Video/Audio conferencing Security Through Elliptic Curve Cryptography (ECC)

Md Shoaib Alam,
Department of Computer Science & Information Technology, Maulana Azad National Urdu University Hyderabad, Telangana, India

***Abstract*— A video or audio conference has the capacity to host live interactive and collective meeting by existing IP infrastructure by using standardized protocols like the Session Initiation Protocol (SIP) or H.323. It provides visual environment to connect between two or more participants residing in separate locations in the world. In many industry, demands of virtual meeting increasing in every industrial department for the better contribution of the productivity. It brings the participant at different location in world virtually together. It also collaborates with content sharing from one location to another location of the world. Now a day many industries using IP technology to conduct virtual meeting, therefore many security risks involve with video or audio conferencing. In this paper, we purposed ECC (Elliptic Curve Cryptography) algorithm to secure the video or audio conference over IP. It also protects confidential shared information from any eavesdropper during transmission.**

***Index Terms*—Digital Signature, Diffie-Hellman, (Elliptic Curve Cryptography) ECC, Video/Audio conference.**

I. INTRODUCTION

New technologies of video or audio conferencing is saving a lot of amount of money every day; industries or any enterprises are now able to save on travel and accommodation expenses. Any participant can attend the meeting from any part of the office. Moreover, visual meeting needs to be delayed or rattled due to many of the reason like strikes, traffic jams and delayed flights. It assertive to enhanced performance and productivity [9]. A video or audio conference grant us to easier decision making for businesses by eliminating the need to attends a face to face meeting. Decision making can now be done even participant during holiday. It saves industries or any enterprises a lot of money by enabling them to reduce office space requirements rather than downsizing their staff. Money is also saved since the need to rent a huge office space is effectively eliminated since most of the staff can work from home. Besides, industries can now spend less on transport allowances for their employees since less fuel is used while commuting to and from the office. The use of audio or video conference call technology has led to big reduction of auto accidents and time lost from work due to auto related injuries. These new technologies allow instant show of meetings worldwide with little notice. Participant can attend meetings even when they are physically unable to. For instance, in areas where leaders are not allowed to meet due to safety or legal restrictions, these collective communication technologies allow them to continue accommodates and administering without reticence. In today's business world, it is essential for any organization to be professional while creating the impact that the company is adequate and cutting edge. Making use of the latest technology, such as the audio or video conference call can set a company out from the competition and highlight to potential clients that its business is growing at the forefront of the latest trends and business practices.

Manuscript received July, 2017.
Md Shoaib Alam, Department of Computer Science & Information Technology, Maulana Azad National Urdu University, *Hyderabad, India, 939 296 1440*

II. LITERATURE SURVEY

This paper explains the vital of security issues in video and audio conferencing. Through the analysis, the customers and the organization to join those in a single aspect with respect to video and audio conferencing security. By such examination of data, it produces an "extensive" perspective. It will reduce the gap between organization and the customers' objectives and their perceptions. By the far-reaching perspective of investigation, data about customer and the open Internet association execute such arrangement which adjusted the customer needs more viably.

A. Security issues in video and audio conferencing at various levels

1. User and devices security Level

1.1. Active Directory or LDAP (Lightweight Directory Access Protocol: These data is very sensitive, private and critical to the any enterprises, industries, client and partner [2]. To access these database, applicant need to submit queries any one the application to the database. These input validation cause code injections. These attacks causing server security problem in system and application. Attacks with malicious inputs can be attacks on

1.1.1. Confidentiality: revealing information

1.1.2. Integrity: corrupting information

1.1.3. Availability: destroying the information.

1.2. Authentication: It is also called two way authentications. If any intruder eavesdropper or unauthorized user comes between the communicating parties or authorized user and commonly authenticate by them, then this creates problem to authorized users. There is some type of authentication attack [3] [5].

1.2.1. Man-in the middle: Attacker catch the communication channel settled between authorized users and adjust the communication between client and server without their knowledge.

1.2.2. Password discovery attack: Attacker obtain several structures to retrieve password.

1.2.3. Video recording attack: In such type of attack launch in public places and attacks.

1.2.4. Session Hijacking: Session hijacking is very much possible if the session ID issued to the authenticated user or authorized user is not protected properly, which in turn can be used for spoofing identity. These attacks capitalized on the loopholes such as insecure communication protocol and unencrypted data can be circumvent by using a secure communication protocol such as HTTPS, by encrypted files that stores user or administration login credential etc.

