Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 13, Number 1, Spring 2024, pp. 52-64
Received: 02/18/2018, Revised: 10/20/2024, Accepted: 10/26/2024

Securing SMS Communications Based on Users' Private Messages on Social Networks

Saeid Yazdanpanah[1], Saman Shojae Chaeikar[2*]
1- Department of Computer Engineering, Khorramabad Branch, Islamic Azad University, Khorramabad, Iran.
2*- Faculty of Computer Engineering, Iranian eUniversity, Tehran, Iran.
[1] yazdanpanah.saeid@iau.ac.ir, [2*] saman.shoja@iranian.ac.ir

Corresponding author's address: Saman Shojae Chaeikar, Faculty of Computer Engineering, Iranian eUniversity, Tehran, Iran.

Abstract- Nowadays, short message communication has a wide range of applications in modern life. Authentication, announcements, reports, and personal communications are the common instances of application of this widely used digital media. At transmission time, the message content spreads in the air without any intrinsic security countermeasure. As a result, the content of messages is interceptable without the need for complicated equipment. In modern methods, security has migrated from hardware to software, especially in smartphones. In this research, a method for securing short message communications is introduced, which uses four distinguished key generation factors to produce a couple of unique and dynamic encryption and decryption keys. The evaluation results show that the proposed method uses secure encryption and decryption keys, is resistant against a wide range of cryptographic and network attacks, outstandingly reduces the cost of establishing secure sessions, and highly satisfies the users with the delivered level of security and usability.

Keywords- SMS Security, Short Message Security, Secure Communications.

مجله علمی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۳، شماره ۱، بهار ۱۴۰۳ ، صفحه ۵۲-۶۴
دریافت: ۱۳۹۶/۱۱/۲۹، بازنگری: ۱۴۰۳/۰۷/۲۹، پذیرش: ۱۴۰۳/۰۸/۰۵

ایمن‌سازی تبادل پیامک بر مبنای تبادل داده خصوصی کاربران در شبکه‌های اجتماعی

سعید یزدانپناه[۱]، سامان شجاع چایی‌کار*[۲]
۱- گروه مهندسی کامپیوتر، واحد خرم‌آباد، دانشگاه آزاد اسلامی، خرم‌آباد، ایران.
*۲- دانشکده مهندسی کامپیوتر، موسسه آموزش عالی الکترونیکی ایرانیان، تهران، ایران.
[1] yazdanpanah.saeid@iau.ac.ir, [2*] saman.shoja@iranian.ac.ir

* سامان شجاع چایی‌کار، تهران، موسسه آموزش عالی الکترونیکی ایرانیان، دانشکده مهندسی کامپیوتر، کدپستی: ۱۴۵۷۸۹۶۳۵۱

چکیده- امروزه پیامک‌ها نقش کاربردی وسیعی در زندگی مدرن کاربران ایفا می‌کنند. احراز هویت، گزارش‌ها، و ارتباطات شخصی نمونه‌هایی از کاربردهای وسیع این رسانه هستند. در زمان ارسال پیامک سیگنال‌های آن بدون هرگونه تمهیدات امنیتی در فضا انتشار می‌یابند و درنتیجه محتویات پیام‌ها بدون نیاز به تجهیزات پیچیده براحتی قابل تصاحب است. روشهای نوین، تامین امنیت را از سخت افزار به نرم افزار و بخصوص برنامه‌های تلفن‌های هوشمند منتقل کرده‌اند. در این تحقیق، یک روش ایمن‌سازی پیشنهاد شده که با استفاده از چهار عامل مختلف، دو کلید منحصر به فرد و پویا را برای رمزنگاری و رمزگشایی پیامک‌ها تولید می‌کند. ارزیابی نتایج نشان می‌دهد که مدل ارائه شده از کلیدهای ایمن استفاده کرده، در برابر طیف وسیعی از حملات مقاوم است، هزینه ایجاد نشست‌های ایمن به شکل چشم‌گیری کاهش یافته، و درصد بسیار بالایی از کاربران از ایمنی و سادگی عملکرد آن رضایت کامل دارند.

واژه‌های کلیدی: امنیت پیامک، امنیت پیام کوتاه، ارتباطات ایمن.

۱- مقدمه

پیام کوتاه (Short Message Service - SMS) یک سرویس پیام متنی بی‌سیم است که به مشترکان سیار امکان تبادل پیام را می‌دهد. طول پیامها به ۱۶۰ کاراکتر محدود بوده و داده‌های غیر متنی پشتیبانی نمی‌شوند. سامانه جهانی ارتباطات سیار (Global System for Mobile communication – GSM) به عنوان رسانه تبادل پیامک‌ها استفاده می‌شود. پیامک پس از ارسال در مرکز پیامک (SMS Center - SMSC) ذخیره شده تا در زمان لازم به گیرنده سیار تحویل داده شود. مرکز پیامک از روش ذخیره و ارسال (Store-and-forward) استفاده کرده و در صورتی که دریافت کننده فعال باشد پیام ارسالی به دست او خواهد رسید. پس از آن، مرکز پیامک یک کد تصدیق دریافت می‌کند که به معنی پایان فرآیند تحویل پیامک است [۱]. پیامک‌ها بصورت متن ساده و بدون رمزنگاری در مرکز پیامک ذخیره می‌شوند. بنابراین کارمندان مراکز پیامک به محتوای پیام‌ها دسترسی داشته و امکان تغییر آنرا دارند. بسیاری از مراکز پیامک نیز با اهداف مختلف (مانند آماری، بازاریابی و غیره) یک نسخه از پیامک‌ها را در مراکز خود ذخیره می‌کنند. ساختار سامانه مخابراتی پیامک‌ها به مهاجمین امکان می‌دهد که با نفوذ به مراکز پیامک به محتویات تمامی پیامک‌های ارسال شده دسترسی داشته باشند [۳،۲].

تا کنون روش‌های رمزنگاری متعددی برای کاهش تهدیدات سامانه پیامک‌ها و تامین امنیت دستگاه‌های سیار طراحی شده است. با این وجود، محدودیت منابع در اغلب تلفن‌های هوشمند امکان پیاده‌سازی این تکنیک‌ها را با کیفیتی برابر با رایانه‌ها نمی‌دهد [۵،۴]. رمزنگاری متقارن مدلی است که امکان تامین ایمنی سرتاسری (end to end) را برای سامانه پیامک‌ها بوجود آورده

است. با توجه به محدودیت‌های انرژی، حافظه و توان پردازشی تلفن‌های هوشمند، رمزنگاری متقارن متناسب با ساختار فنی آنها به شمار می‌آید [۶]. در این روش یک کلید مخفی مشترک بین فرستنده و گیرنده پیامک وجود داشته که وظیفه تامین ایمنی سرتاسری را بر عهده دارد. مهمترین ضعف این روش فرآیند انتشار کلید است که در صورت لو رفتن آن مهاجم امکان تصاحب و حتی تغییر محتوای پیام‌ها را خواهد داشت. از مهمترین نمونه‌های رمزنگاری متقارن می‌توان به DES و AES اشاره کرد [۷].

مشکل انتشار کلید بین کاربران پیامک با استفاده از رمزنگاری نامتقارن قابل حل است. کلید عمومی پیام‌ها را به رمز درآورده و کلید خصوصی آنها را رمزگشایی می‌نماید. با توجه به عدم تعیین هویت در این سامانه، حمله مرد میانی یکی از مشکلات این روش به حساب می‌آید. زیر ساخت کلید عمومی (Public Key Infrastructure - PKI) روشی است که به کمک این سامانه آمده تا سطح امنیتی آنرا بهبود بخشد [۹،۸]. اگرچه امنیت رمزنگاری نامتقارن بالا بوده و فرآیند انتشار کلید آن ساده است، اما بدلیل سربار محاسباتی بسیار بالا و نیاز به زیرساختها معمولا از استفاده آن صرف‌نظر می‌شود [۱۱،۱۰].

ذخیره انرژی، توان محاسباتی، و حافظه تلفن‌های همراه هوشمند رو به گسترش بوده و امکان پیاده‌سازی روش‌های پیچیده‌تری فراهم شده است. در نتیجه این تحولات، روش‌های متعددی بر پایه سامانه‌های رمزنگاری متقارن و نامتقارن طراحی شده [۱۳،۱۲] که هر کدام توانایی‌ها و ضعف‌های خود را داشته و جامعه خاصی از کاربران را هدف می‌گیرند. در این تحقیق یک روش ایمن‌سازی تبادل پیامک بر اساس کلیدهای متقارن طراحی شده است که در آن بجای فرآیند انتشار کلید، کلیدها با استفاده از تبادلات داده‌ای کاربران در شبکه‌های اجتماعی بصورت پویا ساخته می‌شوند. سادگی استفاده و ایمنی بالا از مزیت‌های این روش به شمار می‌آید. مهمترین محدودیت این روش امکان برقراری ارتباط ایمن با طیف خاصی از مخاطبان است. هدف اصلی این مدل، استقلال فرآیند تامین امنیت از اپراتورهای تلفن همراه، قطع دسترسی اپراتورها به محتویات پیام، و کاهش هزینه‌ها است. پیش‌فرض این روش، وجود ارتباط پیشین بین کاربران ارسال و دریافت کننده پیام در شبکه‌های اجتماعی است.

