ŞİFRELİ SMS GÖNDERİMİ İÇİN ANDROİD TABANLI MOBİL UYGULAMA ÇÖZÜMÜ

Hüseyin ÇALIŞKAN[1] ve MURAT DENER[2]
[1]Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe, Ankara
[2]Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Teknikokullar, Ankara
caliskan.huseyin@gazi.edu.tr, **muratdener@gazi.edu.tr**

ÖZET

Haberleşmede, anlık mesajlaşma uygulamaları da kullanılmasına rağmen, günümüzde SMS yaygın kullanılan bir haberleşme aracıdır. SMS; ucuz, hızlı, kullanımı kolay ve internet gerektirmediği için hala iletişim için kullanılan popüler yollardan biridir. SMS ile gönderilen gizli bilgilerin korunması kolay olmamakla birlikte, gönderilen SMS'in yetkisi olmayan kişilerce görüntülenmesi de söz konusu olabilmektedir. Bu çalışmada, mobil cihazlar arasında gönderilen SMS'lerin; gizlilik ve bütünlük olarak bilinen temel iki bilgi güvenliği kuralının sağlanması amacıyla, Android tabanlı mobil bir uygulama geliştirilmiştir. SMS verisinin gönderen ve alıcı arasında şifreli bir şekilde paylaşımını için bir uygulama geliştirilmiştir. Şifreleme işlemlerinde, simetrik şifreleme algoritması olan AES kullanılmıştır. Bu güvenlik çözümünün kısa sürede yaygın olarak kullanılması beklenmektedir. Bu makale ISDFS 2015 Konferansında sunulmuş ve seçilen bildiriler arasında yer aldığı için bu dergide basılmıştır.

Anahtar Kelimeler: SMS, AES, Android, Mobil Cihazlar, Güvenlik Algoritması, Android Uygulaması, Gizli Anahtarlı Şifreleme, Simetrik Şifreleme

AN ANDROID BASED MOBILE APPLICATION FOR SMS ENCRYPTION USING AES ALGORITHM

ABSTRACT

Even though the instant messaging applications are being used in communication, SMS is the most commonly used communication tool. SMS is cheap, fast and easy to use and one of the popular ways is still used for communication as it does not require internet connection. While the protection of the data sent via SMS is not easy, it is possible for the sent message to be seen by unauthorized persons. In this study, an Android based mobile application was developed for the purpose of providing two security rules of the SMSs sent between two mobile devices known as confidentiality and integrity. The application is intended to perform the SMS messaging between the sender and the receiver in an encrypted manner. In the encryption process AES which is a symmetric encryption algorithm was used.

Keywords: SMS, AES, Android, Mobile Devices, Security Algorithm, Android Apps, Secret Key Cryptography, Symmetric Encryption

I. GİRİŞ (INTRODUCTION)

Mobil iletişim cihazları, bilgi toplama ve yayılması için popüler araçlar haline gelmişlerdir. Hassas bilgiler SMS olarak gönderildiğinde, bu mesajın meşru göndereni tarafından iletilmesinin yanı sıra içeriğinin korunması da önemlidir. SMS trafiği şifresiz bir şekilde yapılmaz. A5 şifreleme algoritması kullanılarak şifrelenirler. Fakat günümüzde bu algoritma kırılabilmektedir. Kırılabilmesi nedeniyle güvensiz bir haberleşmeye neden olmaktadır [1].

International Telecommunication Union (ITU) raporuna göre 2010 yılında 6,1 Trilyon SMS mesajı gönderilmiştir [2]. SMS hizmetlerinin çok yaygın kullanılmasının nedenleri; ucuz, hızlı, kullanımı kolay

ve internet gereksiniminin olmaması şeklinde sıralanabilir. SMS, cep telefonu aracılığı ile yazılan bir mesajın cep telefonlar arasında gönderilmesini sağlayan mesajlaşma hizmetidir.

Gönderilen mesajların içeriği, şebeke operatörü ve personeller tarafından görüntülenebilmektedir.

Bu, bilgi güvenliği temel prensiplerinden biri olan gizlilik prensibi ile çelişmeye neden olmaktadır. Yetkililer dışında, SMS gönderiminde kullanılan şifreleme algoritmasının zayıf olması nedeniyle kötü niyetli kişilerde bu şifreyi kırabilir, SMS bilgisini görüntüleyebilir ve hatta SMS içeriğini değiştirebilir. Buda bilgi güvenliği prensiplerinden hem gizlilik hem de bütünlük prensipleri ile çelişkiye neden olur. Çalışmada, bu iki bilgi güvenliği prensibinin sağlanması için SMS gönderileri şifrelenecektir.