1.2.5. Denial of service: The main objective of DOS attacks is to overload the target machine with fake services to prevent it from responding to appropriate request. Unable to handle all the services request on its own, it envoy the work load to other similar services instance which ultimately leads to flooding attacks [5].

2. Network Security Level

It is hard to handle the security management because there are great threats in security management. There are many viruses with high transmission speed on the web, which may cause economic loss.

2.1. NAT (Network Access Traversal): The lack of public IP addresses means corporate networks are commonly structured as private networks, assigning addresses to internal network devices from standard pre-defined address ranges. These private addresses are not reachable from the public Internet making conferencing quite hectic. Network access transversal (NAT) is a popular and well know method for allowing a one-to-many relationship of IP addresses in a corporate network. It maps the private, non-routable IP address of an internal network device to a public, routable IP address and keeps track of requests from machines inside a network to websites outside the network.

To the outside world, all requests appear to come from one IP address, the public address. As information comes back, NAT handles the translation from the one public facing address back into the internal addressing scheme. By performing the translation at the border to the public network, one address can be used for a multitude of machines. Because all communication occurs through the NAT device, the network endpoints are obscured thus, provides a level of security to the network as it is difficult for prying eyes to know how many hosts exist on a network, much less the types of devices located there [6].

Another security consideration is that since the connection to the endpoint must be initiated from inside the network and cannot come from the outside, it is impossible to connect into the network uninvited [6].

This security provided by NAT causes a hassle for audio or video conferencing over IP. A combination of firewall and NAT provide a relatively strong barrier of protection against external intruders. From the audio or video conference perspective, firewalls and NAT keep unauthorized user and systems from connecting to enterprise conference systems. Unfortunately, they can also hamper authorized, required connections between internal and external systems [6].

2.2. Firewall: It is desirable that the packet based networks/H.323/SIP terminal is protected from unwanted external internet access by use of an appropriate firewall [9]. Firewalls are designed to keep certain types of traffic out of a network and are usually expand in strategic points in the network infrastructure, primarily between the public Internet and the corporate network, between branch offices and the corporate network or even between segments of the corporate network. Firewalls can be implemented in either hardware or software, or a combination of both, and are frequently used to prevent unauthorized video conferencing users from accessing private networks, such as intranets, connected to the audio or video conferencing[9].

All data entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. VC systems were designed to work in a few ports thus, opening a large range of ports on the corporate firewall is a risk which, quite rightly, many network security administrators find improper.

3. Data Security Level

Sensitive information emerges as major problems regarding security in primarily based system. Firstly, whenever an information is on a cloud, anyone from anyplace, anytime will access information from the cloud since information could also be common, private and sensitive information in a very cloud. Therefore, at a similar time, several cloud computing service shopper and supplier accesses and modify information. Therefore, there's a requirement of some knowledge, integrity, technique in cloud computing. Secondly, information stealing could be a serious issue in a cloud computing environment [1][6].

Several cloud service suppliers don't give their own server instead they achieve server from alternative service suppliers because of it is price emotive and versatile for operation and cloud supplier. Therefore, there's a way chance of information is taken from the external server. Thirdly, knowledge loss could be a common downside in cloud computing. If the cloud computing service provider back up his services due some money or legal downside, then there will be a loss of knowledge for the user. Moreover, information is lost or injured or corrupted due to miss happening, natural disaster, and fire [1][6].

Because of higher than condition, information might not be accesses able to users. Fourthly, information location is the problems what needs focus in a cloud computing environment. Physical location of information storage is incredibly necessary and crucial. It ought to be clear to user and client [1].

B. Security approaches for video and audio conferencing at various levels

1. Application System level

1.1. Confidentiality: It analyze that only authorized users can access the information in the system.

1.2. Integrity: It tells that only authorized users can change any information over the network.

1.3. Anonymity: It is important to develop techniques which provide receiver, sender and exchanges of data anonymity.

1.4. Availability: Almost all video and audio conferencing applications require of trusted party such as Key Distribution Center (KDC) for Distribution of public key, it removes the problem of denial of service attack.