۲- پیشینه تحقیق

قالب ساده و پشتیبانی تمامی تلفن‌های همراه، پیامک را تبدیل به رسانه‌ای پر استفاده در زمینه‌های مختلف کرده است. اطلاع رسانی در سامانه‌های دولت الکترونیک، تبادلات بانکی، سامانه‌های اطلاع رسانی، تبادل پیام و بسیاری موارد دیگر را می‌توان ازجمله کاربردهای این رسانه پر استفاده برشمرد. تا کنون روش‌های متعددی برای ایمن‌سازی تبادل پیامک در شبکه های GSM طراحی شده است. اولین گروه از روش‌های ابداع شده، تغییر ساختار GSM را برای تامین امنیت هدف قرار داده‌اند. مدل پیشنهادی Hossain [۱۴] تغییر ساختار پروتکل GSM در لایه انتقال (transport) بین تلفن همراه و ایستگاه GSM است. با پیاده‌سازی این سامانه، امنیت در سطح زیرساخت‌ها تامین شده و به تبع آن تبادل پیامک نیز ایمن می‌گردد. بدلیل نیاز به سرمایه گذاری بالا و مشکلات سخت‌افزاری، روش ارائه شده را نمی‌توان قابل پیاده‌سازی در نظر گرفت.

گروه دوم از روش‌های ارائه شده، تامین امنیت را به لایه کاربردی منتقل کرده‌اند. افزایش توان پردازشی تلفن‌های همراه و کاهش چشمگیر هزینه‌های پیاده‌سازی، امکان بکارگیری روش‌های این گروه را افزایش می‌دهد. این روش‌ها را نیز می‌توان بر اساس محل ذخیره کلیدهای رمزنگاری و مدل پیاده‌سازی تقسیم‌بندی کرد. گروه IPC [۱۵] و Rongyu [۱۶] روش ذخیره برنامه و کلیدهای رمزنگاری در درون سیم‌کارت‌های قابل برنامه‌ریزی را معرفی کردند. ویژگی‌های برتر سیمکارت‌های قابل برنامه ریزی عبارتند از (۱) عدم امکان جعل (tamper resistance)، و (۲) امکان جابجایی بین تلفن‌های همراه بدون از دست رفتن اطلاعات. از مشکلات این روش می‌توان به توان پردازشی محدود اشاره کرد که مانع پیاده‌سازی روش‌های مدرن امنیتی می‌شود. جایگزین مناسب سیم‌کارت‌های قابل برنامه‌ریزی، استفاده از سیم‌کارت برای ذخیره کلید رمزنگاری و تلفن همراه به عنوان واحد پردازش است [۱۸،۱۷]. اگرچه پیاده‌سازی این روش بسیار آسان است، اما زمانی که در یک ارتباط چند اپراتور در مسیر قرار می‌گیرند، مشکلات تکنیکی متعددی مشاهده می‌شود.

با انتقال سامانه امنیتی از ترکیب سخت‌افزار و نرم‌افزار به نرم‌افزار، بسیاری از مشکلات شمرده شده برطرف خواهد شد. روش‌های MIABO [۱۹]، SafeSMS [۲۰] و تکنیک‌های ارائه شده توسط Lisonek [۲۱] و Hassinen [۲۲] از رمزهای عبور از پیش به اشتراک گذاشته شده و یا رمزنگاری کلید عمومی برای تامین امنیت در لایه کاربردی استفاده می‌کنند. محدودیت‌های این روش عبارتند از (۱) محدودسازی ارتباط بین دو کاربر خاص، و (۲) وابسته بودن امنیت ارتباطات به فرآیند تبادل کلید. Belanger و Carter [۲۳] یک روش مبتنی بر کلیدهای نامتقارن RSA، متقارن AES/CTR و تعیین هویت با استفاده از رمز را برای ایمن‌سازی ارتباطات بین کاربر و اپراتور شبکه معرفی کردند. این روش

محرمانگی و یکپارچگی پیام را در محدوده بین تلفن همراه کاربر و اپراتور تضمین می‌کند.

راه حل دیگر پیشنهاد شده در این زمینه، استفاده از مدل سرویس‌دهنده/سرویس‌گیرنده (client-server) است که موجودیت‌های درگیر در آن انسان، سازمان‌های امنیتی و یا مراکز صدور گواهی (Certificate Authorities - CAs) هستند. نمونه روش‌های ارائه شده در این زمینه عبارتند از SMSSec [۲۴] و TrustedSMS [۲۵]. الگوریتم AES نیازمند توان محاسباتی و حافظه کمتری در مقایسه با روش‌های 3DES و RSA که مبتنی بر زیرساخت کلید عمومی طراحی شده‌اند است. SMSSec [۲۴] از ترکیب سامانه‌های رمزنگاری متقارن و نامتقارن برای تامین محرمانگی پیام‌ها بهره می‌برد. Lisonek و Drahansky [۲۱] یک روش مبتنی بر کلیدهای RSA ارائه کرده‌اند. بدلیل عدم امکان اجرای حمله جستجوی گسترده (brute force) به کلیدهای RSA با طول ۱۰۲۴ بیت، روش پیشنهادی آنها در مقابل این حمله ایمن به شمار می‌آید. نتایج منتشر شده توسط Agoyi و Seral [۲۶] نشان می‌دهد که الگوریتم‌های رمزنگاری با طول کلیدهای بلند بدلیل حافظه محدود و توان محاسباتی پایین دستگاه‌های تلفن همراه انتخاب مناسبی برای ایمن‌سازی پیامک‌ها نیستند. با توجه به محدودیت‌ها، الگوریتم EC (Elliptic Curve) گزینه مناسب‌تری در مقایسه با RSA (Rivest–Shamir–Adleman) و EL-Gamal به شمار می‌آید. با توجه به همین مساله، الگوریتم Secure SMS [۱۷] بر پایه کلید عمومی، رمزنگاری متقارن را با امضای دیجیتال ترکیب کرده و یک مدل ایمن تبادل پیامک را ارائه کرده است. ترکیب رمزنگاری متقارن و EC حجم محاسباتی را نسبت به روش‌های پیشین کلید عمومی کاهش داده و آنرا تبدیل به روشی کاراتر می‌کند. Narendiran [۲۷] یک روش سرتاسری ایمن‌سازی تبادل پیامک برای سامانه‌های بانکی را بر اساس زیرساخت کلید عمومی ابداع کرده‌اند. بهره‌گیری از رمزنگاری کلید عمومی برای گواهینامه‌های کاربری و امضای دیجیتال امکان پیاده‌سازی تعیین هویت قوی کاربران و عدم انکار را در این مدل فراهم آورده است.

در روش ارائه شده توسط Ahamed و همکاران [۲۸]، از یک روش رمزنگاری نامتقارن استفاده شده است که به دلیل پویا بودن فرآیند تولید کلید در برابر حملات دیکشنری و متن ساده مقاوم است. حمله به این روش برای مهاجمین بسیار مشکل خواهد بود چراکه پیام ابتدا به اعداد در مبنای ۱۰ تبدیل می‌شود و پس از آن مبنای ۲ آن برای فرآیند رمزگشایی و رمزنگاری استفاده می‌شود. در فرآیند تولید کلید، الگوریتم RSA با Vigenere ترکیب شده و در عمل کلید حاصل ترکیبی از روش‌های متقارن و نامقارن است. در نتیجه این ترکیب، امنیت ارایه شده بالاتر از الگوریتم‌های متقارن بوده و در عین حال کلیدها در زمان کمتری نسبت به روش‌های نامتقارن تولید می‌شوند. نویسندگان محدودیت این الگوریتم را صرف زمان بیشتر در مقایسه با الگوریتم‌هایی که صرفا بر اساس Vigenere طراحی شده‌اند اعلام کرده‌اند.

تحقیق ارائه شده توسط Zam Zam و همکاران [۲۹] در راستای بهبود امنیک پیامک‌ها، یک برنامه تحت سیستم عامل اندروید به نام ECSS (Efficient Cryptographic Scheme for SMS) را ارائه می‌دهد. نویسندگان در این مقاله نرم‌افزار ECSS را از نظر زمان و دقت قابل اطمینان ارزیابی کرده‌اند و استفاده از آنرا باعث بهبود امنیت اعلام می‌کنند. برنامه تولید شده، کلیدهای رمزنگاری تصادفی ایجاد می‌کند که باعث مقاومت آن در برابر حملات دیکشنری و متن ساده می‌شود. محققین مقادیر DNA (Deoxyribonucleic acid) پیام‌ها را در فرآیند رمزنگاری و رمزگشایی استفاده می‌کنند که شکست آن برای مهاجمین کار آسانی نیست. نتایج آزمون‌ها بیانگر یک تاثیر بهمنی (avalanche effect) بسیار عالی در فرآیند رمزنگاری است و مقاومت روش پیشنهادی را بسیار بالا می‌برد.

حجم تحقیقات صورت گرفته برای ایمن‌سازی تبادل پیام کوتاه بسیار گسترده بوده و تا کنون روش‌های متعددی ارائه شده‌اند. جدول ۱ مزایا و معایب مهم‌ترین روش‌های رمزنگاری استفاده شده در تامین امنیت الگوریتم‌های تامین ایمنی پیام کوتاه را نمایش می‌دهد.