Uygulama, mobil bir işletim sistemi olan Android platformu üzerinde geliştirilmiştir. IDC'nin raporuna [3] göre, 2014'ün üçüncü çeyreğinde Android işletim sistemi, pazarın %84'üne hakim durumdadır. Bu nedenle Android işletim sistemi, kullanıcısı en çok olan işletim sistemidir. Android, Linux 2.6 çekirdeği kullanılarak yapılmış açık kaynak kodlu bir mobil işletim sistemidir [4]. İşletim sistemleri, içinde yüklü olan uygulamalar ile kullanılabilir hale gelir. Android işletim sisteminde kullanılan her hizmet bir uygulamadır.

Bu çalışmada, SMS veri güvenliğini sağlamak için bir şifreleme tekniği kullanılmış ve mobil bir uygulama geliştirilmiştir. Önerilen teknik ile SMS verisi, AES algoritması kullanarak şifrelenir ve gönderilmesi gereken numaraya şifreli bir şekide gönderilir. Şifreli SMS verisini alan taraf, önceden belirlenmiş olan parola ile şifreyi çözerek SMS verisine ulaşır.

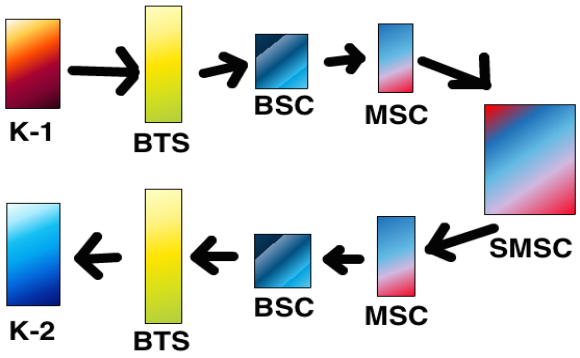
Bu çalışma 6 bölümden oluşmaktadır. İkinci bölümünde SMS hakkında bilgiler verilmiştir. Üçüncü bölümde çalışmada kullanılan şifreleme hakkında bilgi verilmiştir. Dördüncü bölümde uygulamada kullanılan teknolojiler ve uygulama tasarımı hakkında bilgi verilmiştir. Beşinci bölümde, gerçekleştirilen uygulamadan bahsedilmiş, son bölümde sonuç ve öneriler sunulmuştur.

II. SMS

SMS, mevcut haliyle bir kısa mesaj servisidir. Basitçe, cep telefonlar arasında kısa metinler gönderimi veya Global System for Mobile Communications (GSM) bulunduran cihazlar arasında kısa metinler gönderimi yapar. Her bir SMS başına 160 karakter (Latin alfabesinde bulunan; harfler, numaralar, semboller) limiti bulunmaktadır [5]. Diğer alfabelerde, örneğin Çince'de maksimum boyut 70 karakterdir.

A. SMS Çalışma Prensibi

SMS servisi bir cep telefonu özelliği olarak bilinmektedir, Fakat SMS diğer bilgisayar cihazları ile de çalışabilmektedir. SIM kartı kullanıldığı sürece PC, Laptop veya Tablet PC örnek olarak verilebilir. Cihazların SIM kartına ihtiyacı vardır, çünkü SMS servisi dahili SIM kartı istemcisine ihtiyaç duymaktadır.



Şekil 1. SMS Transfer İşlemi

BTS
Base Transceiver Station (BTS) kullanıcı ekipmanı ile bir ağ arasındaki kablosuz bağlantıyı kolaylaştıran ekipmanın bir parçasıdır. Kullanıcı ekipmanlarına; mobil telefonlar, WLL telefonlar, kablosuz internet bağlantısı olan bilgisayarlar, Wifi ve WiMAX cihazlar örnek olarak verilebilir [6].

MSC
Mobile Switching Center (MSC) GSM/CDMA için en önemli teslimat düğümüdür. MSC, sesli arama ve SMS yanı sıra başka servislerin (örneğin konferans görüşmeleri, faks ve devre anahtarlamalı veri gibi) yönlendirilmesinden de sorumludur. Uçtan uca tüm bağlantıları MSC kurar ve bitirir [7].

