I.J. Education and Management Engineering, **2015, 3, 9-20**
Published Online July 2015 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2015.03.02

Available online at http://www.mecs-press.net/ijeme

Implementation of Non-Repudiation Services in Digital Video Generation & Distribution on Android Devices

Pooja Gupta [1], Ankita Lavania [1], Madhuri Agarwal [1] & Dr. Vrijendra Singh [2]

Associate Professor IIIT Allahabad

Abstract

With the onset of Digital age, digital videos have been highly prevalent in every sphere of our lives and have replaced other sources of entertainment, information sharing & social interaction. With the increasing use of Mobile devices, Internet & its application it has been quite evident that digital videos are generated and distributed with ease. Quite often such videos are used as evidence depending on the kind of information they provide. Since the video has been distributed at a large level it becomes very difficult to identify the generator device of the digital video especially if the case is of objectionable video contents etc. This paper aims at proposing a framework which will embed the generator device information in the video & will make sure the user identification information can't be changed during the distribution process using internet or other networking services (i.e. Bluetooth).

Index Terms: International Mobile Equipment Identity, International Mobile Subscriber Identity, Non-Repudiation, Elliptic Curve Cryptography.

1. Introduction

With innovations and development in the field of multimedia, their sharing over internet or other networking equipments using portable devices, it is required to affirm the origin and authenticity of videos [1]. Using smart phones and tablets anyone can anywhere record videos and share it with others, using internet within minutes it spreads without knowing where it came from and if it is original. In this paper we embed the user identification information which includes device and service provider information, with the video during its creation or editing. The method that we propose can be used as a library module with the video recording and editing software to perform the encryption and decryption of user identification operation.

This body of research can be of immense help in legal proceedings where digital videos are used as evidence to establish the non- repudiation of digital video. It takes into consideration every possible scenario that can be

* Corresponding author. Tel: +91-7376581984
E-mail address: ankita.lavania003@gmail.com, madhuri.agarwal21@gmail.com, pooja07061990@gmail.com, vrijendra.singh@gmail.com

encountered during the video generation & distribution & the role of digital video as legal evidence. Through this research work we also aim to reduce the search space for digital video creation when it is used as legal evidence.

For implementing security in the proposed model, the user & device information being embedded in the video codec has been encrypted using ECC (Elliptic Curve Cryptography) [10].Elliptic curve cryptography allows to achieve the security in the framework proposed as well as gives the freedom to implement it on devices with constraint energy requirements such as mobile devices or PDAs. The Elliptic curve cryptography algorithms can be implemented in order to achieve the generation of public/private key pair or digital certificate for signature generation & verification.

The objective of this body of research is to propose something innovative in the field of mobile & multimedia technology which can be useful in our day to day lives. There is an urgent need to address the problem of non-repudiation in digital videos generation & distribution because in the absence of such a mechanism to address this issues there have been cases in which offensive & demeaning digital videos have been circulated in the cyber space & nothing can be done to catch the culprits who are responsible for the generation of such digital videos. Certainly there is a strong need to address this grave issue & propose a concrete solution to handle such a situation when it arises either from technological point of view or from legislative point of view. As seen from the legislative view , in the absence of any technical evidence against the culprits in such cases they are set free & continue to live in the society despite committing heinous crime against the individual & society as whole. We have attempted to address the issues in its entirety & have tried to cover the issues in its lengths from every possible technical perspective. The framework which has been proposed has stages in a waterfall model fashion, which cover the different steps which can to be followed for the achievement of non-repudiation in digital videos generation & distribution.