2. Encryption Technology Level

This technology change the readable text or plain text into unreadable text which helps to protect the data from being viewed and it also offers a technique to detect whether the receiving data is modified or not. Encryption technology offers secure communication over unsecure network. We classify encryption techniques in two ways per the used key [2][7].

2.1. Symmetric Key Encryption: It is also called the private key cryptography or private key encryption. In this, we use same key for message encryption and decryption. This key (r) is also called secret key [3][9].

2.2. Asymmetric Key Encryption: It is also called the public key encryption. In asymmetric key cryptography, we use two keys, one for encryption method and other key for decryption method. One key is Public and second one is private. Public key is known to all communication party in networks and private key is secret [3][9].

C. Comparative Analysis of key size and time

Comparisons of key sizes of symmetric and asymmetric cryptography algorithms are given in table 1 and figure 1. The key size of Elliptic Curve Cryptography algorithm is approximately 5 times less compared to RSA algorithm and also the ECC security level is higher than RSA. ECC algorithm takes less time to encrypt the message as compare to RSA algorithm. As indicated by breakdown time reckoning in table 1, ECC algorithm is more powerful and secure than RSA algorithm [3][8].

ECC		RSA	
Key Size (in bits)	Key Generation (in time)	Key Size (in bits)	Key Generation (in time)
163	0.08	1024	0.16
233	0.18	2240	7.47
283	0.27	3072	9.8
409	0.64	7680	133.9
571	1.44	15360	679.06

Table 1. Comparative Analysis of Key Sizes and time

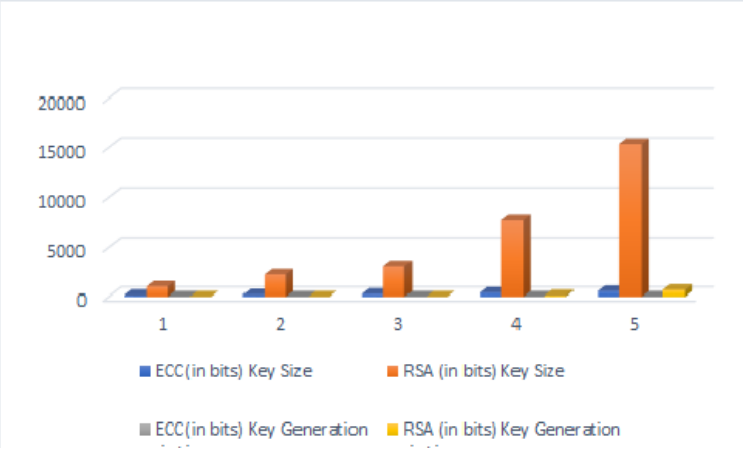


Figure 1. Breakdown Time Computation of ECC and RSA

3. PROPOSED MODEL

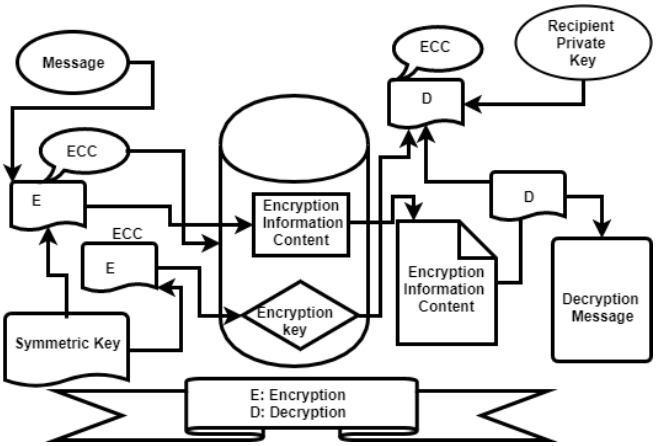
To design an audio and video conferencing structure with effective security steps, we need analyses the audio and video transaction (Sharing the content).

A. *Working of Proposed Model*

We designed a model to under the secure algorithms like ECC. You know that secure for transaction purpose in the audio and video conferencing but it is not successful in the audio and video conferring environment because it has a lot of deficiency.

1. message is exchanged between participant.
2. digital signature is computed
3. There are encryption/decryption cycles and
4. certificate verification.

