International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

ANDROID BASED ENCRYPTED SMS SYSTEM

Nithish Kumar B[#1], Dr.T.Velumani[*2]

[#]Student, B.Sc Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021
ali.alsyani73@gmail.com

[*]Assistant Professor, Department of Computer Science, Rathinam College of Arts and Science, Coimbatore, Tamil Nadu, India -641021
velumani.cs@rathinam.in

Abstract - **The improvement of media communications innovation is so quick has given such extraordinary advantages. With the media transmission innovation, distance and time never again is a critical deterrent. One of the aftereffects of broadcast communications innovation that is notable is the Short Message Service (SMS). Android SMS is a local assistance that permits the clients to get SMS on cell phone and send messages to other telephone numbers. In this work an application is created on the cell phone to adjust the SMS message into ciphertext so the data content of the SMS isn't known by others. SMS conveyance framework for encoding messages into ciphertext utilizing a key that is placed by the shipper then, at that point, ships off the objective number. SMS gathering framework to unscramble it to others by means of SMS without the apprehension about data from these messages will be known by others. It utilizes normalized correspondence conventions that let cell phones trade short instant messages. Joined encryption has been proposed to authorize information classification while making information practical. It scrambles/decodes an information duplicate with a joined key, which is gotten by figuring the cryptographic hash worth of the substance of the information duplicate. After key age and information encryption, clients hold the keys and send the ciphertext to the beneficiary. The Messages conveyance server, and any individual or outsider who could get sufficiently close to information for messages and content sent between gadgets, will not have the option to peruse start to finish encoded messages since they don't have the key. The model is being created utilizing altered blowfish encryption and the code check is performed utilizing the MD5 hashing calculation.**

Keywords - Short Message Service, Encryption, MD5 hashing Algorithm.

I. INTRODUCTION

Electronic display devices such as tablets, eReaders, mobile phones, smart phones, personal digital assistants (PDAs), and other such touch screen electronic display devices are commonly used for displaying consumable content. The content may be, for example, an eBook, an online article or blog, images, a movie or video, a map, just to name a few types. Such display devices are also useful for displaying a user interface that allows a user to interact with an application running on the device. The user interface may include, for example, one or more touch screen controls and/or one or more displayed labels that correspond to nearby hardware buttons. Thus, and in accordance with an embodiment of the present invention, image pattern unlocking techniques are disclosed for use in electronic touch screen devices. In some embodiments, after an electronic device has been locked, placed into sleep or power-saving mode, or restarted, the user must first unlock the device before it can be used again. Such a locking function provides security, helping to prevent unauthorized use of the device. By implementing the image pattern unlocking techniques described herein, the user may further personalize the unlocking function. In one specific example, when a device is locked the device may display an unlock screen whenever a user indicates a desire to begin using the device.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

II. RELATED WORK

EXISTING SYSTEM

In this case, the screen displayed on the mobile phone changes from information related to the interrupted function to information related to the subsequent function. For example, when an incoming email or call is received while the user is browsing a website with an Internet connection (i.e. Internet connectivity being used), the conventional mobile phone switches the screen displayed from information related to the website to information notifying the user that a call or email has been received. For this reason, users are calling for information related to other functions to be displayed without interrupting display of information related to the current function.

In view of this, an object of the present invention is to provide a mobile phone and a display method capable of displaying video and other information in a user-friendly manner without interrupting video display, in the case where other information is displayed during the display of received video. The access may be restricted by requiring a user seeking access to draw a pattern on a display of the device, such as by drawing with their finger or a stylus across elements on a touch screen display in a connect-the-dots fashion.

Mobile Pattern, Fingerprint, Face Unlock, PIN and password are the available method to unlock the mobile. A mobile pattern is a grid of 3X3 cell, where drawing a specific pattern (connecting specific sequence of cells in order) will unlock the mobile. In some embodiments, the unlock mode can display an unlock screen to the user, prompting the user to arrange or create or otherwise select a specific image pattern in order to unlock the device.

Limitations:

The desired image pattern that will unlock the device may be configured by the user. The customizable image pattern may include any uniquely identifiable unlocking pattern including a single image or a combination of images. In some embodiments, the unlocking mechanism may include personalized images gathered from the user's photo collection and/or one or more social media profiles associated with the user (e.g., online services that employ user avatars or photos associated with each account) that the user of the locked device can recognize, and the unlock pattern could be a selection of such images. In other embodiments, a combination of color and images can also be used, such as matching colors to images. If a correct color-image pattern is arranged, the device is unlocked.

