IDENTITY BASED DRM SYSTEM WITH TOTAL ANONYMITY AND DEVICE FLEXIBILITY USING IBES

Sharath Palavalli, U S Srinivas and Alwyn R Pais
Department of Computer Engineering
National Institute of Technology Karnataka, Surathkal, Srinivasnagar (PO), India-575025
Email: palavalli.sharath@gmail.com

KEYWORDS

Digital Rights Management System, Identity Based Encryption System, Smart card based DRM System, Total anonymity

ABSTRACT

Most of the Digital Rights Management (DRM) systems fail to cover all requirements like user anonymity, user fairness, security and others. Device based DRM systems, adopted by most providers, lack user fairness and mostly follow proprietary formats. On the contrary, Smart Card DRM systems satisfy user anonymity and fairness, but have certain vulnerabilities, as identified in this paper. We propose a DRM system using Identity Based Encryption System (IBES) that overcomes the deficiencies and vulnerabilities of the existing DRM systems. The proposed DRM system is an approach towards an open framework, wherein, the content processing application can be independent of the DRM provider, and the security is controlled with the help of the smart cards.

INTRODUCTION

Digital Rights Management (DRM) Systems are used to protect and manage digital content. DRM is basically an aggregation of Security Technologies to protect the interest of content owners so that they may maintain persistent ownership of their content (William and Chi-Hung, 2004). Content owners are concerned regarding the content security of individual items, e.g., pictures, videos, music, e-books, programs and games. The rampant piracy that was witnessed in the heyday of the Internet, with sharing of copyrighted videos and music, has driven the industry toward the digital rights management of content. This implies that the rights of viewing (or listening, reading, or forwarding) of each item can be controlled by the license holders, using, for example, a server that administers the rights. The rights can be administered in a number of ways, including (Amitabh, 2007):

- who can view the content,
- how many times the content can be viewed,
- at what time the rights to view content expire,
- in which geographical area the content can be viewed,
- on what devices the content can be viewed,
- restrictions on forwarding of content, and
- renewal of rights through payment mechanisms.

This mechanism of management of rights for content has given birth to the technology of digital rights management or DRM. DRM creates an essential foundation of trust, between authors and consumers, that is a prerequisite for robust market development. The desired requirements of a DRM system can be summarized as follows:

- Non-Restrictiveness
  - Device mobility
  - Communication networks Interoperability
  - Off-line usage (As applicable)
- Content Security
- Key/License management
- Consumer privacy/Anonymity
- Rights persistence
- Versatility/Content Format independent
- Monitoring/Traceability and Accountability
- Choice of multiple security levels

DRM Systems can be categorized into Device-based and Identity-based systems. Basically, the security of a Device based DRM comes from enforcing usage of compliant players and unique global device identifiers. A consumer purchasing some digital content from a server will be given a license. The license will explicitly specify the device on which the content can be used. These systems restrict user flexibility in moving content across different devices and also do not provide user/device anonymity.

Identity based DRM systems differ from device based DRM systems in the license description. Here the license would contain a user identity, which the user would prove to the application by means of a password, fingerprint scan, smart card, etc. Although in these systems the user can move content to any device, user anonymity is lost.

Proceedings of the 2008 High Performance
Computing & Simulation Conference ©ECMS
Waleed W. Smari (Ed.)
ISBN: 978-0-9553018-7-2 / ISBN: 978-0-9553018-6-5 (CD)

To overcome this deficiency of identity based DRM systems, Hung-Min Sun et al proposed an IP based DRM system (Hung-Min et al., 2006), wherein the IP (Internet Protocol address) of the user device would be used as the identity. Although this does provide considerable user anonymity, it still can be traced back, and the approach for user fairness is accomplished in a very complex and tedious manner. Also, there is an enormous dependence on the content processing application for license validation, which decreases the system security.

A Smart card-based DRM system provides the users with more flexible usage of contents and fulfills the consumers' expectations according with "fair use" (Erickson, 2003) in the real world. Privacy has an equally important consideration. Anyone, including the server, should not know the relationship between the users and the contents. More precisely, the identity of a user for the purchased content should be anonymous, even to the servers. Besides, eavesdropping on the user-device communication channel, to the extent possible must be prevented, none the less, should not reveal any relation between the user and the content when intercepted. Conrado et al propose a Smart card based DRM system (Conrado et al., 2003) wherein the smart card acts as the user authentication device. Using the smart card provides a certain level of user anonymity and user fairness in terms of device mobility. Hung-Min Sun et al (Hung-Min et al., 2007) enhance this system to provide stronger user anonymity and also add content security to secure the content during transmission.