Because of this, we proposed a model to secure the conferencing transactions. Suppose, we have shared information. We encrypt the information by ECC algorithm and send the encrypted participant to Internet open network. These encrypted messages data are mix with each by ECC algorithm and the private key of the recipient will decrypt the encrypted content. In such ways, receiver gets information.



B. Mathematical Simulation:

Suppose one participant needs to make the audio or video call and shared the content like images or doc file or any confidential data.

For shared content encryption, we use ECC algorithm. Suppose message is M (7, 9). The following steps show how the message encrypt and decrypt by the ECC algorithm.

Generation of Key:
Randomly select private key r ϵ [1, n-1], r = 17
Suppose Sender choose base point T = (2, 7) in E_{11} (1, 6).
S = r*T = 17(2, 7) = 17G = 13G+4G = 4G
Public key: S = (10, 2)

Encrypt the message:
Cipher text: C_1=rT, C_2=M+qS
Let's take the random number q = 19
Message: M (7, 9)
C_1 = rT = 19(2, 7) = 19G = 13G+6G = 6G
C_1 = (7, 9)
C_2 = M+qS = (7, 9) + 19 (10, 2) = 6G+76G = 4G
C_2 = (10, 2)

Decrypt the message:
Plaintext: M = C_2 - (r*C_1)
M = (10, 2) – 17*(7, 9) = 4G – 17*6G = 4G – 102G = -98G = -7G = - (7, 2)
M = (7, 9)

Diffie-Hellman Secret Key Exchange Using ECC

Sender and Receiver choose Elliptic curve E_{11} (1, 6) and a base point T (2, 7) on the curve.

1. Sender chooses a secret integer I_S = 9 i.e. I_S < I (I=13) G.
2. Sender generates point:
   $H_S = I_S*T = 9(2, 7) = 9G = (10, 9)$ on the elliptic curve. The Sender sends H_S to the Receiver.

3. Receiver chooses a secret integer I_R = 12 i.e. I_R < I
4. Receiver Generates point

   $H_R = I_R*T = 12(2, 7) = 12G = (2, 4)$ on the Elliptic curve. The Receiver sends H_R to the Sender.

Sender and Receiver calculate a shared secret key:

$\boldsymbol{Q_{sender}} = I_S*H_R = 9(2, 4) = 108G = 104G+ 4G = 4G$
$\mathbf{Q_{sender}} = (10, 2)$
$\mathbf{Q_{receiver}} = I_R*H_S = 12(10, 9) = 12*9G = 108G = 104G+4G = 4G$
$\mathbf{Q_{receiver}} = (10, 2)$
$\mathbf{Q_{sender}} = \mathbf{Q_{receiver}} = (10, 2)$

4. CONCLUSION

The aim of this paper has to enhance the audio and video conferencing security through dual signature. Our proposed model focused on some point like the security, its cost and the time consumption. We used ECC algorithm which is most secure and less time engrossing. It will control all the encryption and the decryption with the help of private and public key of sender and the receiver.

REFERENCES

[1] Singh, B., K.s., J.: Security Management in Mobile Cloud Computing: Security Management in Mobile Cloud Computing. 148–168.
[2] LDAP Injection & Blind LDAP Injection - Black Hat, https://www.bing.com/cr?IG=55CFF1389D0444A386E14D01E75AFF3F&CID=05DCEF4D10BB67BA2019E58E11BD6672&rd=1&h=Fa9LcTdGEAqEWEaPSdEiQbZCVj3cc5rxh6_K6EsKB10&v=1&r=https%3a%2f%2fwww.blackhat.com%2fpresentations%2fbh-europe-08%2fAlonso-Parada%2fWhitepaper%2fbh-eu-08-alonso-parada-WP.pdf&p=DevEx,5062.1.
[3] Piedra, A.D.L., Braeken, A., Touhafi, A.: A performance comparison study of ECC and AES in commercial and research sensor nodes. Eurocon 2013. (2013).
[4] Analysis of Cryptographic Algorithms, http://www.academia.edu/6829046/Analysis_of_Cryptographic_Algorithms.
[5] Authentication Attacks in Cloud computing: A survey, http://docplayer.net/3212277-Authentication-attacks-in-cloud-computing-a-survey.html.