۳- مدل پیامک ایمن بر مبنای شبکه‌های اجتماعی

در این بخش ساختار مدل پیامک ایمن بر مبنای شبکه‌های اجتماعی (Social-network-based Secure SMS) که از این پس با نام اختصاری SSS به آن اشاره می‌شود تشریح شده است. پیش از بررسی جزییات مدل، ساختار پیامک و مهم‌ترین توابع درهم‌سازی بررسی شده‌اند تا خواننده درک بهتری از ساختار ارائه شده و دلایل انتخاب نوع کلید رمزنگاری بدست آورد. علامت‌های اختصاری استفاده شده در فرمول‌های این مقاله در جدول ۲ شرح داده شده‌اند.

۳-۱- معماری و امنیت پیامک

در طول فرآیند ارسال پیامک در GSM دو پایگاه سیار Mobile Station – MS (معمولا تلفن همراه) و چند دکل Base Transceiver Station – BTS درگیر هستند. پیام‌ها از یک مرکز سرویس پیام (Message Service Center – MSC) به یک مرکز

جدول۱: مزایا و معایب مهم‌ترین الگوریتم‌های رمزنگاری مورد استفاده در مدل‌های تامین امنیت سرویس پیام کوتاه [۱]

تکنیک	مزایا	معایب
RSA	• امنیت بالا • سادگی پیاده‌سازی • عدم انکار • بهره‌گیری از تولید کننده عدد تصادفی قوی	• سرعت پایین • ضعف در برابر حمله جعل هویت • بزرگی طول داده رمزنگاری شده
J-PakE	• مکانیزم تبادل کلید بسیار قوی • تصدیق کلید صریح • مقاوم در برابر حمله دیکشنری • دارای ویژگی محرمانگی پیشرو (forward secrecy)	• هزینه بالای پیاده‌سازی
XTR	• سرعت بالا در تولید/انتخاب کلید • هزینه محاسباتی پایین • سرعت رمزنگاری و رمزگشایی بالا • کلید کوتاه • سرعت بالا در فرآیند بررسی امضا • سرعت بالا در تولید عامل‌ها (parameters)	• طول بالای کلید عمومی XTR (بزرگتر از ECC) • آسیب‌پذیر در برابر حمله کانال جانبی
NTRU	• مصرف پایین منابع • طول کوتاه کلید عمومی • مناسب برای سامانه-های نهفته • سریعتر از ECC و RSA • مصرف پایین حافظه	• سرعت رمزگشایی پایین
EC	• استفاده از کلیدهای کوتاه اما ایمن • مصرف پایین پردازنده • مصرف پایین حافظه • حجم پایین داده‌های ذخیره شده	• ایجاد گروه‌های عملیاتی پیچیده • نیاز به جداول از پیش محاسبه شده
Knapsack	• سادگی • یکسویه بودن • شفافیت	• زمان محاسباتی نسبتا بالا • ایمنی پایین
Chor Rivest	• سادگی پیاده‌سازی • سختی شکستن کلید	• کلید عمومی بزرگ • کندی فرآیند تولید کلید • کندی فرآیند رمزگشایی
Blum Goldwasser	• ایمنی معنایی (semantic) • استفاده بهینه از حافظه ذخیره‌سازی • مدل بهینه برای متن‌های طولانی	• آسیب‌پذیری در برابر حمله به متن اصلی • ایمنی پایین بر اساس محاسبات • هزینه محاسباتی بالا
El Gamal	• سامانه رمزنگاری تصادفی • استفاده از کلیدهای کوتاه • استفاده از ایمنی معنایی • تولید سریع امضا • تولید سریع کلید	• هزینه بالای بررسی امضا • طولانی‌سازی پیام • هزینه بالای تولید عامل‌های گروهی
Blow Fish	• استحکام مناسب کلید • سرعت مناسب • الگوریتم متن‌باز • سرعت بالا • بهینگی در استفاده از انرژی	• نامناسب برای متن‌های طولانی • استفاده از کلیدهای با طول متغییر • زمان آماده‌سازی بالا • استفاده از توابع رمزنگاری پیچیده • زمانبر
AES	• بهینگی بالا • پیچیدگی پایین • امنیت بالا • مصرف منابع پایین	• نیاز به پردازش بالا • نیاز به تعداد دفعات برقراری ارتباط بالا • پیچیدگی تنظیمات • کندی اجرا
DES	• استفاده از کلیدهای یکسان در رمزنگاری و رمزگشایی • محرمانگی بالا • سرعت مناسب	• طول کلید کوتاه • سادگی شکستن کلید • استفاده از جداول جایگزینی ضعیف • ایمنی پایین • آسیب‌پذیری در برابر حملات جستجوی فراگیر • وابسته به کلید

جدول۲: شرح علامت‌های اختصاری استفاده شده

علامت اختصاری	شرح	علامت اختصاری	شرح
E_{ka}	کلید رمزنگاری کاربر A	M	پیامهای انتخابی مشترک
E_{kb}	کلید رمزنگاری کاربر B	U_{hd}	ساعت و تاریخ یکپارچه شده
D_{ka}	کلید رمزگشایی کاربر A	P_a	داده‌های استخراج شده از نمایه (profile) کاربر A
D_{kb}	کلید رمزگشایی کاربر B	P_b	داده‌های استخراج شده از نمایه کاربر B
T_a	شماره تلفن کاربر A	t	متغییری با مقادیر ۰ یا ۱ که تعیین کننده نوع تفسیر m است. t=1: مقدار توان پردازشی و حافظه به ازای ۱ دلار که در هر دوره m-ماهه دو برابر می‌شود. t=0: مقدار توان پردازشی و حافظه صرف نظر از ارزش مالی که در هر دوره m-ماهه دو برابر می‌شود
T_b	شماره تلفن کاربر B	m	تعداد ماه‌هایی که در آن انتظار می‌رود توان پردازشی پردازنده‌ها دو برابر شده و حجم حافظه‌ها افزایش یابد
Y	حاشیه عمر ایمن کلید	IMY	حجم غیر ممکن پردازش در سال y
y	سال آغازین در یک محدوده زمانی خاص	V	ضریب کندی سرعت بین کلیدهای متقارن و نامتقارن
s	سال پایانی در یک محدوده زمانی خاص	b	تعداد سال‌هایی که در آن انتظار می‌رود بودجه به دو برابر افزایش یابد

سرویس پیام کوتاه (Short Message Service Center – SMSC) هدایت می‌شوند. پیامک تا زمان تحویل و یا پایان تاریخ انقضا در SMSC باقی می‌مانند. گیرنده می‌تواند MS و یا دروازه پیامک (SMS Gateway) باشد. دروازه‌ها سرویس دهنده‌هایی هستند که با یک و یا چند SMSC بمنظور تولید محتوا برای کاربران در ارتباط هستند. محتوا می‌تواند ارسال یک نماد، زنگ، سرویس‌های بانکی، سرگرمی، و یا امثال آن باشد [۳۰].

حداکثر حجم داده‌های ارسالی در پیامک ۱۱۲۰ بیت است و بسته به نوع کاراکترهای استفاده شده، طول رشته ارسالی متغییر خواهد بود. در صورت تخصیص ۷ بیت به هر کاراکتر، طول رشته ۱۶۰ کاراکتر، برای کاراکترهای ۸ بیتی طول رشته ۱۴۰ کاراکتر، و در حالت کاراکترهای ۱۶ بیتی طول رشته ۷۰ کاراکتر خواهد بود. رشته‌هایی با طول بالاتر به چند پیامک تقسیم شده و در این حالت قسمتی از فضا به اطلاعات مورد نیاز برای ترکیب مجدد داده‌ها و چینش صحیح داده‌های دریافتی اختصاص می‌یابد.

سامانه‌های مصرفی معمولا با مشکلات امنیتی مواجه هستند. مهمترین مشکلات ساختاری پیامک عبارتند از:

- ساختار فنی ناامن پیامک
- تمرکز مهاجمین بر روی کاربران بجای سامانه برای نفوذ امنیتی

محتوای پیامک‌ها بطور کامل در دسترسی اپراتورها قرار دارد. بنابراین پیامک را نمی‌توان یک رسانه ایمن به شمار آورد. اگرچه دسترسی و نفوذ به سامانه‌های اپراتورها برای دستیابی به پیامک‌ها ممکن است کار پیچیده و مشکلی باشد، اما استراق سمع (sniff) و تصاحب (intercept) پیامک‌ها کار آسانی است. علاوه بر این، کاربران سطح بالا در شبکه اپراتور کسانی هستند که به راحتی به محتویات پیامک‌ها دسترسی دارند [۳۱]. ضعف‌های ساختاری قرارداد تبادل پیامک مشکلات امنیتی عدیده‌ای را تولید کرده که براحتی می‌تواند توسط مهاجمین بهره‌برداری گردد. مهم‌ترین ضعف‌های قرارداد پیامک عبارتند از:

- تصاحب پیامک (intercept): معمولا در شبکه‌های بی‌سیم (البته گاهی در شبکه های کابلی نیز دیده می شود)
- کاوش داده‌ها (snooping): ارسال عناصر شبکه از محل ذخیره و یا دستگاه
- جعل (spoofing): تصاحب دروازه پیامک بویژه در کاربرد ابزارهای تجاری
- حمله به دستگاه گیرنده/فرستنده (MS): دسترسی آسان به محتوای پیامک‌ها در درون دستگاه‌های فرستنده و گیرنده

۳-۲- توابع درهم‌سازی

تابع درهم‌سازی یک متن با طول دلخواه را به متنی با طول ثابت که با نام‌های مقدار درهم‌سازی، کد درهم‌سازی و یا مجموع درهم‌سازی شناخته می‌شود تبدیل می‌کند. تابع درهم‌سازی رمزنگاری یک تابع یک‌طرفه است که یک متن را به یک کد درهم‌سازی که قابل برگشت به حالت اولیه نیست تبدیل می‌کند. در توابع درهم‌سازی رمزنگاری مقدار ورودی با عنوان پیام (message) و مقدار خروجی با عنوان چکیده پیام (message digest) شناخته می‌شود. مهم‌ترین ویژگی‌های یک تابع درهم‌سازی عبارتند از [۳۳،۳۲]:

- محاسبه کد در هم‌سازی شده آسان است
- فرآیند تولید کد درهم‌سازی برگشت پذیر نیست
- تغییر پیام بدون تحت تاثیر قرار دادن کد درهم‌سازی امکان‌پذیر نیست
- دو پیام متفاوت با کد درهم‌سازی یکسان وجود ندارند

توابع درهم‌سازی کاربردهای فراوانی در تامین امنیت اطلاعات مانند امضای دیجیتال و یا کد اصالت سنجی پیام (Message Authentication Code-MAC) دارند [۳۵،۳۴]. جدول ۳ ویژگی‌های فنی مهم‌ترین توابع درهم‌سازی را نمایش می‌دهد.