PROPOSED SYSTEM

A non-transient computer program product comprising a plurality of instructions encoded thereon that when executed by one or more processors cause a process to be carried out, the process comprising: display on the electronic device an unlock screen, wherein the unlock screen is configured to display a random image and prompt a user to input an unlock code; and unlock the electronic device in response to receiving the unlock code, the unlock code including a correct unlock screen input that corresponds to the random image, wherein the combination of the random image and the correct unlock screen input is pre-established and provides at least part of the unlock code.

The computer program product may include one or more computer readable mediums such as, for example, a hard drive, compact disk, memory stick, server, cache memory, register memory, random access memory, read only memory, flash memory, or any suitable non-transitory memory that is encoded with instructions that can be executed by one or more processors, or a plurality or combination of such memories. In this example embodiment, the process is configured to display on the electronic device an unlock screen, wherein the unlock screen prompts the user to input a unique image pattern. In some cases, the unique image pattern is user configurable. In some cases, a user inputting the unique image pattern includes the user selecting or arranging a plurality of images in a predetermined order.

Lock screen module displays a lock screen view on the mobile device to prevent unauthorized or inadvertent access to a mobile device. In that example, lock screen module may not accept any other input until a particular touch gesture input is received. Lock screen module may prevent unauthorized access to a user's personal data on a mobile device. In an example, the input may be a touch gesture that the user had pre-set for authentication purposes. In an example, touch receiver may receive touch input on a view (not shown) of mobile device. The touch input received may include a position that the user touched as defined by an X and Y coordinate on the screen. The screen may detect touches using any technology known in the art including, but not limited to, resistive, capacitive, infrared, surface acoustic wave, strain gauge, optical imaging, acoustic pulse recognition, frustrated total internal reflection, and diffused laser imaging technologies.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

Features:

According to this configuration, the mobile phone displays display information related to an incoming signal and video currently being displayed in different areas of the screen partitioned in two when incoming signal information or detection information is acquired, thereby enabling the display information to be notified to the user without interrupting video display on the screen. In some embodiments, an image pattern unlock screen may include various UI features including, for example, a number of image tiles that the user may select or drag into a certain order, a color palette for selecting a desired color, a number of color input areas where the user can paint or otherwise input a color pattern, and/or a drawing or inking input area for detecting words or images drawn on the touch screen device. Other image pattern unlocking features will be apparent in light of this disclosure, and some embodiments may include some or all of the features described above. In some embodiments, the user may interact with these various UI features using a finger, an active or passive stylus, or any other suitable implement. In one example embodiment, in order to unlock the device the user must create the appropriate image pattern on the unlock screen.

SOFTWARE DESCRIPTION

Front End: Java and XML

XML (Extensible Markup Language) is a very popular simple text-based language that can be used as a mode of communication between different applications. It is considered as a standard means to transport and store data. JAVA provides excellent support and a rich set of libraries to parse, modify or inquire XML documents. Basic XML concepts and the usage of various types of Java based XML parsers in a simple and intuitive way.

Back End: MS SQL

MS SQL Server is a relational database management system (RDBMS) developed by Microsoft. This product is built for the basic function of storing retrieving data as required by other applications. It can be run either on the same computer or on another across a network. Some basic and advanced concepts of SQL Server such as how to create and restore data, create login and backup, assign permissions, etc. Each topic is explained using examples for easy understanding.

III. SYSTEM DEVELOPMENT

Access to data included in the mobile device is permitted when the presence of an authentication device having the proper authentication information is received by the mobile device. Currently a variety of methods are used to protect data on such devices, most commonly the utilization of the entering of a password and/or the entering of a combination of user name and password. However, it has been shown that the use of a password and/or the inconvenience that a user must input a password each time the information is to be accessed has been shown to be undesirable.

PROPOSED WORK:

Creating The App Interface

Systems and methods for developing, customizing, and deploying mobile device applications are provided through a mobile application development and deployment platform. Preferably, these systems and methods are implemented in an Internet based environment that allows non-technical users to build sophisticated, highly-customizable cross-platform mobile applications. The platform allows users to select, input, create, customize, and combine various content, design characteristics, and application components, such as modules, some of which utilize features and functionality associated with various mobile devices and mobile operating systems. In certain embodiments, the platform allows users to compile, and generate a configuration file for, the mobile application that can be distributed to end users for execution on various mobile devices and mobile operating systems. When the mobile application is installed on, or executed by the mobile device, the configuration file may enable the retrieval of various data associated with the mobile application.