2. Elliptic Curve Cryptography

Elliptic Curve Cryptography is a public key cryptosystem like Diffie-Hellman and RSA [15]. ECC is suitable for digital signature, key exchange and agreement protocols. ECC has speed and security advantages over RSA and Diffie-Hellman [18].It is a replacement for problems found in other public key algorithms like discrete log used in DSA and integer factorization in RSA. The security level of 1024 bits key size of RSA can be achieved by 160 bits of ECC [12]. Computationally also it is much faster and thus suitable for devices with limited computation capability like mobile devices [3]. Being a light weight cryptosystem in terms of speed and security it works well for constrained devices like mobile phones [18]. ECC is a kind of public-key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA, can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of a RSA could be offered by 163 bit security strength of ECC. Other than this, ECC is particularly well suited for wireless communications, like mobile phones and smart cards. EC point of multiplication operation is found to be computationally more efficient than RSA exponentiation [21].

The elliptic curve used for key generation and Encryption/Decryption is defined over prime field FP (where p is a large prime number). (a, b) are curve parameters and are smaller than p[10]. The equation used to generate the points of the curve, given values a, b and p is:

$$y^2 = x^3 + ax + b, \; where \; 4a^3 + 27b^2 \neq 0$$

$$E = \{(x, y); \; y^2 \; mod \; p = (x^3 + \mathrm{a}x + \mathrm{b}) \; mod \; \mathrm{p}\}$$

By varying values of (a, b) different curves can be generated. Generator point G is a point on the curve selected using an algorithm or simply the lowest valued point. G is used in key generation algorithm.

2.1 ECC Algorithms

Following are the algorithms used for ECC curve generation, key generation and Encryption/Decryption process. The elliptic curve used for key generation and Encryption/Decryption is defined over prime field FP (where p is a large prime number). (a, b) are curve parameters and are smaller than p [11].

$$y^2 = x^3 + ax + b, \; where \; 4a^3 + 27b^2 \neq 0$$

$$E = \{(x, y); \; y^2 \; mod \; p = (x^3 + ax + b) \; mod \; p\}$$

a) ECC algorithm to generate points of the curve:

```
{
 x=0
  While(x<p)
   {
      Compute (x3+ax+b) mod p;
      Calculate different values of y^2 mod p equal to above value;
      Compute square root of y;
      Find all values of (x, y) on the curve;
   }
}
```

b) Generate Public and Private Key:

```
{
      Select a random number K for Private Key;
      Select Generator point G from above calculated points;
      Public key Kp is K multiplied by G (using ECC point multiplication algorithm);
}
```

c) Points Multiplication:

```
{
For doubling a point P to 2P whose coordinates are (XD, YD) -
      M = [(3x2 + a) / 2yp] mod p;
      XD = (M2 - 2x) mod p;
      YD = [M (x - XR) - y] mod p;

For 3P, use P + 2P and 2P=Q. P has Coordinates (X, Y), and Q has coordinates (XQ, YQ) -
      M = [(YQ-Y) / (XQ-X)] / mod p;
      P+Q=-R;
      XD= (M2-X-XQ) mod p;
      YD= (M(x-XD)-y) mod p;
}
```

d) ECC text Encryption Algorithm:

{
Convert the message string in ASCII, M;
Select a random number r, P=r*G is a point on the curve;
Multiply ASCII value and P to get another point Q (using ECC point multiplication algorithm);
Cipher text = {P, Q + r*Kp};
}

e) Decrypting Text:

{
From above –
M = Q + r*Kp – P*K;
Convert the ASCII to string to get the message;
}

3. Android

The implementation on the proposed framework has been done on android platform [17]. Certain identification parameters have been used which can be successfully fetched and used in android platforms.

3.1 Unique Identification Information

In the framework proposed the parameters that we consider for unique identification of the mobile device used to capture or edit a video are given below. The information uniquely identifying the device is:

- **a** **IMEI (International Mobile Equipment Identity):** IMEI is unique for all devices with SIM card (MEID in case of CDMA devices) and dual SIM devices have two IMEI numbers. Devices with no SIM card have another unique device identification number like ESN.
- **b** **WLAN MAC Address String:** The address string uniquely identifies the wireless network interface for communication with the network.
- **c** **Bluetooth Address String:** The address string uniquely identifies the Bluetooth network interface for communication with the network.