جدول۳: نام و مشخصات فنی توابع پرکاربرد درهم‌سازی

نام تابع		سایز خارجی (بیت)	سایز داخلی (بیت)	مقاوم در برابر تصادم	مقاوم در برابر حمله افزایش طول
MD5		۱۲۸	۱۲۸	X	X
SHA-0		۱۶۰	۱۶۰	X	X
SHA-1		۱۶۰	۱۶۰	X	X
SHA-2	SHA2-224	۲۲۴	۲۵۶	✓	X
	SHA2-256	۲۵۶		✓	X
	SHA2-384	۳۸۴	۵۱۲	✓	X
	SHA2-512	۵۱۲		✓	X
	SHA2-512/224			✓	✓
	SHA2-512/256	۲۵۶		✓	✓
SHA-3	SHA3-224	۲۲۴	۱۶۰۰	✓	✓
	SHA3-256	۲۵۶	۱۶۰۰	✓	✓
	SHA3-384	۳۸۴	۱۶۰۰	✓	✓
	SHA3-512	۵۱۲	۱۶۰۰	✓	✓

۳-۳- ساختار مدل SSS

مدل ارائه شده، یک برنامه نصب شده بر روی تلفن‌های هوشمند است که کلیدهای رمزنگاری و رمزگشایی مورد نیاز برای ایمن‌سازی پیامک‌ها را بر اساس داده‌های تبادل شده بین کاربران در شبکه‌های اجتماعی تولید می‌کند. در این مدل، با استفاده از کد تابع درهم‌سازی تولید شده بر اساس نمایه‌های کاربری در شبکه اجتماعی انتخابی، دو کلید پویا برای رمزنگاری و رمزگشایی تولید می‌شود. این روش مستقل از شبکه GSM عمل کرده و برای ایجاد نشست ایمن نیازمند تبادل ۰ تا ۳ پیامک است. تا حجم یک کیلوبایت از آخرین اطلاعات استخراج شده از نمایه کاربری و پیام‌های متنی تبادل شده بین کاربران در تابع درهم‌سازی برای ایجاد کلید استفاده می‌شود. در صورت عدم وجود پیام، یک پیام تصادفی متنی تولید و ارسال شده و سپس از ترکیب آن با نمایه کاربر زمینه ساخت کلید ایجاد می‌شود. شمای کلی این روش برای تولید کلید در شکل ۱ نمایش داده شده است.

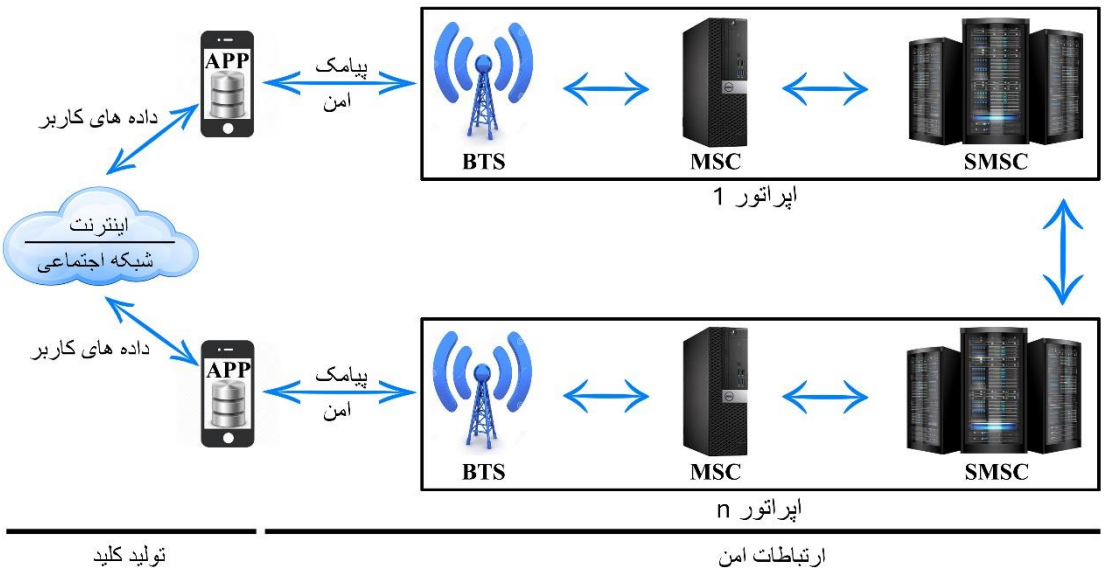
۳-۳-۱- تابع تولید کلید رمزنگاری و رمزگشایی

تابع درهم‌سازی مورد استفاده در این روش باید دو شرط اساسی را دارا باشد. اولین شرط، ارائه سطح ایمنی لازم برای تضمین محرمانگی پیام‌های رمز شده است. شرط دوم، برابری طول کلید با ضریبی از حداکثر طول یک پیامک است. در صورت بلندتر بودن طول کلید از حداکثر طول یک پیامک، فرآیند رمزنگاری نیازمند عملیات لایه‌گذاری (padding) خواهد بود. علاوه بر این به بیش از یک پیامک برای ارسال پیام نیاز است که منجر به افزایش هزینه می‌شود. در صورت کوتاه تر بودن طول کلید از ۱۱۲۰ بیت، باید دقت کرد که اولا طول آن باید ضریبی از ۱۱۲۰ بیت باشد تا در صورت تکرار کلید تمامی پیامک پوشش داده شود، و دوم اینکه طول کلید سطح ایمنی لازم را ایجاد کند.

در بین توابع درهم‌سازی ارائه شده در جدول ۳، طول پنج تابع SHA-0، SHA-1، SHA2-224، SHA2-512/224 وSHA3-224 برابر با ضریبی از طول پیامک است. با توجه به طول ۱۶۰ بیتی SHA-0 و SHA-1، و آسیب‌پذیری در برابر حملات تصادم و افزایش طول، این دو گزینه انتخاب‌های ایمنی برای استفاده در سامانه رمزنگاری به شمار نمی‌آیند. سه تابع SHA2-224، SHA2-512/224، و SHA3-224 دارای طول ۲۲۴ بیتی هستند که با ۵ بار تکرار، طول پیامک را پوشش می‌دهند. تابع SHA2-224 به دلیل ضعف در برابر حمله افزایش طول ایمن به شمار نمی‌آید. SHA3-224 در برابر حملات اشاره شده مقاوم است اما طول سایز داخلی آن ۱۶۰۰ بیت است که از طول یک پیامک بیشتر بوده و برای رمزنگاری آن مناسب نیست. SHA2-512/224 در برابر حملات جدول ۲ مقاوم بوده و سایز داخلی و خارجی آن هر دو ضریبی از طول پیامک و برابر با ۲۲۴ بیت است. بنابراین، این تابع درهم‌سازی برای تولید کلیدهای رمزنگاری مورد استفاده در مدل SSS انتخاب شده است.

۳-۳-۲- عوامل ساخت کلید

روش ارائه شده، با استفاده از داده‌های چهار عامل مختلف یک رشته متنی ایجاد می‌کند که مقدار درهم‌سازی شده آن توسط



شکل ۱: شمای کلی مدل تبادل ایمن پیامک بر مبنای شبکه‌های اجتماعی

تابع SHA2-512/224 به عنوان کلید رمزنگاری/رمزگشایی استفاده می‌شود. کلیدهای ایجاد شده مختص ارتباط بین دو کاربر خاص در یک محدوده زمانی خاص بوده و هر ساعت بروز رسانی می‌شوند. هر کاربر با استفاده از کلید پویا و یکتای خود پیام دریافت شده را رمزگشایی کرده و رمزنگاری هر پیام با استفاده از کلید مختص گیرنده آن صورت می‌پذیرد.