In order to encourage and facilitate the development of mobile apps for certain types of mobile operating systems and/or devices, the manufacturers and developers of these systems and devices frequently distribute software development kits (SDKs) that are associated with their devices and/or operating systems (or particular versions or releases thereof). While these SDKs assist with the development of mobile apps, in order to utilize these SDKs a significant degree of technical knowledge and expertise in software programming and mobile devices is typically required. In particular, use of these SDKs requires programmers to possess an understanding of and experience with both the programming language and the specific mobile operating system platform for which the application is being developed.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

Configure SMS Gateway

In addition to the challenges associated with building mobile apps, deploying these applications and distributing them to end users can often be a complex and involved process. In part, this is due to the fact that many of the mobile device and operating system manufacturers and developers require that all mobile apps to be used with their devices and operating systems must be distributed through their digital distribution platform (e.g., iOS's App Store, Android's Market, webOS's App Catalog).. As a result, an understanding of, and experience with, the requirements and restrictions imposed by manufacturers is often necessary in order to deploy and distribute applications to mobile device users successfully and efficiently.

Given the high level of skill and expertise needed to create, deploy and update mobile applications, many non-technical individuals, as well as individuals lacking experience in a particular programming language or mobile operating system or digital distribution platform, have are not able to develop and/or distribute mobile applications. Although there have been attempts to make mobile application development more accessible to a wider public through software systems that allow persons who do not have significant experience in programming or specific mobile operating system platforms to create mobile applications devices, these systems have exhibited a number of drawbacks and limitations which have resulted in their failure to be widely adopted by consumers.

Key Generation

The system is designed to create the dedicated key and shared key between the sender and receivers. The uploaded file content is encrypted using the shared public key. And receivers' device decrypts the data using private key. Elliptic curve key generation algorithm is used to generate the shared key between user. The file content is encrypted and decrypted using the shared key. Device ID and session information with plain text data of the video content are taken as input parameter and Dedicated key and Shared key is generated and the encrypted video content is transmitted between devices.

SMS Encryption and Transmission

Content based encryption is applied to encrypt the text data. The contents are subdivided into number of encodes for the Encode processing model. Encode based encryption with the handling of macro blocks of text data is applied by differentiating the encode type content. The system sub divides the macro block structure and to provide the ease of encryption modeling of text data. Text content in terms of content and encode content of text data are taken as input and the Encrypted text content with successful decryption are obtained as output and signature generated for validating the decryption of data.

Receive SMS and Decryption

The invention herein disclosed improves upon the scroll-like display of data on electronic display screens by making it possible for a user/viewer to access a desired portion of a long list of data and information by scrolling to the location of that portion rapidly and in a more natural manner than therefore possible. The present invention overcomes and avoids the limitations of known control systems for scrolling electronic displays by providing a touch-screen responsive system that imparts a scrolling motion to the displayed image in response to the motion of a finger in contact with the screen. After the finger separates from the screen, the image continues to move in the same direction at a gradually decreasing speed until motion is stopped manually by touching the screen without movement of the finger, or the speed decreases to zero, or to a predetermined minimum speed, or until the image reaches its "end". Alternatively, continued motion of the image may be achieved or again increased by repeating the "sweeping motion" of the user's finger along the screen. Still further, if the finger touch on the screen is made to move with the display, but at a slower rate than the then-current rate of movement, the display will be slowed to a rate corresponding to the motion of the finger at the movement that contact is broken.

This operation of the system of this invention is achieved by programming a microprocessor-based control system to displace the image on a screen display, such as the screen of a conventional cathode ray tube, in response to a finger touch on the screen and the direction of a finger motion along the surface of the screen at the initial speed of the finger motion. Thereafter, the speed of displacement is caused to decay at a selected rate (units of displacement per unit of time, or a function thereof), until the displacement finally stops (for example, due to having reached the end of the "scroll") or until it is stopped deliberately as explained herein. In accordance with this invention, the scrolling motion of data on the display screen moves in a seemingly "natural" way, moving initially at a speed imparted by the motion of the user's finger, with the speed thereafter slowing at a constant rate until it ultimately comes to rest, unless it is terminated earlier.

A mobile device includes a user interface that has a plurality of non-password-protected desktop screens and at least one

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

password protected desktop screen. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the scope of the invention. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

IV. TESTING METHODOLOGIES

Testing consists of activities that can be planned and is used to verify and validate the designed system. The various tests that are done to the system are tabulated. Testing is vital to the success of the system. System testing makes a logical assumption that if all the parts of the system are correct, the global will be successfully achieved. In adequate testing if not testing leads to errors that may not appear even many months.