The unique identification parameter of SIM is:

- **a** **IMSI – International Mobile Subscriber Identity:** It is a 15 digit number provisioned in the SIM card that is unique for each SIM from the subscriber. The number can be broken into parts to identify subscriber, country code, and unique serial number for the subscriber.

Algorithms used for implementation of the framework on Android platform are as follows:

a) Algorithm to check root status of device

{

Check builds information for “test-keys”;
Check system files for “Superuser.apk” file;
Check internal and external storage system bin files for a file named “su”;
Try executing command as super user “which su”;
If any of above checks is positive, the device is rooted;
}

3.2 Implementation of ECC on Android

Java has inbuilt APIs available for implementing cryptographic algorithms. As Android is Java based it uses the same API but Android being designed for Smartphone it does not contain all libraries. We used third party library by SpongyCastle which provides ECC APIs of service provider BouncyCastle [16].These third party libraries helped us to implement the framework we have proposed on android platform. These APIs provide the ease of using cryptographic algorithms without the complexity of implementing them this is a true example of data abstraction.

4. Proposed Framework

The proposed framework aptly depicts the flow of steps to be followed for the implementation of Non-Repudiation Services in digital video generation & distribution. The proposed model has been designed into five parts.

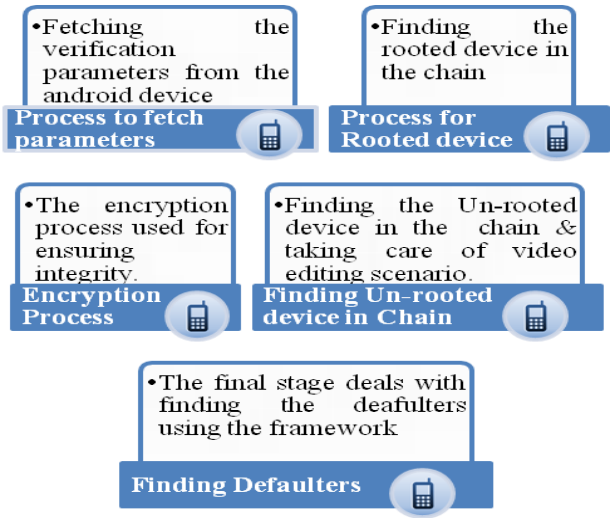

Fig.1. The different stages of the proposed Framework

The different stages of the model work as follows:

- **Stage 1:** The first stage simply describes the process for fetching the validation parameters. Once we capture the video, the parameters such as IMEI, ICCID, IMSI, Wi-Fi & Bluetooth Mac address are

fetched and embedded in the video. Then it is checked whether the device is in root state or not. If the device is in root state then Stage 2 is refereed else stage 3 is referred [5].

- **Stage 2:** If a rooted device is encountered then all the IDs configured in the system are fetched. If Google ID is available then it is also used along with other parameters. Else any other ID such as Twitter or Viber ID is used. Then the data is carry forward to the next stage i.e. encryption.
- **Stage 3:** The next stage is encrypting the embedded information. Firstly a sting of all the fetched information and timestamp is created. Then the string is encrypted using ECC algorithm with user public key. This information is then hidden in the video using video Steganography [17]. Video Steganography is the process of covertly hiding some secret data into video files [19]. This data hiding is done in such a way that it is not recognizable to the end user of the video file. Then the signature is embedded in the video.
- **Stage 4:** This stage takes care of finding an un-rooted device in the chain. Also editing or morphing of the video has also been taken care of in this stage [7]. Firstly it is checked if the video has been edited or not. If not then it is checked if the video has been forwarded using a rooted or un-rooted device. If not then do nothing else the process traces back to stage 1 or 3.
- **Stages 5:** This Stage takes care of the fact that how the whole process will be helpful in finding the defaulters. First a request needs to be sent to the device manufacturer requesting him to share the information stating valid reasons for it. Manufacturer can extract and decrypt the information using the user's private key. If the fetched string contains root status embedded parameters are discarded like IMEI, ICCID etc since they are not unique in root state. In such a case account IDs can be used. If the device is not found in root state then embedded information like IMEI , ICCID , IMSI , Wi-Fi & Bluetooth MAC address etc are used for verification purposes.