SMSC
SMS bir cep telefonundan iletildiğinde, mesaj SMS Center (SMSC) tarafından alınır. Ardından hedef bulma ve hedefin telefonuna mesaj gönderme işlemlerini gerçekleştirir. SMSC, SMS servisinin merkezinde yer alır. SMS iletmenin yanında, SMSC gelen mesajları kayıt altında tutabilir. Fakat limiti ölçüsünde mesaj tutabilir. Limitini aşarsa tutamaz. Hedef cep telefonu aktif değilse, SMS kaydedilir ve cep telefonu aktif hale gelince yeniden gönderilir. SMSC, gönderilen SMS'lerin başarılı ulaşıp ulaşmadığını kontrol edip geri bildirimde bulunur. SMS teslim edilirken, gönderici cep telefonu ve SMSC aktif iletişimdedir. Hedefin aktif olmayan cep telefonu aktif olursa, SMSC direk göndericiye haber verir ve SMS teslimatının başarıyla gerçekleştiğini bildirir [8].

B. SMS Güvenliği
SMS güvenliğini tehdit eden saldırılar mevcuttur. Bunlar aşağıda açıklanmaktadır.

- Ortadaki adam saldırısı (man-in-middle attack): Ortadaki adam olarak isimlendirilmesinin nedeni, SMS trafiği ortasında bilinmeyen bir kimsenin trafiğe müdahale edebilmesidir. Kullanıcı ağı doğrulamaz böylece saldırgan man in the middle saldırı gerçekleştirmek için meşru ağ ve aynı şebeke kodu ile yanlış BTS kimliğini kullanabilir.

- Replay Attack: Saldırgan tekrar bir saldırı gerçekleştirmek için daha önce abone ve ağ arasında alınıp verilen mesajları kötüye kullanabilir.

- Message Disclosure: Şifreleme kısa mesaj iletiminde kullanılmadığından iletim sırasında mesajlar yakalanabilir. Buna ek olarak SMS mesajları hedeflenen alıcıya başarılı bir şekilde ulaşmadan önce SMSC tarafından düz metin olarak depolanır. Bu mesajlar mesajlaşma sistemine erişimi olan SMSC kullanıcıları tarafından görüntülenebilir.

- Hizmet aksattırma saldırıları (denial of service): DOS saldırısı, kurbanın cep telefonunu ulaşılmaz hale getirebilmek için yapılmaktadır. Tekrarlanan mesajlar gönderilerek yapılır.

- SMS Tapping: Saldırgan bir SMS'i farklı yerlerden dinleyebilir. Bir mobil telefondan BTS'ye gönderilmiş veya alınmış bir SMS'in, bir radyo yayınından dinlenmesi kolay değildir. Mobil telefondan BTS'ye giden trafik A5 şifreleme algoritması kullanılarak şifrelenir. Saldırganlar A5 algoritmasını biliyor, fakat çözmek için trafiğin büyük bir kısmını analiz etmeleri gerekir. Eğer saldırgan, BTS'ye erişim sağlarsa veya GSM ağının farklı noktalarına erişebilirse dinleme kolaylaşır [9].

III. ŞİFRELEME (CIPHERING)

Şifrelemedeki ana amaç, SMS ile gönderilen bilgilerin gizliliğinin sağlanmasıdır. Modern şifreleme sistemleriyle yapılan güvenlik, yeterince güçlü olmalı ama kullanıcıların kullanımını zorlaştırmamalıdır.

Şifreleme algoritmaları; Asimetrik Şifreleme, Simetrik Şifreleme ve Anahtarsız Şifreleme olmak üzere üç çeşittir.