However, the system proposed in (Hung-Min et al., 2007) does not consider various desirable license parameters like validity, etc and more importantly, is vulnerable to a Smart Card Imposter Attack as discussed later. In our proposed approach, we employ Identity Based Encryption System (IBES) to provide anonymity and also simplify the license purchase and key retrieval processes. We modify the Identity based Encryption algorithm to give out obfuscated identities, as discussed further.

The rest of this paper is organized as follows. In Section "PREVIOUS WORK", we review the smart card-based DRM system proposed by Hung et al (Hung-Min et al., 2007) and discuss about Identity based encryption systems. In Section "PROBLEMS IDENTIFIED", we point out the various drawbacks and problems identified. In Section "THE PROPOSED APPRAOCH", we propose a new approach which improves on the weaknesses and vulnerabilities of (Hung-Min et al., 2007). In Section "SECURITY", we focus on the security issues of our approach. Finally, we conclude this paper "CONCLUSION".

PREVIOUS WORK

In this section, we review the smart card based DRM system proposed by Hung-Min Sun et al (Hung-Min et al., 2007).

Smart Card Based DRM System

The system proposed has three main entities, viz, the Content Server, the License Server and the User (Client). The Content server encrypts the content in a key K_c and stores it for download/streaming. The License server issues licenses to users for viewing the content hosted on the Content server. The License server would also take care of the payment options. The license would consist of the content encryption key, K_c, used for encrypting the content the user purchases. The User, in this case the smart card, talks to the License server through the client application, for the specific licenses, and also decrypts them for the client application. The complete process would consist of four phases. They are, the Register Phase, the Purchase Phase, the Play Phase, and the Download Phase.

1. *Register phase:* The content provider uploads the unencrypted digital content, to the content server using SSL or other secure mechanisms. The content server will package the content to an encrypted format using a content key K_c, which is randomly generated by the content server. The encrypted content is stored in the content server and hosted for download. After packaging, the content key K_c will be transmitted to the license server as $E_{PKls}(c\_id||K_c)$ and the associated signature, where E_{PK1s} is an asymmetric encryption, $PKls$ is the license server's public key, c_id is the content identity, and $||$ represents the concatenation of strings. The license server will store c_id and K_c in its database and use them for creating licenses.

2. *Purchase phase:*

   (a) The user browses the shopping website and initiates a purchase.

   (b) The device generates a random number RAN and requests the smart card to calculate $H(RK||RAN)$ and $E_{PKls}(SSI||SK)$. Here H is a hash function, SSI is a Secret Security Identity in an anonymous payment system like 'eCash', and $SK = H(RK||c\_id||UK)$ is a content and user unique key. RK and UK are the secret keys installed apriori in the smart card. Because this calculation is executed inside the smart card, the user cannot know the secrets. SK would be used to encrypt the content key (K_c) in the license. The device transmits $\{c\_id,\ E_{PKls}(SSI||SK),\ H(RK||RAN),\ E_{UK}(RAN)\}$ to the license server.

   (c) The license server verifies the validity of the SSI and checks for sufficient funds. On successful completion of both these verifications, the license server will create the corresponding license:

$$
\begin{aligned}
Hash &= H(RK||RAN) \\
Details &= \{c\_id, Hash, E_{UK}(RAN)\} \\
User\_Right &= \{Details\}_{signLS} \\
License &= \{E_{SK}(K_c)||User\_Right\}
\end{aligned}
$$

Here $\{.\}_{signLS}$ is the signature of the message signed by the license server. $E_{SK}(K_c)$ and $E_{UK}(RAN)$ are both symmetric encryptions with keys SK and UK respectively. An license index $Index = \{c\_id||H(SK)\}$ would be created for quick access and public hosting.

(d) The license server sends the license to the user.

3. *Play Phase:*

(a) On "Play" initiation, c_id is extracted from the header of the downloaded content package. Then, the device calculates the license index $\{c\_id||H(SK)\}$ and retrieves the license. If the license does not exist in the device, it tries to fetch it from the License server. Failing to find it on the License server would imply that the user has not purchased the license.

(b) The license retrieved is passed to the smart card for validation, rights verification and content key decryption.