4.1 Process to fetch parameters

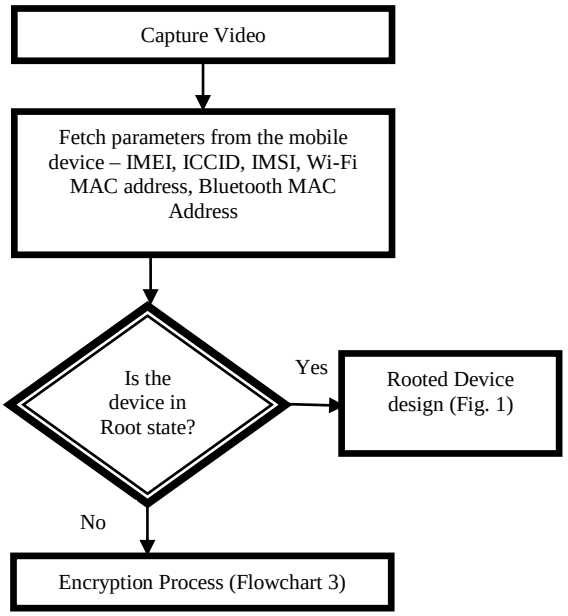

Fig.2. Proposed Framework

6.2 Process for Rooted device

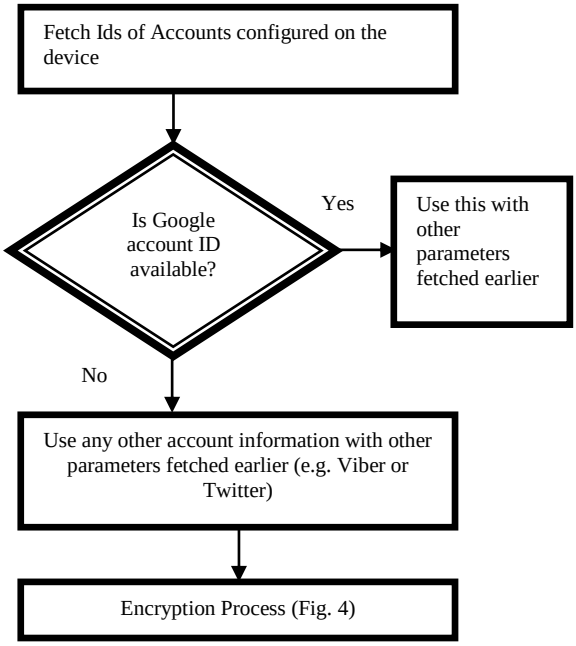

Fig.3. Framework for rooted device

6.3 Encryption Process

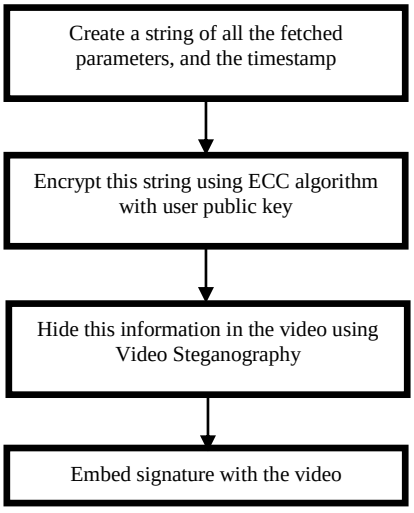

Fig.4. Encryption Process

6.4 Un-Rooted Device in the chain and Video Editing

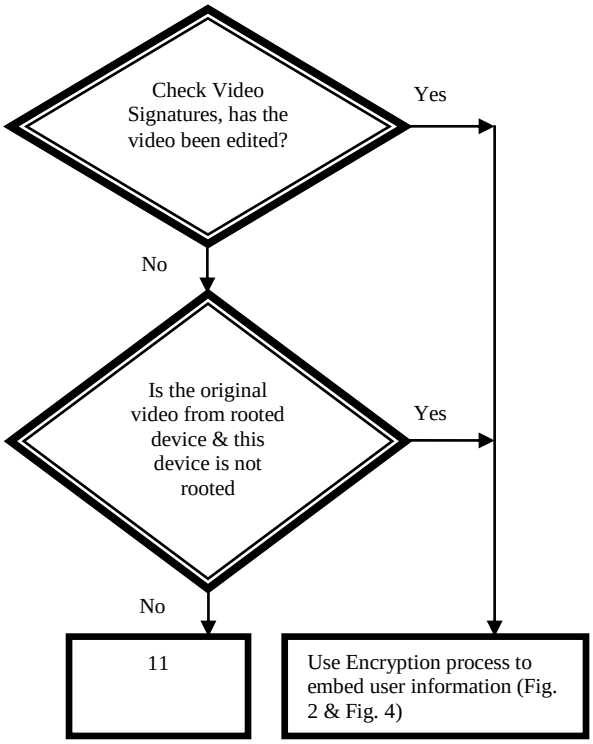

Fig.5. Process for un-rooted device in the chain

6.5 Finding Defaulters

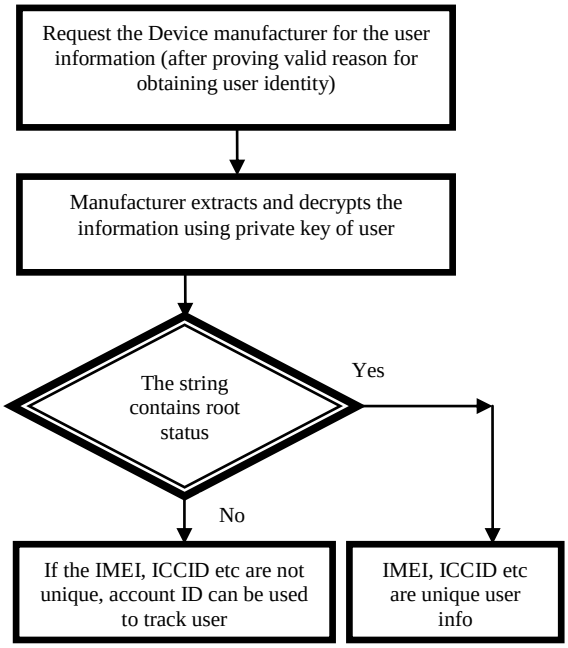

Fig. 6: Catching Defaulters Process

5. Probabilistic Model: How Reduction in Search Space is achieved?

The search space will be reduced in the scenarios where the digital video has been used as an evidence for legal proceedings .The probability of device being in root state is very less. Hence the search space is reduced. The Poisson probability model can be applied in this scenario because if the probability p is so small that the function has significant value only for very small x, then the distribution of events can be approximated by the Poisson distribution.

The Poisson distribution can be used to calculate the probabilities of various numbers of "successes" based on the mean number of successes. In order to apply the Poisson distribution, the various events must be Independent.

The probability distribution of a Poisson random variable X represents the number of successes occurring in a given time interval or a specified region of space is given by the formula:

$$p=e^{-\mu}\ \mu^{x} / x!$$

Where,

E is the base of natural logarithms (2.7183)

μ is the mean number of "successes"

x is the number of "successes" in question.

In this scenario the success is defined by finding a device in root state. The various events of finding the device in root state are independent of each other.