Asimetrik Şifreleme:
Asimetrik anahtar şifreleme aynı zamanda açık anahtarlı şifreleme olarak da bilinir. Bu metot şifrelenmiş mesaj yapmak için bir ortak anahtar ve bir özel anahtar olmak üzere iki anahtar kullanır. Ortak anahtar halka açık yapılır (herkes ulaşabilir) ve bu anahtarı olan kişiye mesaj göndermek isteyen herhangi biri tarafından şifrelemek için kullanılır. Özel anahtar gizli tutulur ve alınan mesajı çözmek için kullanılır. Asimetrik anahtarlı şifreleme sisteminin bir örneği RSA'dır**.** Asimetrik şifreleme kullanmanın dezavantajları:

- Açık anahtarlar kimlik doğrulaması gerektirir.
- RSA şifreleme çok güçlü değildir.
- Yavaştır ve daha fazla bilgisayar kaynağı kullanır.
- Özel anahtarların kaybı onarılmaz olabilir.
- Fazla işlem gücü gerektirir.
- Asimetrik şifreleme kullanılan uygulamalar daha fazla işlem gücüne sahip cihazlar için yazılmış olmalıdır.

Simetrik Şifreleme:
Paylaşılan anahtar, tek anahtar, gizli anahtar, özel anahtar veya tek anahtarlı şifreleme olarak bilinir. Bu mesaj şifreleme, gönderici ve alıcı mesajı şifreleme ve deşifreleme işleminde aynı anahtarı kullanır. Gönderici ve alıcı başlangıçta paylaşılan anahtarı belirtmek zorunda daha sonra mesajı şifremek ve deşifremek için bu anahtarı kullanırlar. Uygulamada bu tip şifreleme algoritması olan AES şifreleme algoritması kullanılmıştır [10].

AES (Gelişmiş Şifreleme Standardı) AES-128, AES-192 ve AES- 256 olmak üzere üç blok şifre içerir. Sabit blok boyutu 128 bit, anahtar boyutu ise 128, 192 ya da 256 bittir. Blok boyutu maksimum 256 bittir ancak anahtar boyutunun harhangi bir teorik maksimum boyutu yoktur. Düz metinden şifreli metine dönüştürme işlemi yapılırken şifre kullanılır. Her turun çıktısı bir sonraki çıktının girdisini oluşturur. Son turun çıktısı olan şifreli düz metin şifre metni olarak bilinir [11]. Uygulamada AES şifreleme algoritmasının 128 bit sürümü kullanılmıştır. Simetrik anahtar şifrelemenin dezavantajları:

- Gizli anahtarın değişimi içi güvenli bir kanala ihtiyaç duyulur.
- Mesaj doğruluğu garanti edilemez.
- Anahtar değişimi problemi vardır.

IV. UYGULAMA GEREKSİNİMLERİ VE UYGULAMA TASARIMI (APPLICATION REQUIREMENTS AND APPLICATION DESIGN)

Uygulama Gereksinimleri:
Uygulama, MacOS işletim sisteminde java programlama dili kullanılarak yazılmıştır. Kodlama ve tasarım işlemi, Android Studio1.0.1 programı üzerinde Android Developer Tools (ADT) v23.0 ile mimimum Android 2.2 versiyonu destekleyecek şekilde 4.0 versiyonda geliştirilmiştir. Android arayüzünün geliştirilmesi için, XML standardı kullanılmıştır. Uygulama; SMS göndermek ve SMS almak için iki adet izin gerektirmektedir. Uygulama gerçek ortamda Samsung Galaxy Note 2 N7100, Samsung Galaxy S5 cihazlarında test edilmiştir.

Uygulama Tasarımı:
Uygulama tasarımı dört kısımdan oluşmaktadır. Birinci kısımda, uygulama başlatıldığında çalışan ve

mesaj gönderme veya gelen mesajları okuma bölümüne gidilebilmesini sağlayan iki buton bulunmaktadır. İkinci kısım, mesajların gönderilidiği kısımdır. Üçüncü kısım, gelen şifreli mesajların okunduğu kısımdır. Dördüncü kısım ise gelen şifreli mesajların deşifre edildiği kısımdır. Uygulamayı oluşturan kısımlar şu şekildedir:

1. Ana Ekran
2. Mesaj Gönderme Ekranı
3. Gelen Mesajlar Ekranı
4. Mesaj Ekranı

Uygulama açıldığında ekrana ilk önce "Mesaj Gönder" ve "Gelen Mesajlar" butonlarının seçilebileceği alan gelir. "Mesaj Gönder" butonuna tıklandığında mesaj gönderme ekranı gelir. "Gelen Mesajlar" butonuna tıklandığında gelen şifreli SMS'ler görüntülenir. Görüntülenen mesajlardan birine tıklandığında, ekrana parola ekranı gelir. Parolaya giriş yapılınca şifreli metin deşifre edilip "Mesaj" ekranında görüntülenir.