چهار عامل در SSS در فرآیند تولید کلید استفاده می‌شوند. اولین عامل، داده‌های نمایه کاربر است که داده‌های آن با توجه به شبکه اجتماعی انتخابی متفاوت است. دومین عامل، پیام‌های تبادل شده بین دو کاربر در شبکه اجتماعی انتخابی است. از بین چهار عامل انتخابی، پیام‌های تبادل شده تنها عامل مخفی و انحصاری بین دو کاربر است و عوامل دیگر بصورت عمومی در دسترس هستند. سومین عامل، شماره تلفن کاربر است. از آنجا که یک کاربر ممکن است از چندین شماره تلفن استفاده کند، استفاده از این عامل می‌تواند به تولید کلیدهای مختص به هر خط تلفن کمک کند. ترکیب ساعت و تاریخ، چهارمین عامل استفاده شده در تولید کلید است. این ترکیب در هر ساعت تغییر کرده، باعث ایجاد کلیدهای پویا شده و امکان اجرای برخی از حملات رمزنگاری را مسدود می‌کند.

هر کاربر از دو کلید جداگانه استفاده می‌کند. کلید اول با استفاده از اطلاعات فرستنده ایجاد شده و کلید دوم بر اساس مشخصات گیرنده تولید می‌شود. پیام در زمان ارسال با استفاده از کلید گیرنده به رمز در می‌آید. گیرنده نیز پیام‌های دریافتی را با استفاده از کلید خود رمزگشایی می‌کند. بنابراین، همانطور که در معادله‌های ۱ و ۲ نشان داده شده است، کلید رمزنگاری کاربر A(E_{ka}) معادل کلید رمزگشایی کاربر B(D_{kb}) بوده، و کلید رمزگشایی کاربر A(D_{ka}) برابر کلید رمزنگاری کاربر B(E_{kb}) می‌باشد. نمادهای استفاده شده برای تولید کلیدهای رمزنگاری و رمزگشایی کاربران A و B در جدول ۲ شرح داده شده است. در طول یک نشست، تغییرات داده‌های تبادل شده و نمایه کاربری تاثیری بر روی فرآیند تولید کلید نداشته و تنها عامل متغییر ساعت و تاریخ است.

$$E_{ka} = D_{kb} \quad (۱)$$

$$E_{kb} = D_{ka} \quad (۲)$$

عوامل استفاده شده در تولید هر یک از کلیدها در معادله‌های (۳) تا (۶) نمایش داده شده و عبارتند از:

$$E_{ka} = SHA2-512/224(\mathrm{M} + \mathrm{U_{hd}} + \mathrm{T_b} + \mathrm{P_b}) \quad (۳)$$

$$E_{kb} = SHA2-512/224(\mathrm{M} + \mathrm{U_{hd}} + \mathrm{P_a} + \mathrm{T_a}) \quad (۴)$$

$$D_{ka} = SHA2-512/224(\mathrm{M} + \mathrm{U_{hd}} + \mathrm{T_a} + \mathrm{P_a}) \quad (۵)$$

$$D_{kb} = SHA2-512/224(\mathrm{M} + \mathrm{U_{hd}} + \mathrm{T_b} + \mathrm{P_b}) \quad (۶)$$

از آنجا که ساعت یکی از عوامل مورد استفاده در تولید کلید است، حداکثر عمر کلیدهای تولید شده ۶۰ دقیقه می‌باشد. بنابراین، در صورتی که یک پیام در آخرین لحظات کلید جاری به رمز درآمده باشد و در زمان اعتبار کلید بعدی به دست گیرنده برسد، قابل رمزگشایی نخواهد بود. این مشکل همچنین ممکن است بدلیل تاخیر اپراتور در تحویل پیام و یا در دسترس نبودن کاربر هم بوجود آید. برای حل این مشکل در زمان رمزگشایی پیام‌ها ابتدا از کلید جاری استفاده شده و در صورت عدم موفقیت کلید پیشین نیز تست می‌گردد. در صورت عدم موفقیت در رمزگشایی با استفاده از هر دو کلید، پیامک دریافتی به عنوان یک پیام نامعتبر شناسایی خواهد شد.

کاربران این روش ممکن است در دو منطقه زمانی مختلف قرار داشته و از تقویم‌های متفاوتی نیز استفاده کنند. عدم تطابق ساعت و تاریخ کاربران منجر به تولید کلیدهای متفاوت خواهد شد. برای پیشگیری از این مشکل، ساعت UTC (Coordinated Universal Time) و تقویم میلادی به عنوان مرجع درنظر گرفته شده، و ساعت و تقویم محلی ابتدا به مرجع تبدیل شده و سپس در فرآیند تولید کلید استفاده می‌شوند.

پس از نصب برنامه، در صورت عدم وجود تبادل پیام بین کاربران در شبکه اجتماعی مدنظر، یک پیام تصادفی ایجاد و ارسال می‌گردد. این پیام در پایگاه‌داده‌های برنامه SSS در درون تلفن‌های همراه هر دو کاربر ذخیره شده، و از آن برای داده‌های اولیه تولید کلید استفاده می‌شود. در هر بار اتصال به اینترنت، SSS اطلاعات پایگاه‌داده خود را بروز رسانی می‌کند و پیام‌های مبادله شده به پایگاه‌داده مد نظر افزوده می‌شوند. در صورت توافق کلید و برقراری یک نشست ایمن جدید، داده‌های قبلی به شرط عبور از مرز ۱ کیلو بایت از پایگاه‌داده حذف می‌گردند. ایجاد نشست ایمن با کاربر جدید پیش از تبادل پیام در شبکه اجتماعی و یا ایجاد داده‌های لازم تصادفی امکان‌پذیر نیست. به همین دلیل، کاربر می‌تواند کاربرانی را که احتمال می‌دهد در آینده با آنها تبادل پیام داشته باشد را به برنامه معرفی کرده و زمینه ایجاد نشست‌های ایمن در آینده را فراهم نماید.

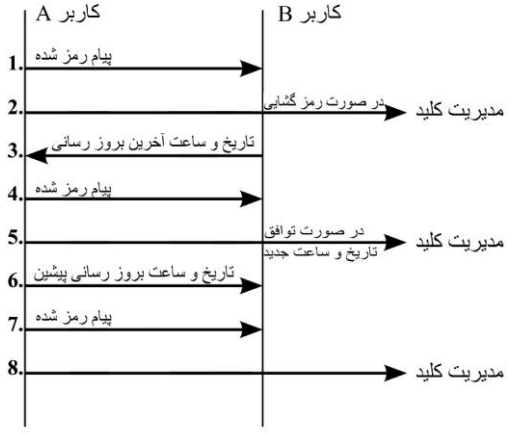
۳-۳-۳- توافق کلید

فرآیند توافق کلید بین کاربران با سه حالت ممکن است مواجه

شود. در اولین حالت، اطلاعات ذخیره شده در دستگاه‌های کاربر A و B هر دو بروز بوده و درنتیجه کلیدهای یکسان بدون نیاز به تبادل پیام اضافی ایجاد می‌شوند. از آنجا که در ابتدا مشخص نیست که هر دو کاربر از داده‌های یکسانی استفاده می‌کنند یا خیر، کاربر A پیام خود را با استفاده از آخرین نسخه داده‌های ذخیره شده برای کاربر B ارسال می‌کند. موفقیت رمزگشایی پیام دریافت شده توسط کاربر B مشخص می‌کند که داده‌های ذخیره شده هر دو کاربر بروز بوده و نسشت ایمن آغاز می‌شود. در این حالت، هیچ‌گونه پیام سرباری برای توافق کلید ارسال نشده است. شکل ۲ این مراحل با اعداد ۱ و ۲ مشخص کرده است.

حالت دوم زمانی است که پیام دریافتی توسط کاربر B قابل رمزگشایی نیست. برای ایجاد یک نشست ایمن، کاربر B آخرین ساعت و تاریخ بروز رسانی داده‌های خود را بر اساس زمان مرجع در قالب متن ساده برای کاربر A ارسال می‌کند. در صورت وجود داده‌های مرتبط با ساعت و تاریخ ذکر شده، کاربر A پیام خود را مجددا با استفاده از کلید ایجاد شده توسط داده‌های تاریخ تعیین شده به رمز درآورده و برای کاربر B ارسال می‌کند. در این حالت ۲ پیام سربار برای فرآیند توافق کلید ارسال شده است. در شکل ۲، مراحل توافق کلید حالت دوم با شماره های ۳، ۴، و ۵ مشخص شده‌اند.

حالت سوم زمانی اتفاق می‌افتد که اطلاعات پایگاه‌داده کاربر A قدیمی‌تر از کاربر B است. برای حل این مشکل کاربر A آخرین تاریخ بروز رسانی خود را برای کاربر B ارسال می‌کند. پس از آن، بدون ارسال هرگونه پیام اضافی فرآیند توافق کلید صورت گرفته و کاربران می‌توانند نشست‌های ایمن را برقرار کنند. در حالت سوم تعداد پیام‌های سربار ۳ پیام است. مراحل توافق کلید در حالت



شکل ۲: مراحل توافق کلید

سوم با شماره‌های ۶، ۷، و ۸ در شکل ۲ علامت‌گذاری شده‌اند.

۳-۳-۴- آغاز و پایان نشست

نشست ایمن با ارسال یک پیام از کاربر A به B ایجاد می‌شود. اگرچه نشست ایمن پس از توافق کلید آغاز می‌شود، اما پیامی برای پایان نشست ارسال نمی‌شود. پایان نشست بصورت خودکار یک ساعت پس از استفاده از آخرین کلید صورت می‌پذیرد. به عبارت دیگر، پایان نشست بین ۶۰ تا ۱۱۹ دقیقه پس از ارسال آخرین پیام پایان می‌یابد. اهمیت تعیین پایان نشست در آغاز نشست بعدی است. پیش از پایان یک نشست، پیام‌های تبادل شده بین کاربران در شبکه اجتماعی و یا بروز رسانی نمایه تاثیری در فرآیند تولید کلید نخواهد داشت.