Let us assume that the digital video is being distributed or forward to 100 android devices & the number of devices found to be root state in the chain is 2.So the probability of finding a device in root state is:

$$P=2/100=.02$$

If during any legal investigation procedure the search space is found to be 1000 devices which means, it is discovered that the digital video containing objectionable content has been forwarded to 1000 android devices then the probability distribution can help the judiciary in finding the probability of the sample space containing exactly n rooted devices

Let us consider n=10 as example. Than the probability can be calculated as

$$\mu=.02\times1000=20$$

The probability of getting 10 rooted devices is

$$P(X) = ((e\text{^}-20) * 20\text{^}10) / 10 ! =.00581630$$

The probability of getting 10 rooted devices in a sample space is .00581630, which is very low. So, during the investigation process the complexities involved while using a rooted device as evidence are reduced.

6. Discussion & Conclusion

The use of Digital videos is highly prevalent in our lives in today's era. Sometimes these digital videos are also used for offensive & demeaning purposes. In such cases these video have legal implications & cam be used as digital evidences in court of law. But again it becomes difficult to identify the generator of the digital video once the video is widely spread in the digital world with the help of technologies like internet or Bluetooth. This body of research address the issues & purposes a framework that will be useful in

implementation of non-repudiation services in digital videos i.e. the generator of the video could not deny the fact that he/she generated the video. The framework addresses many technical issues that can be encountered within the process of implementation of non-repudiation services in the digital video.

7. Future Scope

The proposed model, if implemented, can be highly successful against demeaning and offensive video being circulated using internet & Bluetooth services. It is a heinous crime against individual and can cause serious defamation to the individual or society as whole.

Culprits usually walk free in absence of evidence against generation of the video. This model can help to get a hold against this malpractice.

Legal proceedings can also be benefitted by the evidence which this model may help in collecting against the real culprits.

References

[1] Saurabh Upadhyay, Sanjay Kumar Singh, *Video Authentication- An Overview,* International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[2] Dinesh Goyal,Naveen Hemrajani, *Novel Selective Video Encryption for H.264 Video,* International Journal of Information Security Science D. Goyal, N. Hemrajani ,Vol. 3, No. 4.

[3] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Eric Wustrow, *Elliptic Curve Cryptography in Practice.*

[4] KANEKO Hiroshi, OZAWA Takato, NOMURA Toshiyuki, IWAMOTO Kota, *Video Identification Solution Using a "Video Signature".*

[5] Xiaochun Cao 1, Siyuan Li 1, Feng Jiang 1, Hua Zhang 1, Ling Du1,Xiangui Kang, *Device identification Based On H.264 Cues.*

[6] Thomas Wiegand, Gary J. Sullivan, Gisle Bjøntegaard, Ajay Luthra, *Overview of the H.264/AVC Video Coding Standard,* IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 7, July 2003.

[7] Sabu Emmanuel, Mohan S. Kankanhalli, *Digital Rights Management Issues for Video.*

[8] Nicholas D. Beser, Thomas E. Duerr, Gregory P. Staisiunas, *Authentication of Digital Video Evidence.*

[9] Saurabh Upadhyay, Sanjay Kumar Singh, *Video Authentication: Issues and Challenges,* IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 3, January 2012.

[10] Joseph H. Silverman, Brown University, *An Introduction to the theory of Elliptic Curves.*

[11] Qiong Pu, Xiuying Zhao and Jianmin Ding Department of Electronics, Science Institute, Information Engineering University, Zhengzhou, He'nan, China , *Cryptanalysis of a Three-party Authenticated Key Exchange Protocol Using Elliptic Curve Cryptography.*

[12] Sahbuddin Abdul Kadir, Arif Sasongko, Muhammad Zulkifli Electrical Engineering, Bandung Institute of Technology Ganesha 10, Bandung, Indonesia , Simple Power *Analysis Attack Against Elliptic Curve Cryptography Processor on FPGA Implementation*, 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[13] BAI Qing-hai1, 2, ZHANG Wen-bo1, JIANG Peng1, LU Xu1, 1.Department of Computer Science and Technology, Jilin University, Changchun 130012, P.R.China 2. College of Computer Science and Technology, Inner Mongolia University for Nationalities, Research on *Design Principles of Elliptic Curve Public Key Cryptography and Its Implementation,* 2012 International Conference on Computer Science and Service System.