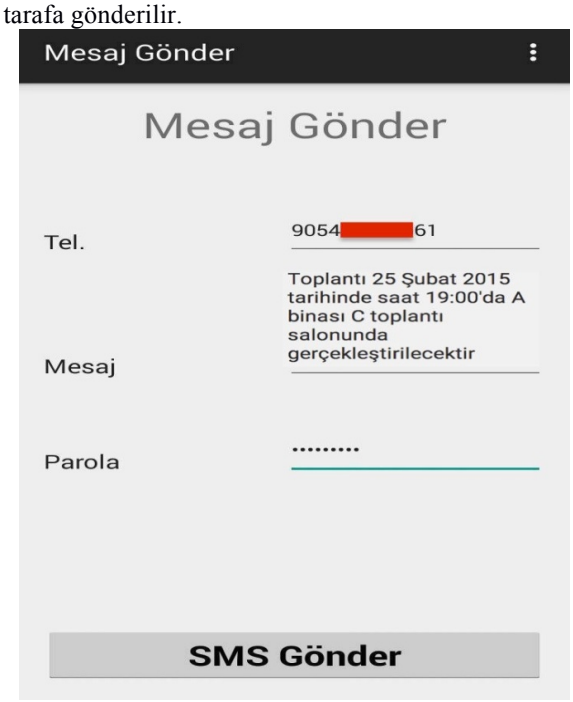
V. UYGULAMA (APPLICATION)

Ana Ekran:
Uygulamaya giriş yapılınca gelen ekrandır. Ekran içerisinde iki adet buton bir adet textview bulunmaktadır. Bu butonlara tıklamak suretiyle, "Mesaj Gönder" ve "Gelen Mesajlar" bölümlerine ulaşılabilmektedir.

Şekil 2. Ana Ekran Görüntüsü

Mesaj Gönderme Ekranı:

Bu ekrana, ana ekrandan seçilen "Mesaj Gönder" butonu aracılığı ile ulaşılır. Bu ekran içerisinde, dört textview, üç editview ve bir buton bulunmaktadır. Editview'lere gönderilmek istenen telefon numarası, gönderilmek istenen mesaj ve karşılıklı olarak belirlenmiş olan parola girilir. Ardından "SMS Gönder" butonuna basılır ve SMS şifrelenip karşı tarafa gönderilir.



Şekil 3. Mesaj Gönderme Ekranı

Gelen Mesajlar Ekranı:
Bu ekrana, ana ekrandan seçilen "Gelen Mesajlar" butonu aracılığı ile ulaşılır. Bu ekranda bir textview bir de Listview bulunmaktadır. Gelen mesaj tespit edildiği zaman, gelen mesajın telefon numarası ve şifreli mesaj Listview'e eklenir. Listview'de listelenen mesajlardan biri seçilince, ekrana parola girilmesi için bir dialog gelir. Buradan girilen parolaya göre şifre deşifre edilip "Mesaj Ekranı" bölümü açılır.

Şekil 4. Gelen Mesajlar Ekranı

Şekil 5. Parola Giriş Ekranı

Mesaj:
Gelen mesajlar bölümünde bulunan listeden bir mesaj seçilir ve seçilen mesaj için parola girişi yapılır. Mesaj ekranına parola girişinden sonra ulaşılır. Bu ekranda beş textview bulunmaktadır. Eğer doğru parola girilmişse şifre çözülür, yanlış parola girilmişse şifre çözülemez.

VI. SONUÇ VE ÖNERİLER (CONCLUSION AND RECOMMENDATIONS)

Kullanıcılar, SMS verisinin gönderildiği yolu dinlendiklerini düşündükleri ana kadar önemsemezler. Ama SMS gönderilerinin dinlenmesi sonrasında önlem almanın bir yararı olmayacaktır.