۴- ارزیابی و بحث

در ادامه، این روش با چهار معیار عمر ایمن کلید، مقاومت در برابر حملات، توجیه اقتصادی، و رضایت کاربران در سادگی کاربری ارزیابی شده است. برای ایمنی کلید، حداقل عمر ایمن آن بحث شده است. مقاومت در برابر حملات از هفت وجه مختلف بررسی شده، و از دید اقتصادی هزینه این روش با مدل توافق کلید بر اساس Diffie-Hellman مقایسه شده است. برای سنجش رضایت کاربران از سادگی کاربری، نتایج پرسشنامه انتشار یافته بین ۵۰ کاربری که از این برنامه استفاده کرده‌اند تحلیل شده است.

۱-۱- ارزیابی

۴-۱-۱- عمر ایمن کلید

این روش از کلیدهای متقارن برای رمزنگاری و رمزگشایی استفاده می‌کند. Lenstra و Verheul [۳۶] مدلی را برای ارزیابی عمر ایمن کلیدهای رمزنگاری ارائه کرده‌اند که در آن عوامل توان پردازش در سال، ضریب رشد توان پردازش رایانه‌ها، هزینه سخت افزاری با ضریب تغییر قیمت، ضریب سرعت بین کلیدهای متقارن و نامقارن، و طول کلید، عمر ایمن کلید را مشخص می‌کند. در معادله ۷، عبارت $2^{12\,(y-s)/m}$ نشانگر سرعت مورد انتظار پردازنده‌ها مابین سال s تا y بوده و $2^{t(y-s)/b}$ پیش بینی افزایش بودجه است.

$$\mathrm{IMY}\,(y) = 5 * 10^5 * 2^{12\frac{y-s}{m}} * 2^{\frac{t(y-s)}{b}} Mips - Years \quad (۷)$$

$$Secure\ lifetime = Key\ bits + Log_2\left(\frac{IMY(y)}{5*10^5*v}\right) = 56 + (y-s)\left(\frac{12}{m}+\frac{t}{b}\right) - Log_2\ v\ bits \quad (۸)$$

بر اساس محاسبات صورت گرفته توسط Lenstra و Verheul [۳۲] بر مبنای معادله ۸، کلیدهای متقارن با طول ۱۰۹ بیت حداقل تا سال ۲۰۵۰ ایمن خواهند بود. با توجه به طول 224 بیتی کلیدهای مورد استفاده، در حال حاضر محدودیت طول عمر ایمن برای کلیدهای مورد استفاده در SSS وجود ندارد.

۴-۱-۲- مقاومت در برابر حملات

حمله بازنشر (Replay attack): حمله بازنشر نوعی از حملات شبکه است که در آن ارسال یک داده معتبر با اهداف مخرب تکرار شده و یا با تاخیر ارسال می‌شود. مهاجمین این داده‌ها را تولید کرده و یا داده‌های معتبر را در میان راه تصاحب کرده و مجددا به عنوان بخشی از یک حمله تغییر شکل یافته با جایگزینی بسته های IP ارسال می‌کنند. در مدل طراحی شده، پیامک‌های به رمز درآمده عمری بین ۶۰ تا نهایتا ۱۱۹ دقیقه دارند. مدت زمانی که یک مهاجم می‌تواند یک پیامک رمز شده را مجددا ارسال نماید محدود بوده و پیامک‌ها پس از گذر عمر معتبر کلید قابل رمزگشایی و پاسخگویی نیستند. بنابراین در این مدل امکان اجرای این حمله محدود شده است.

حمله سرقت نشست (Session hijacking attack): سرقت نشست بهره برداری غیر مجاز از یک نشست معتبر است که گاهی کلید نشست نیز نامیده می‌شود. در این حمله سعی بر ایجاد دسترسی غیر معتبر به داده‌ها و یا خدمات در حال ارائه است. در مدل SSS، یکی از عوامل تولید کلید شماره تلفن دستگاه تلفن همراهی است که سعی بر رمزگشایی پیام دریافت شده دارد. بنابراین حتی در صورتی که کاربر A از دو شماره تلفن مختلف برای برقراری نشست با کاربر B استفاده کند، بدلیل بررسی مطابقت شماره تلفن با کلید رمزگشایی، امکان استفاده از نشست ایجاد شده در تلفن همراه دیگر با وجود یکسان بودن کابران، داده‌های شکبه اجتماعی، و تمامی عوامل دیگر ساخت کلید وجود ندارد.

حمله مرد میانی (Man in the middle attack): این حمله زمانی اتفاق می‌افتد که مهاجم داده‌های در حال تردد بین دو کاربر را از کانال خود عبور داده و محتوای آنرا در صورت لزوم تغییر دهد. در ابتدای ایجاد نشست، مهاجم بین کاربران قرار گرفته و با تظاهر به اینکه کاربران مستقیما با یکدیگر در ارتباط هستند، دو ارتباط مستقل با آنها ایجاد می‌کند. هر داده ارسال شده ابتدا به دست مهاجم رسیده و سپس بعد از اعمال تغییرات برای کاربر دیگر ارسال می‌شود. در مدل SSS از آنجا که کانال ایجاد نشست اولیه (اینترنت) با کانال ارتباطی پیامک (اپراتورهای تلفن همراه) متفاوت می‌باشد، مهاجم شانس نفوذ به فرآیند ایجاد کلید نشست را از طریق داده‌های تبادل شده در شبکه تلفن همراه نخواهد یافت. روشهای مبتنی بر Diffie-Hellman در برابر این حمله آسیب پذیر هستند. علاوه بر این، به دلیل استفاده از اینترنت برای دریافت عوامل ساخت کلید بجای شبکه GSM، و همچنین تولید کلید در دستگاه بجای انتشار آن، حملات پیش انتشار کلید در مدل SSS قابل پیاده سازی نیستند.

حمله جستجوی گسترده (Brute force attack): در جستجوی گسترده تمامی حالات ممکن تا زمان دستیابی به پاسخ صحیح بررسی می‌شود. چنین حمله‌ای زمانی اجرا می‌شود که ضعف شناخته شده‌ای در سامانه رمزنگاری مد نظر یافت نشده باشد. تعداد محاسبات مورد نیاز در جستجوی گسترده 2^L است که در آن L تعداد بیت‌های کلید رمزنگاری است. با توجه به طول ۲۲۴ بیتی کلید ایجاد شده توسط SHA512/224، تعداد محاسبات لازم برای کشف کلید مورد استفاده در مدل SSS تعداد 2^{224} است که از لحاظ فنی امکان پیاده سازی چنین حمله‌ای وجود ندارد. علاوه بر این، کلیدهای تولید شده پویا بوده و در هر ساعت تغییر می‌یابند.

حمله تاریخ تولد (Birthday attack): نوعی از حمله به سامانه‌های رمزنگاری است که بر پایه محاسبات احتمالاتی مساله تاریخ تولد قرار گرفته است. مساله تاریخ تولد بر اساس احتمال تصادف (collision) بین تلاش‌ها در حمله‌های تصادفی و درجه ثابتی از جایگشت قرار گرفته است. در این حمله، احتمال کشف تصادفی یک ورودی که مقدار در همسازی آن با کلید ایجاد شده از درهم‌سازی متن اصلی یکی باشد، به دو برابر حمله جستجوی گسترده افزایش می‌یابد. به عبارت دیگر، حجم جستجوها از 2^L در جستجوی گسترده به $2^{\frac{L}{2}}$ کاهش می‌یابد. با توجه به طول کلید ۲۲۴ بیتی در SSS، تعداد محاسبات لازم برای کشف کلید در حمله تاریخ تولد 2^{112} محاسبه است که از لحاظ فنی غیر ممکن به شمار می‌آید. مجددا باید مد نظر داشت که کلیدهای مورد استفاده SSS پویا بوده و در هر ساعت تغییر می‌یابند.

حمله توسعه یافته بر طول مقدار درهم‌سازی شده (Length extension attack): این حمله زمانی صورت می‌گیرد که مهاجم می‌تواند از Hash(message 1) و طول message 1 برای محاسبه Hash(message1‖ message 2) که در آن message 2 تحت کنترل مهاجم است استفاده کند. این حمله می‌تواند بر روی مقادیر درهم‌سازی شده با ساختار Hash(secret ‖ message) در زمانی که پیام و طول رمز شناخته شده است صورت گیرد. الگوریتم‌هایی مانند MD5، SHA-1، و بعضی از انواع SHA-2 در

برابر این حمله آسیب‌پذیر هستند. SHA512/224 و SHA512/256 تنها نمونه‌های ایمن از خانواده SHA2 در برابر حمله توسعه یافته بر طول مقدار درهم‌سازی شده به شمار می آیند. بنابراین، با توجه به استفاده SSS از SHA512/224، این مدل در برابر حمله توسعه یافته بر طول مقدار درهم‌سازی شده مقاوم است.

