concatenate with SERVUT and DS which encrypt with SKEY and send to the doctor.

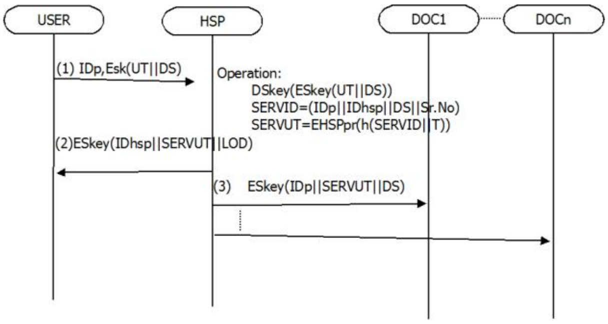

Figure 9: Service and UT negotiation

2.3.4 Treatment phase

This is phase doctor get form and details from the user and stored at RA, and cure user.

Step 1

A user sent a request to doctor for treatment which includes ID_U and ID_{DOC} which are present in LOD.

Step 2

Doctor verify the user identity and SERVUT and from the hospital. Retrieve details from RA about disease and symptoms of the user then send the Treatment form and CA_{DOC} to the user.

Step3

User send filled form to concatenate with SERVUT and SKEY. Encrypts data packet with the public key of a doctor. The user sends the hash of filed form to encrypt with SKEY. The form data are transfers securely.

Step4

Doctor decrypt the message by using his private key and get SERVUT, SKEY and filled form now decrypt the data with the session key, and get hash of response of form check with the calculated hash of filled form if both are equal then he sends a request to get PHI previous data of the user. Doctor send a request to RA which includes ID_{DOC}, ID_U and encrypted data SKEY(ID_{HSP}||ID_U).

Step5

RA verify the message data first decrypted data using SKEY then verify the HSP and IDU with the database if match then retrieves the data and send with IDU and Data encrypted using E_{SKEY}(ID_U||PHI) to doctor.

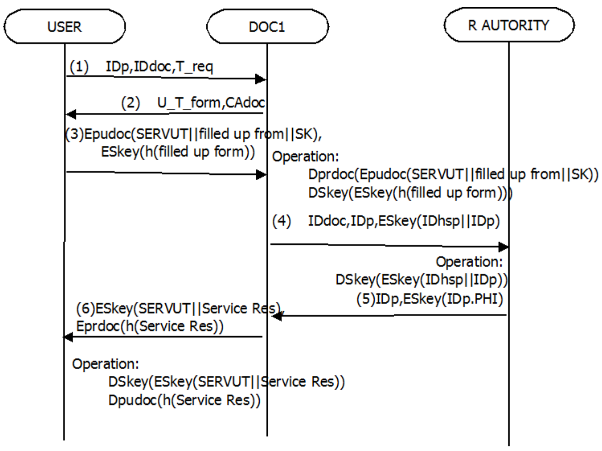

Figure 10: Treatment phase

Step6

Now doctor has previous data and old medical cases of client in PHI and DS where doctor then can decide it is possible to treatment or not if yes the send response to user which sign by his private key as signature then on hash of response actual data are encrypted using SKEY data packets included the SERVUT || service response. Hash of message are in send part of data is hash(received response) = DPUDOC(EPRDOC(h(received response))) if equal then select else reject. If treatment is giving benefits to the user then continue with DOC otherwise change the DOC form LOD.

2.3.5 Diagnostic Report

After completion of treatment, the data and treatment detail should save in PHI in storage database of RA to benefit for future.

After completion of treatment, the data and treatment detail should save in PHI in storage database of RA to benefit for future.

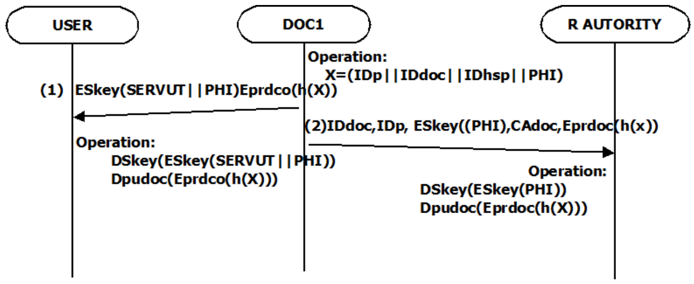

Figure 11: Diagnostic Report

Step1

Doctor get all data with SERVEUT||PHI now encrypt the data using SKEY. And doctor generates X = (ID_U|| ID_{DOC}|| ID_{HSP}||PHI) which sign by doctor's private key user can store the data PHI by decrypting using his SKEY and verify the signature of data using doctors public key.