[6] Balboni, P.: Data Protection and Data Security Issues Related to Cloud Computing in the EU. ISSE 2010 Securing Electronic Business Processes. 163–172 (2011).
[7] Hemalatha, N., Jenis, A., Donald, A.C., Arockiam, L.: A Comparative Analysis of Encryption Techniques and Data Security Issues in Cloud Computing. International Journal of Computer Applications. 96, 1–6 (2014).
[8] Benefits of Elliptic Curve Cryptography, http://www.bing.com/cr?IG=F2F8EADAA1DA4ACE8A3FCF6279360B9F&CID=3F388FB1E71A6ED017438572E61C6FBE&rd=1&h=yNN_wHGlJ09wPkRNQA10DXfoC82OsNG6KuAlih91ZD0&v=1&r=http%3a%2f%2fwww.securitydocumentworld.com%2fcreo_files%2fupload%2fclient_files%2fgov_wp_ecc1.pdf&p=DevEx,5061.1.
[9] IP BASED SECURITY ON VIDEO CONFERENCING (PDF Download ..., https://www.bing.com/cr?IG=C0A9CAEEF9E140828F12C518051375A0&CID=3B7F7154971F6D2F0DEE7B9796196C42&rd=1&h=Fj0tg9zNo5AYxB8cywX1rC5jY3uwg3gqvmT0VuX9HCQ&v=1&r=https%3a%2f%2fwww.researchgate.net%2fpublication%2f251237171_IP_BASED_SECURITY_ON_VIDEO_CONFERENCING&p=DevEx,5061.1.
[10] Digitalsignature [online] http://simple.wikipedia.org/wiki/Digital_signature (Last accessed 12 Sept 2013).
[11] Liu, Jiangchuan, Sanjay G. Rao, Bo Li, and Hui Zhang. "Opportunities and challenges of peer-to-peer internet video broadcast." Proceedings of the IEEE 96, no. 1 (2008): 11-24.
[12] Chawathe, Yatin, Steven McCanne, and Eric Brewer. "An architecture for internet content distribution as an infrastructure service." Unpublished, available at http://www.cs.berkeley.edu/yatin/papers (2000).
[13] Chu, Yang-hua, Sanjay G. Rao, Srinivasan Seshan, and Hui Zhang. "A case for end system multicast." IEEE Journal on selected areas in communications 20, no. 8 (2002): 1456-1471.
[14] Francis, Paul. "Yoid: Extending the internet multicast architecture." (2000).
[15] Chu, Yang, Sanjay Rao, Srinivasan Seshan, and Hui Zhang. "Enabling conferencing applications on the internet using an overlay muilticast architecture." ACM SIGCOMM computer communication review 31, no. 4 (2001): 55-67.
[16] Luo, Chong, Wei Wang, Jian Tang, Jun Sun, and Jiang Li. "A multiparty videoconferencing system over an application-level multicast protocol." IEEE Transactions on Multimedia 9, no. 8 (2007): 1621-1632.
[17] Chen, Minghua, Miroslav Ponec, Sudipta Sengupta, Jin Li, and Philip A. Chou. "Utility maximization in peerto-peer systems." In ACM SIGMETRICS Performance Evaluation Review, vol. 36, no. 1, pp. 169-180. ACM, 2008.
[18] Ponec, Miroslav, Sudipta Sengupta, Minghua Chen, Jin Li, and Philip A. Chou. "Multi-rate peer-to-peer video conferencing: A distributed approach using scalable coding." In 2009 IEEE International Conference on Multimedia and Expo, pp. 1406-1413. IEEE, 2009.
[19] Koh, Eunyee. "Conferencing room for telepresence with remote participants." In Proceedings of the 16th ACM international conference on Supporting group work, pp. 309-310. ACM, 2010.
[20] Isaacs, Ellen A., and John C. Tang. "What video can and cannot do for collaboration: a case study." Multimedia Systems 2, no. 2 (1994): 63-73.

Mr. Md Shoaib Alam

Mr. Md Shoaib Alam is an M. Tech Computer Science student at the Department of Computer Science & Information Technology, Maulana Azad National Urdu University, Hyderabad, India. He had completed his B.Tech from Rashtrasant Tukadoji Maharaj Nagpur University, India. He had worked 5 years as a software engineer in the reputed MNCs viz. Tata Business Support Services, Tausch Technologies Private Limited and Polycom IIC (R & D) center Private Limited. He had official visit to UAE as a software developer.