درک محتوا و دستکاری داده (tampering) در SMSC/پراتورها: در روش‌هایی که ایمنی آنها توسط مولفه سوم تامین می‌شود (مانند روش‌های مبتنی بر CA و یا کلیدهای از پیش به اشتراک گذاشته شده)، اپراتورهای سرویس‌دهنده امکان درک محتوا و دستکاری داده‌ها را دارند. از آنجا که کانال اولیه برقراری ارتباط ایمن در SSS متفاوت از شبکه سرویس دهنده پیامک است، اپراتورها از فرآیند ایجاد کانال ایمن حذف شده‌اند و بنابراین بر محتوای تبادل شده تسلط نخواهند داشت.

ویژگی‌های امنیتی SSS در برابر حملات در جدول ۴ بصورت خلاصه ارائه شده است.

جدول۴: ویژگی‌های امنیتی SSS در برابر حملات

حمله	مقاوم	مقاومت نسبی
حمله بازنشر		✓
حمله سرقت نشست	✓	
حمله مرد میانی	✓	
حمله جستجوی گسترده	✓	
حمله تاریخ تولد	✓	
حمله توسعه یافته بر طول مقدار درهم‌سازی شده	✓	
درک محتوا و دستکاری داده	✓	

۴-۱-۳- توجیه اقتصادی

SSS وابسته به زیرساخت‌هایی مانند مراکز CA و یا اپراتورها نیست. بنابراین، ساختار آن از جنبه اقتصادی با روش Diffie-Hellman برای ایجاد یک کانال ایمن مقایسه شده است. به همین منظور، تعداد پیام‌های تبادل شده برای ایجاد کانال ایمن در هر دو روش مقایسه گردیده است.

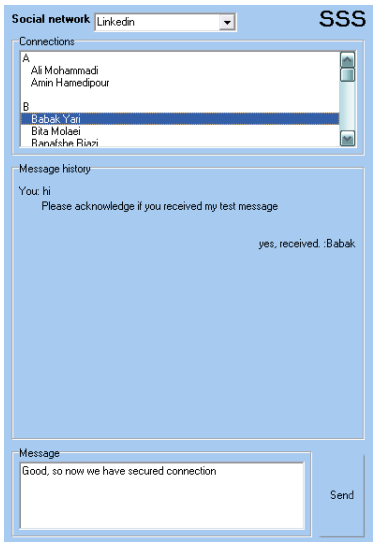
Diffie-Hellman در پی مجموعه‌ای از محاسبات ریاضی یک زوج کلید متقارن را به منظور ایجاد یک کانال امن تولید می‌کند. برای ایجاد این کانال هفت پیام باید تبادل شود [۳۷]. روش ارائه شده نیازمند تبادل ۰ تا ۳ پیام است. نتایج مقایسه دو روش در جدول ۵ نشان می‌دهد هزینه تولید پیام در روش پیشنهادی بین ۵۷.۱۴٪ تا ۱۰۰٪ کاهش یافته است.

جدول۵: مقایسه هزینه SSS با Diffie-Hellman در تولید کانال ایمن

مراحل توافق کلید SSS	تعداد پیام‌ها SSS	تعداد پیام‌ها Diffie-Hellman	بهبود اقتصادی
حالت اول توافق	۰	۷	۱۰۰٪
حالت دوم توافق	۲		۷۱.۴۳٪
حالت سوم توافق	۳		۵۷.۱۴٪

۴-۱-۴- رضایت کاربران از ایمنی و سادگی کاربری

به منظور ارزیابی رضایت کاربران از سادگی استفاده و ایمنی ایجاد شده، یک نمونه آزمایشی از این برنامه تولید و در اختیار ۵۰ کاربر قرار گرفت. شکل ۳ تصویر نمونه تولید شده را نمایش می‌دهد.



شکل ۳: تصویر نمونه آزمایشی برنامه SSS

کاربران بصورت تصادفی از دانشجویان دانشگاه انتخاب شدند. پس از تجربه کار با نمونه تولید شده از کاربران خواسته شد پرسشنامه‌های ارائه شده را پاسخ دهند. سوالات پرسیده شده در جدول ۶ و نتایج بدست آمده از پرسشنامه‌ها در جدول ۷ ارائه شده است.

پرسشنامه متشکل از ۴ سوال بوده که سطح استفاده از اینترنت، عضویت کاربر در شبکه‌های اجتماعی، استفاده از تلفن‌های هوشمند، و رضایت کاربران در استفاده از ابزار ارائه شده را می‌سنجد. بر اساس پیش‌نیازهای استفاده از این ابزار، در سنجش سطح رضایت، نظرات کاربرانی لحاظ شده که به سه سوال اول پاسخ مثبت داده‌اند.

تحلیل نتایج در جدول ۵ نشان می‌دهد که ۹۱.۱٪ از کاربران واجد شرایط، SSS را به عنوان ابزاری قابل اعتماد برای تامین امنیت ارتباطات خود ارزیابی کردند و ۸.۹٪ از کاربران علاقه‌ای به استفاده

از این نرم افزار نشان ندادند. ۱۰٪ از کل کاربران، واجد شرایط پیش نیازهای تعیین شده نبودند.

جدول۶: پرسشنامه ارزیابی سطح رضایت کاربران

شماره	سوال
۱	آیا در شبکه‌های اجتماعی عضو هستید؟
۲	آیا از تلفن‌های هوشمند استفاده می‌کنید؟
۳	در صورت استفاده از تلفن‌های هوشمند، معمولا در چه بازه‌های زمانی از اینترنت آن استفاده می‌کنید؟ (روزانه، هفتگی، ماهانه، استفاده نمی‌کنم)
۴	آیا مایل به استفاده از SSS برای ایمن‌سازی تبادلات پیامکی خود هستید؟

جدول۷: تحلیل آماری سطح رضایت کاربران

عنوان	تعداد	تعداد کل	درصد
عدم استفاده از شبکه‌های اجتماعی	۳	۵۰	۶٪
عدم استفاده از تلفن‌های هوشمند	۴	۵۰	۸٪
عدم استفاده از اینترنت در تلفن همراه	۵	۵۰	۱۰٪
تعداد پرسشنامه‌ها با پاسخ منفی به سوالات ۱، ۲، یا ۳	۵	۵۰	۱۰٪
تعداد پرسشنامه‌ها با پاسخ مثبت به سوالات ۱، ۲، و ۳	۴۵	۵۰	۹۰٪
تعداد پرسشنامه‌ها با پاسخ مثبت به سوالات ۱، ۲، ۳، و ۴	۴۱	۴۵	۹۱.۱٪

۴-۲- بحث و جمع بندی

مدل SSS با استفاده از داده‌های ذخیره شده خود دو کلید رمزنگاری و رمزگشایی یکتا، وابسته به زمان، منحصر به ارتباط بین دو کاربر خاص، و وابسته به شماره های تلفن خاص تولید می‌کند. این فرآیند پویا بوده و مستقل از اپراتورهای شبکه عمل می‌کند. هدف اصلی این مدل ارائه سرویس ایمن و مستقل از اپراتورهای واسط به کاربرانی است که پیش از آن، از طریق شبکه‌های اجتماعی با یکدیگر در ارتباط بوده و به برقراری ارتباط ایمن از طریق پیامک نیز نیاز پیدا می‌کنند. ساختار ویژه SSS مزایای متعددی در اختیار کاربران خود قرار می‌دهد، اما از سوی دیگر با محدودیت‌هایی نیز مواجه است. مهمترین مزایای این روش عبارتند از:

- کاهش هزینه فرآیند توافق کلید به حداقل ۰ و حداکثر ۳ پیامک
- استفاده از کلیدهای پویا در رمزنگاری و رمزگشایی
- استفاده از کلیدهای متفاوت در رمزنگاری و رمزگشایی
- مقاوم در برابر طیف وسیعی از حملات رمزنگاری (بازنشر، مرد میانی، جستجوی گسترده، تاریخ تولد، توسعه طول مقدار درهم‌سازی شده)
- تولید کلیدهای وابسته به شماره تلفن و مقاوم در برابر سرقت نشست
- استقلال از تمامی اپراتورهای واسط
- عدم امکان درک محتوا و دستکاری داده‌ها توسط اپراتورهای واسط
- عدم نیاز به پیش انتشار کلید
- عدم نیاز به زیرساخت‌های ویژه مانند مراکز صدور گواهی
- سادگی مدل و حجم پردازش پایین در فرآیندهای تولید کلید و رمزنگاری/رمزگشایی
- با وجود مزایای متعدد ارائه شده توسط مدل SSS، بدلیل وابستگی ساختار آن به شبکه‌های اجتماعی، استفاده از آن با محدودیت‌هایی به شرح زیر روبرو است:
- عدم امکان برقراری ارتباط ایمن بین مخاطبانی که از طریق شبکه‌های اجتماعی در ارتباط نیستند
- وابستگی غیر برخط (off line) به اینترنت

۵- نتیجه گیری

در این تحقیق یک روش ایمن‌سازی تبادل پیامک به نام SSS با استفاده از یک برنامه کاربردی مستقل از اپراتورهای شبکه تلفن همراه ارائه شده است. چهار عامل داده‌های نمایه شبکه اجتماعی، پیام‌های تبادل شده در شبکه اجتماعی، شماره تلفن و ساعت و تاریخ یکپارچه شده، یک رشته متنی را تشکیل می‌دهند که مقدار تابع درهم‌سازی SHA2-512/224 آن برای هر کاربر یک کلید وابسته به زمان تولید می‌کند. کاربران پیام‌های دریافتی خود را با استفاده از کلید خود رمزگشایی می‌کنند و رمزنگاری پیام ارسالی با استفاده از کلید ویژه کاربر مخاطب صورت می‌پذیرد.