Step2

Doctor send data to PHI with which encrypts with SKEY, send data along with ID_{DOC}, ID_U.E_{SKEY}(PHI),CA_{DOC},E_{PRDOC}(h(X)). RA verify the h(X) with received h(X) by decrypting the data. If match then save data to Record with RA

2.4 Security Challenge and Defense in VoIP Infrastructures

Some proposed security mechanism by Butcher et al [3]. To provide security to VoIP to achieve secure communication which guarantees of Integrity, Authentication, Confidentiality, and Availability. It can explain as follows.

2.4.1 Separation of VoIP and Data traffic

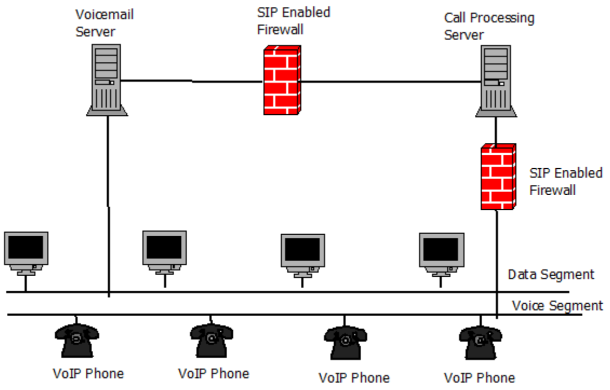

Figure 12: Separation of Voice and data

Segmentation of line as shown in figure 12. the, separating the traffic of data and voice data that separation is the main key to security. The separation will provide security as the computer not have an easy entry in voice line in VoIP network. To avoid the expense of extras network cost using of VLAN is best option to implement segmentation in VoIP. In this system SIP firewall also help to achieve the security. Firewall is connected to the Voice mail and call processing server to achieve controlled connection with the server

2.4.2 Media Encryption

Protecting the data during the transmission provide security against eavesdropping. VoIP uses the RTP for transmitting the data. To achieve we can use Secure real-time transfer protocol(SRTP) published by Internet Engineering Task Force(IETF) as RFC-3711. Adding the security patch to RTP payload. This protocol provides the Authentication and confidentiality of the data packets. This uses the small key size to transfer lightweight communication package payload need of low bandwidth, low processing, and low communication. IPsec uses for the secure key establishment to create a secure tunnel between parties.

2.4.3 Current Security measures in VoIP

VoIP is widely used protocol for communication purpose. In VoIP system SIP(Session Initializations Protocol) and RTP (Real-time Transport Protocol) are handled the major part of communication. There are no security measures happened such as authentication and encryption. Which makes system venerable for various attacks, for example, D.O.S, replay, etc.

Various confidential and important communication happened on Tele-network which make this medium very important for security. This architecture which provides security features like Confidentiality, Integrity, Authentication by using various important key element. for encryption and Decryption use ECC which highly secure and fast also mostly unbreakable. Key generation and encryption process are lightweight because of less number of bits key used in the system. ECC is much secure as compare with other algorithms in less bit secure system.

3. PROPOSED SYSTEM

Due to the drawbacks of the existing system, The new system for secure communication of voice over internet protocol is designed. Diagram depicting the stepwise working of the system shown in figure 13 & 14

The Proposed system has two phases namely key generation, Message transmission by using ECEDHP. The system can make by using MSISDN, and current IP address of the client.

Notation used

E: Elliptic curve on filed F.

F: Finite field on Curve.

P: Point on Curve E(x,y)

g: Generator common with sender and receiver.

MSISDN: Unique number of provider.

PU_R: public key.

Kr: private secrete Number.

IP: IP address on entities.

$META_A$: random function on variable (IP,MSISDN,PU)

E: Encryption

D: Decryption

h(): Hashing function

K(x,y): Shared secrete Key.