(c) The smart card extracts the c_id, $H(RN||RAN)$, $E_{UK}(RAN)$ and User Rights from the license by using the license server's public key. In order to get the value RAN, $E_{UK}(RAN)$ is decrypted. The RAN and the RK stored in the user's smart card are used to calculate the new $H(RK||RAN)$. If the value is not the same with the value extracted from the license, it means the license was not meant for this smart card, hence rejected. After checking $H(RK||RAN)$, the smart card checks if c_id, the identity of the content being played, matches that in the license. If they are not the same, it rejects on terms of license mismatch. If the smart card has passed both verifications, the user will be allowed to access the digital content. Then, the smart card decrypts the content key K_c. The key K_c will be transmitted to a protected memory in the device so as to restrict the access to unauthorized applications.

(d) The encrypted content will be decrypted in the protected memory of the device. Only the authorized applications can access this decrypted content and render it. When the user stops playing the content, the content and K_c in the protected memory will be deleted regardless of the content type.

4. *Download phase:* The user downloads the encrypted content package incase the content does not already exist in his device. When the user inserts his smart card into another device which does not store the content, the download phase will be re-activated. Together with the encrypted content package, the associated license also, if any, would be downloaded if necessary. In case of streaming content, only the URL and the license would be downloaded and stored.

The usage of smart card ensures that the user can play the content on any device that complies with the application requirements. Moreover it ensures the content providers that their content always remains secure, except in one case as identified further.

Identity Based Encryption System

Identity based Encryption System (IBES) is a public key cryptosystem designed mainly to remove the redundant complexity involved in the Public key Infrastructure's certification and certificate verification process. In this system, a recipients well known unique identity ID, like email address, mobile phone number, IP address, URL, etc is used as the public key for the encryption. The system architecture ensures that only the owner of this particular unique Identity has the private key for this ID, and hence none others can decrypt it. This is ensured by a Private Key Generator (PKG), the trust component of the system. Figure 1 depicts the system architecture and the various steps for secure message transfer.

The concept of IBES was proposed by Shamir way back in 1984. But the first successful and computationally feasible system was published in 2001 by Dan Boneh and M Franklin (Boneh and Franklin, 2001). Their system makes use of a concept called Weil Pairings, a bilinear function. But the computationally feasible system for mobile phones was first demonstrated in 2006, by J. S. Hwu, R. J. Chen, and Y.B. Lin with their Fast computation method for Weil Pairings (Hwu et al, 2006). With this advancement, IBES services can now be ported onto handheld devices also, which are prime content usage devices today.

The ID-based scheme consists of four algorithms: Setup, Extraction, Encryption, and Decryption. Setup is run by the PKG to generate a master key and the system parameters. This is done on input of a security parameter k_{ID}, which specifies the bit length of the group order and is regarded as the key size of the ID-based scheme. The Extraction algorithm is carried out by the PKG to generate a private key corresponding to the identity of a user. As with regular public key cryptography, the Encryption algorithm takes a message and a public key as inputs to produce a cipher text. Similarly, the Decryption algorithm is executed by the owner of the corresponding private key to decrypt the cipher text. These four functions are described as follows.

1. *Setup:* With the parameter k_{ID}, the algorithm works as follows:
   (a) Generate a random k_{ID}-bit prime p, two groups $(G_1; +)$; $(G_2; *)$ of order p, and the Weil pairing $e : G_1 \times G_1 \rightarrow G_2$. Choose an arbitrary generator $P \in G_1$.
   (b) Pick a random number $s \in Z_p^*$ and set $P_{pub} = sP$.
   (c) Choose cryptographic hash functions $h_1 : 0,1^* \rightarrow {G_1}^*$ and $h_2 : G_2 \in 0,1^n$ for some n. The public system parameters are $p, G_1, G_2, e, n, P, P_{pub}, h_1, h_2$ and the master key s is kept in secret by the PKG.
2. *Extraction:* For a given string $ID \in 0,1^*$ as the public key, the algorithm works as follows:
   (a) Compute $Q_{ID} = h_1(ID) \in G_1$.
   (b) Set the private key $K_R = sQ_{ID}$, where s is the master key held by PKG.
3. *Encryption:* To encrypt a message M under the public key ID, the algorithm works as follows:
   (a) Compute $Q_{ID} = h_1(ID) \in G_1$.
   (b) Choose a random $r \in Z_p^*$.
   (c) Set the cipher text to be $C = (U, V) = (rP, M \oplus h_2(e(Q_{ID}, sP)^r))$
4. *Decryption:* To decrypt a cipher $C = (U, V)$ encrypted using the public key ID, the algorithm uses the private key $K_R = sQ_{ID}$ to compute $M = V \oplus h2(e(sQ_{ID}, U))$. This decryption procedure yields the correct message due to the bilinearity of the Weil pairing, i.e.,