ساختار ویژه SSS دارای مزایای متعددی مانند کاهش چشمگیر هزینه ایجاد کانال ایمن، مقاومت در برابر طیف وسیعی از حملات، استقلال از اپراتورها، و عدم نیاز به زیرساخت‌هایی مانند CA است. از سوی دیگر، وابستگی این ساختار به شبکه‌های اجتماعی امکان ایجاد کانال ایمن را محدود به کاربرانی می‌کند که از پیش در این شبکه‌ها به یکدیگر متصل بوده‌اند.

نتایج ارزیابی نشان می‌دهد که ایمنی کلیدهای تولید شده تضمین شده است، در برابر حملات متعدد رمزنگاری، سرقت نشست، و دستکاری داده‌ها سطح ایمنی بسیار بالا بوده، از دید اقتصادی بین ۵۷٪ تا ۱۰۰٪ بهینگی وجود دارد، و نهایتا ۹۱.۱۹٪ کاربران آنرا

ایمن دانسته و از سادگی کاربرد آن رضایت دارند.

مراجع

[1] M. W. Khan, “SMS Security in Mobile Devices: a Survey” International Journal of Advanced Networking and Applications, Vol. 5, No. 2, pp.1873-1882, 2013.

[2] S. Bojjagani and V. N. Sastry, “SSMBP: A Secure SMS-based Mobile Banking Protocol with Formal Verification”. In International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 252-259, 2015.

[3] S. Yazdanpanah, and S. Shojae Chaeikar, “IKM-based security usability enhancement model,” IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS), 4, 2012.

[4] N. Saxena and N. S. Chaudhari, “EasySMS: A Protocol for End-to-end Secure Transmission of SMS” IEEE Trans. Inf. Forensic Secur, Vol. 9, No. 7, pp. 1157-1168, 2014.

[5] T. Khodadadi, M. Zamani, S. S. Chaeikar, Y. Javadianasl, M. Talebkhah, and M. Alizadeh, “Exploring the Benefits and Drawbacks of Machine Learning in Cybersecurity to Strengthen Cybersecurity Defences”. In 2023 IEEE 30th Annual Software Technology Conference (STC), 2023.

[6] J. Alwen and J. Blocki, “Towards Practical Attacks on Argon2i and Balloon Hashing”. In International Conference on Security and Privacy, pp. 142-157, 2017.

[7] J. Lee and Y. Oh, “A Study on Providing the Reliable and Secure SMS Authentication Service”. In International Conference on Ubiquitous Intelligence and Computing, pp. 620-624, 2014.

[8] N. B. Anuar and L. N. Kuen, and O. Zakaria and A. Gani, and A. W. Wahab, “GSM Mobile SMS/MMS Using Public Key Infrastructure: m-PKI” WSEAS Transactions on Computers, Vol 7, No. 8, pp. 1219-1229, 2008.

[9] S. Yazdanpanah, S. Shojae Chaeikar, and A. Jolfaei, “Monitoring the security of audio biomedical signals communications in wearable IoT healthcare,” Digital Communications and Networks, 9 (2), pp.393-399, 2023.

[10] M. Raza and M. Iqbal and M. Sharif and W. Haider, “A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication” World Applied Sciences Journal, Vol. 19, No. 4, pp. 1439-1244, 2012.

[11] S. Shojae Chaeikar, A. Jolfaei, and N. Mohammad, “AI-enabled cryptographic key management model for secure communications in the internet of vehicles,” IEEE Transactions on Intelligent Transportation Systems, 24(4), pp.4589-4598, 2022.

[12] S. Shojae Chaeikar, A. Ahmadi, S. Karamizadeh, and N. Shoja Chaeikar, “SIKM–a smart cryptographic key management framework,” Open Computer Science, 12(1), pp.17-26, 2022.

[13] S. Honarbakhsh, M. Masrom, M. Zamani, S. Shojae Chaeikar, and R. Honarbakhsh, “A Trust Based Clustering Model for Dynamic Monitoring in Ad hoc Network,” In International Conference on Computer and Computational Intelligence (ICCCI 2010), 2010.

[14] M. A. Hossain and S. Jahan and M. M. Hussain and M. R. Amin and S. S. Newaz, “A Proposal for Enhancing the Security System of Short Message Service in GSM”. In International Conference on Anti-counterfeiting, Security and Identification, pp. 235-240, 2008.

[15] IPCS Group, “IPCryptSim SMS Encryption”, http://www.ipcslive.com/pdf/IPCSSMS.pdf, 2018.

[16] H. Rongyu and Z. Guolei and C. Chaowen and X. Hui and Q. Xi and Q. Zheng, “A PK-SIM Card Based End-to-end Security Framework for SMS” Computer Standards & Interfaces, Vol. 31, No. 4, pp. 629-641, 2009.

[17] M. Toorani and A. Beheshti, ”SSMS-A Secure SMS Messaging Protocol for the M-payment Systems”. In International Conference on Computers and Communications, pp. 700-705, 2008.

[18] M. Hassinen and K. Hyppönen and K. Haataja, “An Open, PKI-based Mobile Payment System” Emerging Trends in Information and Communication Security, Vol. 1, No. 1, pp. 86-100, 2006.

[19] U. Chirico, “How to Protect Your Privacy in SMS Communication”, http://www.ugochirico.com/post/2010/08/26/How-to-protect-your-privacy-in-SMS-communication, 2018.

[20] M. Hassinen, “SafeSMS-end-to-end Encryption for SMS”. In International Conference on Telecommunications, pp. 359-365, 2005.

[21] D. Lisonek and M. Drahanský, “SMS Encryption for Mobile Communication”. In International Conference on Security Technology, pp. 198-201, 2008.

[22] M. Hassinen and S. Markovski, “Secure SMS Messaging Using Quasigroup Encryption and Java SMS API”, http://www.cs.uku.fi/~mhassine/VOH/Luennot/MIDLET/Presentation.pdf, 2018.

[23] F. Bélanger and L. Carter, “Trust and Risk in E-government Adoption” The Journal of Strategic Information Systems, Vol. 17, No. 2, pp. 165-176, 2008.

[24] J. L. Lo and J. Bishop and J. H. Eloff, “SMSSec: an End-to-end Protocol for Secure SMS” Computers & Security, Vol. 27, No. 5, pp. 154-167, 2008.

[25] A. Grillo and A. Lentini and G. Me, G. F. Italiano, “Transaction Oriented Text Messaging with Trusted-SMS”. In International Conference Computer Security Applications, pp.485-494, 2008.

[26] M. Agoyi and D. Seral, “SMS Security: an Asymmetric Encryption Approach”. In International Conference on Wireless and Mobile Communications, pp. 448-452, 2010.

[27] C. Narendiran and S. A. Rabara and N. Rajendran, “Performance Evaluation on End-to-end Security Architecture for Mobile Banking System”. International Conference on Wireless Days. pp. 1-5, 2008.

[28] B. Ahamed Bazeer, and M. Krishnamoorthy, "SMS encryption and decryption using modified vigenere cipher algorithm" Journal of the Operations Research Society of China, pp 1-14, 2020.

[29] M. Q. U. A. Zam Zam, H. Ashraf, and N. Z. Jhanjhi, "An Improved SMS Security Technique to Avoid Plaintext and Dictionary Attacks" Preprints, 2024.

[30] A. Oberle and P. Larbig and R. Marx and F. G. Weber and D. Scheuermann and D. Fages and F. Thomas, “Preventing Pass-the-Hash and Similar Impersonation Attacks in Enterprise Infrastructures”. In International Conference on Advanced Information Networking and Applications, pp. 800-807, 2016.

[31] S. S. Chaeikar and A. B. Manaf and M. Zamani, “Cryptography and Security in Computing” InTech, 2012.

[32] A. Mirghadri and M. Yosefipour and B. Khadem and M. Sajadieh, "Two New Methods for Designing 192-bit Block Ciphers Based on Switching Structure and Recursive Diffusion Layers" Advanced Defence Sci. & Tech, Vol. 10, No. , pp. 251-259, 2016.

[33] L. Dong and Y. Wang and W. Wu J. Zou, “Known-key Distinguishers on 15-round 4-branch Type-2 Generalised Feistel Networks with Single Substitution–permutation Functions and Near-collision Attacks on Its Hashing Modes” IET Information Security, Vol. 9, No. 5, pp. 277-283, 2015.

[34] M. Kashif, “Secure SMS Communication Using Encryption Gateway and Digital Signature”. In International Conference on Computational Science and Engineering, pp. 1430-1434, 2014.

[35] M. Alizadeh and S. Baharun and M. Zamani and T. Khodadadi and M. Darvishi and S. Gholizadeh and H. Ahmadi, “Anonymity and

Untraceability Assessment of Authentication Protocols in Proxy Mobile IPv6" Jurnal Teknologi. Pp. 31-34, 2015.

[36] A. K. Lenstra and E. R. Verheul, "Selecting Cryptographic Key Sizes" Journal of Cryptology, Vol. 14, No. 4, pp. 255-293, 2001.

[37] A. Faz-Hernández and J. López and E. Ochoa-Jiménez and F. Rodríguez-Henríquez, "A Faster Software Implementation of the Supersingular Isogeny Diffie-hellman Key Exchange Protocol" IEEE Trans. Comput., 2017.