3.1 Key Generation

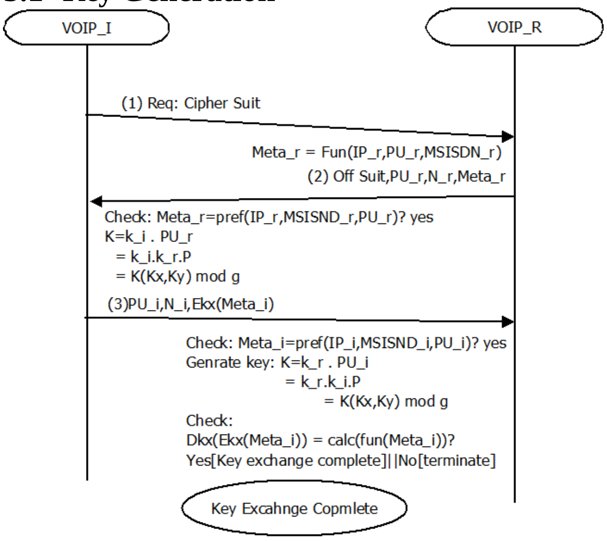

Figure 13: Key Generation

Step 1

The initiator sends cryptographic suite in which supported cryptographical function by the device. This details in the cryptographical suit.

Step 2

Calculate the $META_R$ function (IP_R, $MSISDN_R$, PU_R) with IP_R is IP address of responder, MSISDNR number of responder MSISDN numbers are unique for mobile devices, PU_R this public key $PU_R = K_R.P$ where K_R is the secret key of the responder. Generator g helped to achieve security during transmission. Send all this PU_R, N_R, $META_R$ to VOIPI to the server.

Step3
Checked that $META_R$ is equal to $META_R$ (calculated) if yes the generate the key $K=Ki.PU_R=ki.kr.P = K(K_X,K_Y)$ mod g this shared secret key are generated.

Now encrypt the METAI using KX and send with PU_I, N_I where $META_I$ (IP_I, $MSISDN_I$, PU_I).

Generated the shared secret key which used to decrypt the $D_{KX}(E_{KX}(META_I))$ and responder calculates $META_I$ and if equal then key generated successfully send.

3.2 Message Transmission
Phase I have the key as $K(K_X,K_Y)$ where suing key KY encrypts MSG, MSG_{ID}, h(MSG). hash of massage helps to find any modification is done during transmission on network and ID help to identify the unique message.

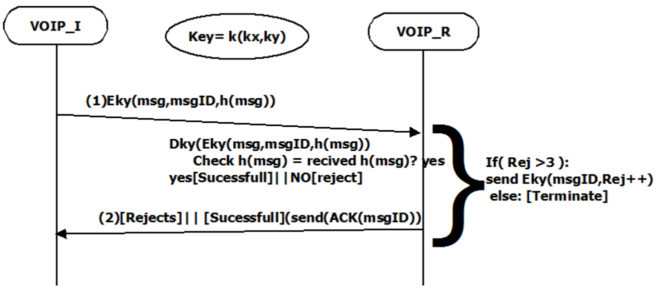

Figure 14: Message Transmission

Step1
Encrypt the message using K_Y with hash. Hash is calculated of send message.

Step2
$VOIP_R$ received that package $D_{KY}(E_{KY}(MSG, MSG_{ID}, h(MSG)))$ if h(MSG) if equal to received h(MSG) then data is correct to accept the data send ACK to the user otherwise reject the package. If rejection happened more than 3 times connection is terminated. to avoid the DDOS.

4. SECURITY ANNALYSIS
The system gets security with the help of multiplying secrete key with point P. and mod buy shared secret key g. which make problem more difficult DLP(Discrete Logarithm Problem) which hard to break.

The key sharing of application used DHP which secure but, on some attacks, Diffie Hellman is vulnerable. Further prevention for overcoming with adding ECC with them.

System security based on ECC problem which far more secure than RSA. Also, the key length in small but security is very high. Because of key size in the small performance of this system is too high as compared to base on RSA.

The combination of ECC and DLP makes system secure and high performance and ECC with DHP for sharing key and using that encrypting the message which makes more secure.

Hashing of the message during the transmission gives a guarantee of Integrity of message. Also, the message ID helps to avoid the replay attack on the system.

4.1. Popular attack and Defense mechanism
4.1.1 Brute Force Attack
It is one of the most popular and famous attacks. This attack is not possible on our architecture because of ECC-DHP the brute force gives no result and outcome is noting. Message in encrypted using $P(K_X, K_Y)$ finding element P is not possible because of ECC find message using brute force not possible.

4.1.2 Man-In-Middle Attack
Man, in middle attacks are not possible on a combination of ECC and DHP. Because of ECC, our system is secure from various types of attack.

$VoIP_I$: $PU_I,N_I,E_{PRI}(META_I)$ where $META_I$ is the hash function of $IP_I,MSISDN_I$ and the public key of the initiator.

$VoIP_R$: $PU_R,N_R,D_{PUI}(E_{PRI}(META_I))$ where the $META_X$ is the hash function from Initiator and sender. Where public key of x = P(the point on EC). private key of x. Because of that features the Man-In-Middle not possible.