This creates two problems,

1. The time lag between the cause and the appearance of the problem.

2. The effect of the system errors on the files and records within the system.

Unit Testing and Integration Testing

A small system error can conceivably explode into a much larger Problem. Effective testing early in the purpose translates directly into long term cost savings from a reduced number of errors. Another reason for system testing is its utility, as a user-oriented vehicle before implementation. The best programs are worthless if it produces the correct outputs. No other test can be more crucial. Unit testing is performed by the developer during the development cycle. Integration testing is a logical extension of unit testing.

Functional Testing

Functional testing of an application is used to prove the application delivers correct results, using enough inputs to give an adequate level of confidence that will work correctly for all sets of inputs. The functional testing will need to prove that the application works for each client type and that personalization function work correctly. When a program is tested, the actual output is compared with the expected output. When there is a discrepancy the sequence of instructions must be traced to determine the problem. The process is facilitated by breaking the program into self-contained portions, each of which can be checked at certain key points. The idea is to compare program values against desk-calculated values to isolate the problems.

Load Testing and Performance Testing

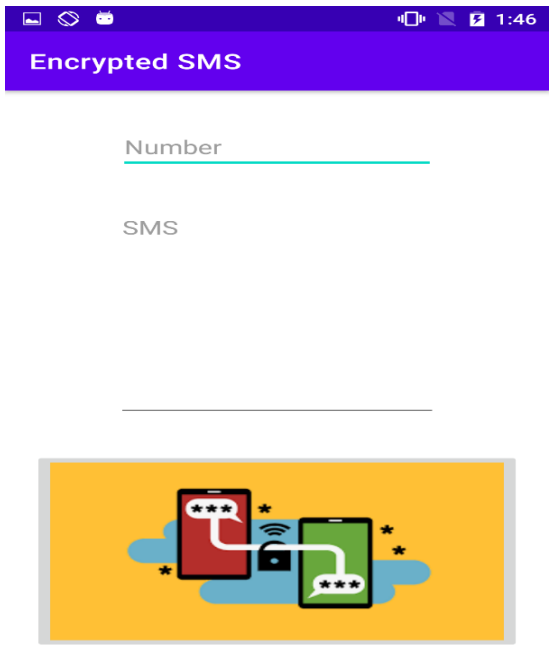
It is necessary to ascertain that the application behaves correctly under loads when 'Server busy' response is received in the load testing. Performance testing is required to assure that an application perforce adequately, having the capability to handle many images, delivering its results in the expected time and using an acceptable level of resource and it is an aspect of operations management. This is to check that the system is rugged and reliable and can handle the failure of any of the components involved in providing the application.