$$e(sQ_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, sP)^r)$$

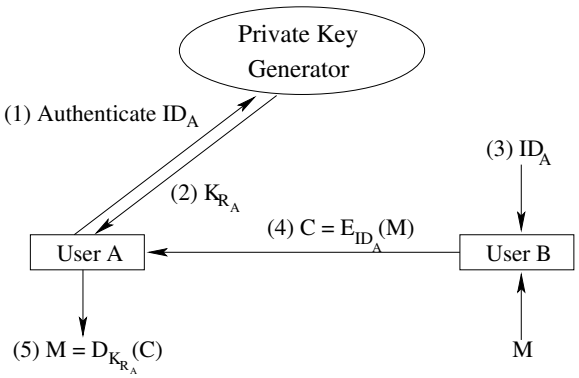

Figure 1: Identity Based Encryption System

In IBES, there is no public key exchange, nor certificate retrieval or verification, before a message transfer, as in other crypto systems. Hence a man-in-the-middle attack is not possible.

PROBLEMS IDENTIFIED

In this section we list the various drawbacks identified in various systems. Then we explain in detail the Smart Card Imposter Attack.

Drawbacks

Lists of problems identified in various types of DRM Systems:

- Device Based DRM systems
  - User fairness and flexibility
  - User Anonymity
  - Proprietary content processing applications
- IP Based DRM systems
  - User Anonymity
  - Complex process for user fairness
  - Dependence on content processing application for license validation
- Smart Card aided DRM systems
  - Vulnerable to Smart-Card Imposter Attack
  - License validity period not taken care of
  - Processing complexity in signature verification and data encryption when communicating with the license server
  - Complex algorithm with two private keys

Smart Card Imposter Attack

Hung-Min Sun et al (Hung-Min et al., 2007) assume all messages that the license server is receiving are from one of the system smart cards. But no where do they specify how to verify or authenticate if the messages are really coming from one of the system smart cards. The system security relies on the secrecy of RK and UK which are random secrets placed in each smart card.

A malicious or tampered program can impose itself as the smart card, choose two random secrets RK and UK and purchase license for a content c_id following the normal procedure, except that the program would perform the encryption operations instead of the smart card. On successful issuance of the license, which the license server would do without any suspicions, the program could decrypt the license and extract the content key K_c. Now the key can be used for decrypting content without any restrictions. Thus failing the purpose of the DRM as such.

The main intention of not verifying the identity of the smart card is to provide user anonymity, but it should not mean loss of authentication. There should be a mechanism where in the system can authenticate that the license purchase and decryption is done by a smart card only, but still not revealing which smart card. Our paper addresses this issue.

THE PROPOSED APPROACH

In this section, we propose a solution to solve the problems mentioned above. Moreover, we improve the efficiency for the low-computational-capacity smart cards. We propose to add an Identity based Encryption server to the architecture given in (Hung-Min et al., 2007), by the aid of which we would provide total user anonymity, as far as the DRM system is concerned, and also reduce the number of keys to be stored and manipulated by the smart card. Moreover it combats the Smart Card Imposter Attack mentioned above, which is a drawback of the system proposed in (Hung-Min et al., 2007).

Figure 2 depicts the architecture of the proposed system.

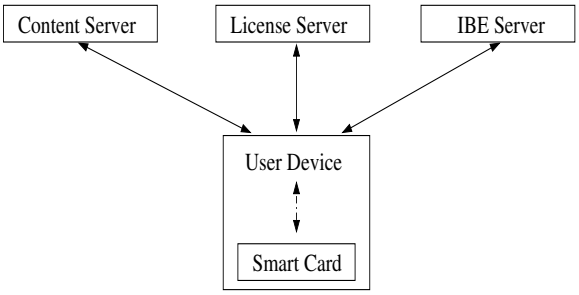

Figure 2: Architecture of Proposed System

This system would have four main roles, viz, the content server, the license server, the IBE server and the client (user). Each user would be issued a smart card which consists of a unique smart card ID and the IBE server generated private key for this ID, sQ_{ID}. It is assumed that the device used to play the content would have a card reader for the smart card. Hence the system would be able to work on any smart card based environment.