Çünkü gönderiler yetkisiz kişiler tarafından erişilmiş olabilir. Gerçekleştirilen çalışma sonucunda; kullanıcılara iletişim için daha güvenli bir yol sağlanmış ve SMS verileri gönderilmesi gereken hedefe, gizlilik ve bütünlük bozulmadan gönderilebilmiştir. Yapılan uygulama gelen mesajları sadece anlık olarak kaydetmektedir. Dolayısıyla SMS bilgilerinin tutulduğu bir veri tabanı bulunmamaktadır. Gelen mesajlara bakıldıktan sonra uygulama kapatılınca mesajlar yok olur. Böylelikle veriler uygulamanın yüklü olduğu cihazda da kayıt altında tutulmayarak gizlilik seviyesi artırılmış olunur. Uygulama tasarımında bir Android teknolojisi olan Listview kullanıldığı için mesajların görüntülenmesi daha kolay olmaktadır. Uygulamanın arayüz yapısı, yapılmış benzer uygulamalardan daha kullanışlıdır. Uygulama, Türkçe ve İngilizce dil desteği sunmak ile beraber internet erişim izni gerektirmemektedir. Bu uygulama, yüksek seviyedeki organizasyonların birbiri ile haberleşmesi, askeri personellerin birbiri ile haberleşmesi ve gizli bilgi paylaşımının önemli olduğu çoğu yerde kullanılabilir.

Şekil 6. Mesaj Ekranı

Bu uygulama Android 2.2 ve üzeri sürümlerinin yüklü olduğu tüm cihazlarda çalışabilir. Uygulama veriler için güvenli, hızlı ve güçlü bir şifreleme sağlar. Kullanılan yöntem, güçlü bir şifreleme sağladığı için saldırganların şifreli bilgiyi çözmeleri çok zor hale gelmiştir.

Matematiksel olarak kırılma zorluğu yüksek bir algoritma seçildiği için kaba kuvvet saldırısına da dayanıklıdır. Birçok SMS şifreleme tekniği mevcuttur fakat bunların bir kısmının uygulanabilirliği tartışılmaktadır. Araştırmalar sonucunda, DES algoritmasının anahtar uzunluğunun yetersiz olduğu ve Blowfish algoritmasının da çok bellek tükettiği görülmüştür. Bu nedenle simetrik şifreleme yöntemleri arasından en uygun şifreleme yöntemi olarak AES algoritması seçilmiştir. AES şifreleme algoritması kullanılarak güçlü bir şifreleme oluşturulmuştur. Uygulama içerisinde, asimetrik şifreleme kullanılmadığı için fazla işlem gücü gerektirmemektedir. Fakat uygulamaya asimetrik şifreleme eklenerek parola giriş işlemi kaldırılıp yerine açık ve gizli anahtarların olduğu bir şifreleme getirilebilir. Bu şekilde parolanın çalınma endişesi ortadan kalkar. Fakat işlem gücü artar gizli anahtarın güvenliğinin sağlanması gerekir.

VII. KAYNAKLAR (REFERENCES)

[1]. M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, C. Manifavas, "Breaking The

Gsm A5/1 Cryptography Algorithm With Rainbow Tables And High-End Fpgas", 2010

[2]. The World in 2010-The rise of 3G, [Offline]. Available: http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf, 2010

[3]. Smartphone OS Market Share, IDC [Online]. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp, 2015

[4]. J. F. DiMarzio, Androıd A Programmers Guıde, McGraw Hill Professional, 2008

[5]. P. Haghirian, M. Madlberger, A. Tanuskova, "Increasing advertising value of mobile marketing – An empirical study of antecedents", Presented at 38th Hawaii International Conference on System Sciences, 2005.

[6]. N. Faruk, A.A Ayeni, M. Y. Muhammad, L.A. Olawoyin, A. Abdulkarim, J. Agbakoba, M. O. Olufemi, "Techniques for Minimizing Power Consumption of Base Transceiver Station in Mobile Cellular Systems", International Journal of Sustainability, Vol.2 No.1, 2013

[7]. Digital cellular telecommunications system (Phase 2+); Circuit switched voice capacity evolution for GSM/EDGE Radio Access Network (GERAN) (3GPP TR 45.914 version 11.0.0 Release 11) ETSI TR 145 914 V11.0.0 (2012-11) ETSI. 2012

[8]. Y. L. Ng, "Short Message Service (SMS) Security Solution for Mobile Devices", Naval Postgraduate School, 2006

[9]. R. R. Chavan, M. Sabness, "Secured mobile messaging" in International Conference On Computing, 2012.

[10]. A. Lecturer, "A Symmetric Key Cryptographic Algorithm", Hindu College of Engineering, 2010.

[11]. P. Pimpale, R. Rayarikar, S. Upadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.10, 2011.