V. EXPERIMENTAL RESULTS

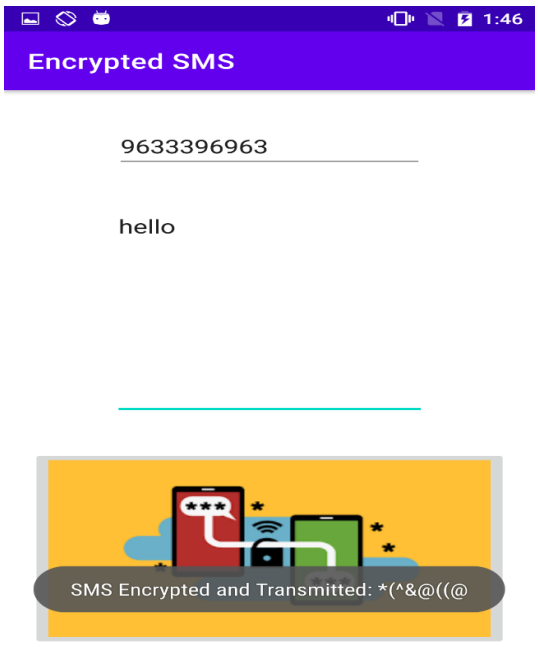
Home Screen

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

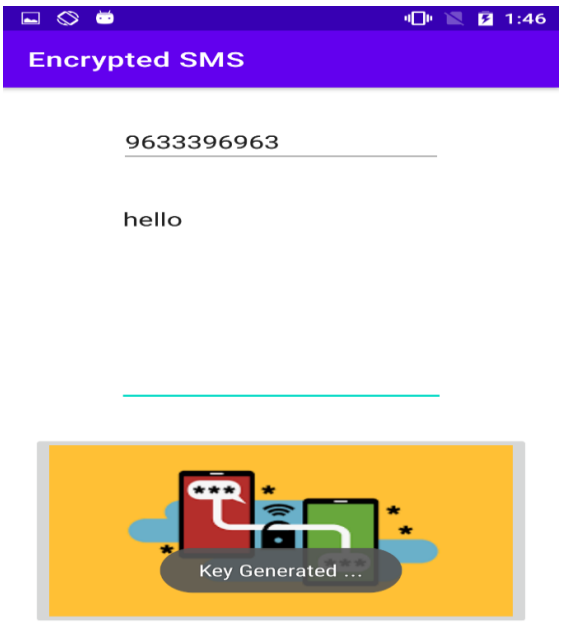
SMS Interface



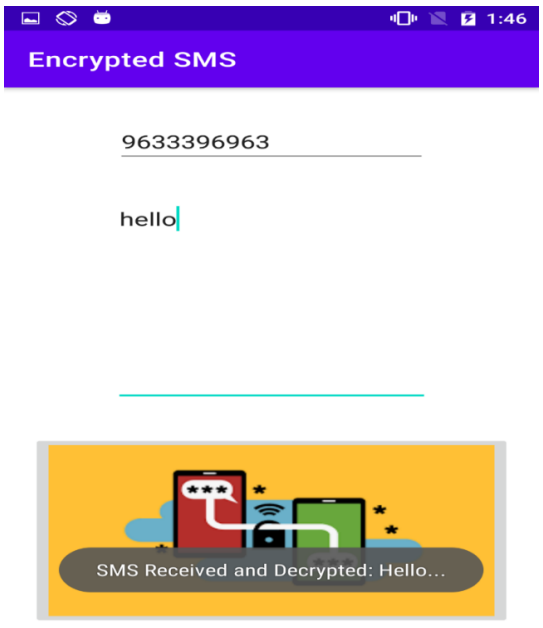
SMS Encryption and Transformation



Key Generation



SMS Decryption



International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 10, Issue 1, No 5, 2022 ISSN: 2348-6600
Reference ID: IJCS-407 PAGE NO: 2770-2776

VI. CONCLUSION

A mobile device comprising: a secure element; a touch sensitive display device that allows a user to navigate between desktop screens using swipe gestures. In this work an application is developed on the mobile phone to modify the SMS message into ciphertext so that the information content of the SMS is not known by others. SMS delivery system for encrypting messages into ciphertext using a key that is entered by the sender then sends to the destination number. SMS reception system to decrypt it to others via SMS without the fear of information from these messages will be known by others.

FUTURE WORK

While the mobile device is locked, a touch gesture having a pre-defined shape is detected on a touch screen of the mobile device independently of the initial position of the touch gesture on the touch screen. In this way, detection of the touch gesture causes the particular action to execute while keeping the mobile device locked. In future the scheme can be combined with the face recognition and fingerprint authentication. Using NFC, SmartTag is a small token that has read/write capabilities to/from the phone when it is in close proximity to the phone. This is convenient if there are multiple users or if the phone is used in different locations. When traveling abroad, one could easily use a SmartTag with a profile in which expensive roaming is disabled.

REFERENCES

[1] Ibrahim, N. and Sellahewa, H., "Touch gesture-based authentication: A security analysis of pattern unlock.", 2017, February.

[2] Hintze, D., Hintze, P., Findling, R.D. and Mayrhofer, R., "A large-scale, long-term analysis of mobile device usage characteristics.", 2017.

[3] Aviv, A.J., Maguire, J. and Prak, J.L., "Analyzing the impact of collection methods and demographics for android's pattern unlock.", 2016.

[4] Aviv, A.J. and Dürmuth, M., "A Survey of Collection Methods and Cross-Data SetComparison of Android Unlock Patterns.", 2018.

[5] Hintze, D., Findling, R.D., Scholz, S. and Mayrhofer, R., "Mobile device usage characteristics: The effect of context and form factor on locked and unlocked usage." 2014, December.

[6] Tsai, Y.C. and Yang, C.H., "Physical forensic acquisition and pattern unlock on Android smart phones." 2013.

[7] Marques, D., Guerreiro, T., Duarte, L. and Carriço, L., "Under the table: tap authentication for smartphones." 2013, September.

[8] Meng, W., Li, W., Wong, D.S. and Zhou, J., "TMGuard: a touch movement-based security mechanism for screen unlock patterns on smartphones." 2016, June.

[9] Findling, R.D., Muaaz, M., Hintze, D. and Mayrhofer, R., "Shakeunlock: Securely unlock mobile devices by shaking them together." 2014, December.

[10] Khare, S., "Finger gesture and pattern recognition-based device security system." 2015, March.