Protocol Overview

The protocol consists of four phases as in (Hung-Min et al., 2007). They are Content Registration phase, Purchase phase, Download phase and Play phase. The Content Registration phase occurs when the content provider uploads content to the content server. After the 'Content Registration Phase', the user can request purchase of the digital content on websites, and the Purchase Phase starts. Once the 'Purchase Phase' has finished, the digital content will be downloaded/streamed to the user's device in the 'Download Phase' and the user can play it in the 'Play Phase'.Finally, if the content which the user has bought disappears, or the user moves to a new device, the Download Phase can be re-done.

Content Registration Phase

In this phase, the content owner uploads the content to the content server, where in the content is encrypted with a randomly generated content key K_c, and a content Identity c_id is associated to it. The content server then communicates information about this content to the License server as $E_{PKls}(c\_id||K_c)$.

Purchase Phase

In the purchase phase, the user locates and shops for a content c_id. The media package would consist of c_id, the license, and the encrypted content or the streaming URL for the content. At this stage the smart card in the client device is supposed to generate an anonymous pseudo ID, SK, as per the system in (Hung-Min et al., 2007). Instead, here the smart card would reveal, to the license server, the point Q_{ID}, which is a point-mapping of the unique identity of the smart card. The smart card would send to the license server, through the user client, $E_{PKls}(SSI||Q_{ID}||c\_id)$ where SSI is the Secret Security Identifier of an anonymous payment system like 'eCash'. On receiving this message from the user, the License server would decrypt it, an extract the SSI, Q_{ID} and c_id of the content requested. It checks if the account presented has sufficient funds for purchase of content c_id and performs the financial transactions. On a successful transaction, it would create a license $L = E_{Q_{ID}}(c\_id||K_c||User\_Right\_XML)$. The license would include a small XML as to what kinds of rights are allowed and various parameters related to each right. Here the encryption followed would be that of Identity based encryption systems (Boneh and Franklin, 2001), with a slight modification that the input would be Q_{ID}, an elliptic curve point, rather than the receiver ID, and hence the initial point mapping algorithm would not be performed. We could follow an anonymous license delivery system as proposed in (Hung-Min et al., 2007), where in the license server would publish the license into a public directory with an index $I = H(Q_{ID}||c\_id)$ or could deliver the license to the user directly, as preferred by the user.

Download/Streaming Phase

This phase allows the user to download the encrypted content package when the content does not exist in his/her device. When the user inserts the smart card into another device which does not have the content, the download phase will be activated. There is no validation/restriction on who can download encrypted content from the content server, as only licensed users will be able to decrypt it correctly. Although this could lead to Denial of service attacks in case of on demand videos, this would not affect broadcast systems.

Play Phase

In this phase, when the user selects to open some content, the application would retrieve the license for the corresponding c_id and submit it to the smart card for decryption. Since the license was encrypted in Q_{ID}, only the smart card with the private key for this would be able to decrypt it, and none other. The smart card would try to decrypt the license and extract c_id. If the extracted c_id

and the content c_id whose license was submitted, are equal, then the license was generated for this smart card only, else invalid. Further, the smart card extracts various user right details like license validity, etc, checks for the expiry and if found valid, extracts the content key K_c and returns it to the application for use on a 'Protected Memory'. The application would use the content key to decrypt the content and process it as per the users request.

SECURITY

Secure against Smart Card imposter attack: Unlike as in (Hung-Min et al., 2007), here the smart card identity is a part of the license, which makes sure that the license server is talking to a smart card only and not an imposter application. Although an imposter application could submit a random Q_{ID}, or any specific Q_{ID} to the license server for procuring the license, the private key for this point would not be available, as the IBE system would insert private keys directly into the smart cards during manufacture, and also would update them, if necessary, in a secure manner. This way, there is no chance for any non-smart card program to get access to a private key in this IBE system.

Content Key Protection

Since the license was encrypted in Q_{ID}, provided by the smart card, only it would be able to decrypt it. Moreover a smart card is tamper resistant, which makes it secure against malicious or tampered applications. Now, irrespective of what application is being used to process the content, the system remains secure, as the smart card is the only one who can decrypt the license and also validate it.