4.1.3 Replay Attack
Our message transmission is secure from Replay attack because of use of message ID for each message and Hash of message in given packet Modification and replays attack not possible on this architecture. Message and message ID is encrypted and Hash function. Because of a hash function and ID, the replay attacks not possible. Sender: $E_{KY}(MSG,MSG_{ID},h(MSG))$

Receiver: $D_{KY}(E_{KY}(MSG,MSG_{ID},h(MSG)))$.

4.1.4 Injection Attack
This system fully secure from Injection attacks. Using ECC the high level of security achieves with the minimum size of the key. $E_{KY}(MSG,MSG_{ID},h(MSG))$ and as in Equation the hash message avoid injection attack during the transmission.

4.1.5 Masquerade Attacks
In System are using MSISDN no and IP address of entities so Masquerade attack not possible. Fully secure from measured attack. $META_R = Fun(IP_R,PU_R,MSISDN_R)$ as of given in equation the having same IP and MSISDN is not possible and using the hash value of that key which makes masquerade attack not possible.

4.1.6 Denial of Service Attack
For avoiding DOS attacks System has Rejection, ACK, Message-ID, MSISDN, and IP address in the system if Message hash not matched then rejected and having rejection from same MSISDN system will auto-terminated.

5. CONCLUSION AND FUTURE SCOPE
Existing VOIP is having no security features like encryption and decryption in the architecture of VoIP that mainly uses the SIP and RTP as major parts. During the complete process, anyone can attack the transmitted data.

Proposed System for secure VoIP communication for increased security has following phases

Key Generation: It the DLP for key exchange algorithm with ECC which make impossible to break. Also, highly secure with the small size of a key.

Message Transmission: Provides the security using the created key in Key Generation which makes transmission secure and safe.

This system is secure against popular attacks explain in trail in this paper. Security is achieved by DHP, ECC, ECDDHP and hashing gives prevention from modification of message.

Future scope: The proposed system uses less number of bit key size which gives fast E_X, and D_X which enhances the performance. For mobile ad-hoc devices, change in IP will cause termination of Message Transmission.

This protocol can be applied to UAV (Unmanned Arial Vehicle). To achieve the secure communication with the control center and Warehouse center. ECC is secure and lightweight (minimum computing power) so we can apply to Ad-hoc devices.

ECC can be used to create the secure VPN tunnel for data communication Also, can be used to secure the WhatsApp and Facebook and another internet communication.

6. REFERENCES

[1] Ray, Sangram, G. P. Biswas, and Mou Dasgupta. "Secure multi-purpose mobile-banking using elliptic curve cryptography." *Wireless Personal Communications* 90.3 (2016): 1331-1354.

[2] Ray, Sangram, Rachana Nandan, and G. P. Biswas. "ECC based IKE protocol design for internet applications." *Procedia Technology* 4 (2012): 522-529.

[3] Butcher, David, Xiangyang Li, and Jinhua Guo. "Security challenge and defense in VoIP infrastructures." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 37.6 (2007): 1152-1162.

[4] Ray, Sangram, and G. P. Biswas. "Establishment of ECC-based initial secrecy usable for IKE implementation." *Proc. of World Congress on Expert Systems (WCE)*. 2012.

[5] Ray, Sangram, Urbi Chatterjee, and G. P. Biswas. "Efficient and Secure Communication Architecture for E-Health System."

[6] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender

[7] Hankerson, Darrel, Scott Vanstone, and Alfred Menezes. "Elliptic Curve Arithmetic." Guide to Elliptic Curve Cryptography (2004): 75-152.

[8] Saxena, Neetesh, Bong Jun Choi, and Rongxing Lu. "Authentication and authorization scheme for various user roles and devices in smart grid." IEEE transactions on information forensics and security 11.5 (2016): 907-921.

[9] Braga, A., et al. "Implementation Issues in the Construction of an Application Framework for Secure SMS Messages on Android Smartphones." The 9th Intl. Conf. on Emerging Security Infornation, Systems and Technologies. 2015.

[10] Thomas, Minta, and V. Panchami. "An Encryption Protocol for end-to-end Secure Transmission of SMS." Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on. IEEE, 2015.

[11] Saxena, Neetesh, and Narendra S. Chaudhari. "A secure approach for SMS in GSM network." Proceedings of the CUBE International Information Technology Conference. ACM, 2012.

[12] Miller, Victor S. "Use of elliptic curves in cryptography." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985.