[14] Dinesh Goyal, Naveen Hemrajani , Department of Computer Science and Engineering, Suresh Gyan Vihar University, Jaipur, India Department of Computer Science and Engineering, JECRC University, Jaipur, India, *Novel Selective Video Encryption for H.264 Video*, INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE D. Goyal, N. Hemrajani ,Vol. 3, No. 4.

[15] *Point Generation And Base Point Selection In ECC: An Overview* Moumita Roy, Nabamita Deb, Amar Jyoti Kumar M Tech. Student, Information Technology, GUIST, Guwahati, India Asst. Professor, Information Technology, GUIST, Guwahati, India M Tech. Student, Information Technology, GUIST, Guwahati, India.

[16] *Implementing ECC with Java Standard Edition* V. Gayoso Mart´ınez1 and L. Hern´andez Encinas Information Security Institute (ISI), Spanish National Research Council (CSIC), Madrid, Spain victor.gayoso@iec.csic.es; 2luis@iec.csic.es, International Journal of Computer Science and Artificial Intelligence Dec. 2013, Vol. 3 Iss. 4, PP. 134-142 DOI: 10.5963/.

[17] *Real Time Implementation of Secured Multimedia Messaging Service System using Android* Geetanjali R. Kshirsagar, Savita Kulkarni , Department of Electronics, Maharashtra Institute of Technology, Pune , Department of Electronics and Telecommunication, Maharashtra Institute of Technology, Pune.

[18] *Securing MMS with High Performance Elliptic Curve Cryptography*, Prof. B. N. Jagdale Prof.R.K.Bedi Sharmishta Desai Assistant Professor, Assistant Professor, PG Student, IT Department, MIT COE, Comp Department, MIT COE, IT Department, MIT COE, Pune, India. Pune, India. Pune, India.

[19] *Framework for media data and owner authentication based on cryptography, Watermarking and biometric authentication* J. Dittmann, M. Steinebach, L. Croce Ferri, C. Vielhauer, R. Steinmetz, Petra Wohlmacher.

[20] *Wireless Network Security Using Elliptic Curve Cryptography* , Hero Modares Department of Computer system and technology University of Malaya, KualaLumpur, Malaysia hero.modares@gmail.com, Amirhossein Moravejosharieh Department of Computer system and technology University of Malaya KualaLumpur, Malaysia, Amirhosein.moravej@gmail.com, Rosli Salleh Department of Computer system and technology University of Malaya Kuala Lumpur, Malaysia rosli_salleh@um.edu.my

[21] *ELLIPTIC CURVE CRYPTOGRAPHY AND ITS* APPLICATIONS Moncef Amara 1 and Amar Siad 2 Universit´e Paris-8, laboratoire LAGA, Saint-Denis / France , amara moncef@yahoo.fr , siad@math.univ-paris13.fr

Author(s) Profile

Ankita Lavania: Post graduate student at Indian Institute of Information Technology, Allahabad Specialization in cyber law & information Security.

Madhuri Agarwal: Post graduate student at Indian Institute of Information Technology, Allahabad Specialization in cyber law & information Security.

Pooja Gupta: Post graduate student at Indian Institute of Information Technology, Allahabad Specialization in cyber law & information Security.

Dr. Vrijendra Singh: Associate Professor at Indian Institute of Information Technology, Allahabad.

How to cite this paper: Pooja Gupta, Ankita Lavania, Madhuri Agarwal, Vrijendra Singh,"Implementation of Non-Repudiation Services in Digital Video Generation & Distribution on Android Devices", IJEME, vol.5, no.3, pp.9-20, 2015.DOI: 10.5815/ijeme.2015.03.02