User Privacy/Anonymity

One major benefit of this protocol would be total user anonymity as far as the DRM system is concerned. Since the smart card is giving out Q_{ID} instead of its ID, there is no way for anyone else to find out what the identity of the smart card is, as Q_{ID} is obtained from a mapping function that includes a one way hash and other steps. So although the license server is satisfied that the license can be decrypted only by a smart card, neither it nor any adversary, track as to who is purchasing and using what content, giving total user anonymity.

CONCLUSION

In this paper, we propose a smart card based DRM system that employs Identity Based Encryption System to combat various vulnerabilities and deficiencies identified in the previous systems. The system security relies totally on the security of the IBE server, License server and the smart cards. Assuming all these are secure enough, which is a fair enough assumption, the application that processes the content need not be a proprietary one and can follow an open architecture with different flavors. However, there is one threat, that the application gets hold of the content key, although in a protected memory area. To make the system more robust, a key evolving scheme could be employed where in the content key of the delivered content keeps changing periodically. The system provides total user anonymity and also the user fairness, as the smart card can be plugged into any compliant device to play the content. This is desirable by both the content consumers and the content providers, as now the content provider is sure that his content would stay secure knowing that only those many copies of the content are usable as many as licenses have been issued.

ACKNOWLEDGEMENT

We would like to express our gratitude towards the Information Security Education and Awareness (ISEA) Project, MCIT, DIT, Government of India, for its sponsorship, and the Department of Computer Enginering, NITK, Surathkal for providing us the necessary infrastructure and co-operation to complete this paper. We would like to thank "Prof. Asoke K Talukder", Indian Institute of Information Technology-Bangalore (IIITB), for his motivation, guidelines and review comments.

REFERENCES

William Ku, and Chi-Hung Chi. (2004). Survey on the technological aspects of Digital Rights Management. *7th Information Security Conference*, LNCS 3225:391-403.

Amitabh Kumar. (2007). Mobile TV: DVB-H, DMB, 3G Systems and Rich Media Applications. *Focal Press publications*, ISBN 13: 978-0-240-80946-5.

Hung-Min Sun, King-Hang Wang, and Yih-Sien Kao. (2006). IP-Based DRM - A Fair and Privacy Preserving DRM Framework. *International Computer Symposium 2006*, Taipei, Taiwan.

Erickson, J. S. (2003). Fair use, DRM, and Trusted Computing. *Communications of the ACMV*, April, volume 46:34-39.

Conrado, C,; Kamperman, F,; Schrijen, C. J,; and Jonker, W. (2003). Privacy in an Identity-based DRM System. In *Proceedings of the 14th IEEE International Workshop on Database and Expert Systems Applications*, 389-395.

Hung-Min Sun, Chi-Fu Hung and Chien-Ming Chen. (2007). An Improved Digital Rights Management System based on Smart Cards. *Inaugural IEEE International Conference on Digital Ecosystems and Technologies*, IEEE DEST.

Boneh, D and Franklin, M. (2001). Identity-based Encryption from the Weil Pairing. *Advances in Cryptology*, CRYPTO'01:213-239.

Hwu,J.S,; Chen, R. J,; and Lin, Y.B. (2006). An Efficient Identity-based Cryptosystem for End-to-end Mobile Security. *IEEE Transactions on Wireless Communications*,September, Vol. 5, No. 9.

AUTHOR BIOGRAPHIES

Sharath Palavalli was born in Karnataka, India. He completed his Bachelor of Engineering in Information Science from JSS Academy of Technical Education, Visveshwaraiah Technological University, Bangalore. He is currently pursuing his Master of Technology Degree in Computer Science from NITK, Surathkal. His email is palavalli.sharath@gmail.com.

U S Srinivas was born in Andhra Pradesh, India. He completed his Bachelor of Engineering from Mother Teresa Institute of Science and Technology, Sathupally, affiliated to JNTU Hyderabad, Andhra Pradesh. He is currently pursuing his Master of Technology Degree in Computer Science from NITK, Surathkal. His email is chus84@gmail.com.

Alwyn Roshan Pais was born in Karnataka, India. He completed his Bachelor of Engineering from the Mangalore University, Karnataka and Master of Technology from IIT Bombay. He is currently pursuing his PhD from NITK, Surathkal. He is currently serving as a Senior Scale Lecturer in the Department of Computer Engineering, NITK, Surathkal. He is also the coordinator of the ISEA project at NITK. His areas of interest are Algorithms, Cryptography and Computer Vision. His email is alwyn.pais@gmail.com and has personal webpage at http://compengg.nitk.ac.in/alwyn.htm.