DS&AI 2023
DATA SCIENCE AND ARTIFICIAL INTELLIGENCE CONFERENCE 2023
1ST - 3RD FEBRUARY 2023

SECURE MESSAGING APPLICATION.

CHEROTICH VELORINE
MARTIN MURUTHI
CYNTHIA JEMUTAI

Sponsored by Artificial Intelligence Journal, Google TensorFlow

BACKGROUND

In this era of digital communication, messaging application has continued to dominate various communication platform. This has led to the need of considering maximum security on this applications. Most of the dominating apps have upheld data privacy by ensuring encryption on their servers. Though this is a good move, a gap exist. This is because interception of their communication can be easily decrypted as the devices in use have decryption key within their storage. Further users cannot be guaranteed of their data integrity. We will consider the following publication in our case:

Kenya at high risk of cyber-attacks.

This is was a publication by the star where various cases on cyber-attacks. Research has shown that 56 million cyber threats for the quarter ended December 2020 this is according to communication authority (ca) data. Further, web application attacks have been published to be 7.8 million.

End –to-end encryption becoming the norm for social media.

This was a publication that noted social media platform of not having strong grip on consumer privacy. The statement above was supported by the crisis of Edward and Cambridge analytical scandal. People were becoming skeptical on using social media. They therefore needed the assurance of their privacy hence realization that end-to-end encryption was the way to go.

The two publication are among publications that ensued the relevance of our application which provide maximum security through encryption as well as guarantee integrity of data through integrity checker.

PROBLEM

Current messaging application uses weak encryption method. This is vulnerable to attacks that could lead to privacy infringement. It is simple to bypass the encryption method as the encryption key on our applications are stored within the storage device. Encryption is further implemented in the server only. Users on the other end need to be keen enough much attention of user to avoid being shoulder surfed as their messages are usually in decrypted form. Therefore the weak and static encryption is alarming due to advanced cyber-attacks. Additionally the integrity of the messages we receive and we transmit cannot be accounted for as we do not have an integrated mechanism for that. Above gaps needed to be bridged.

STUDY / PROJECT OBJECTIVES

To develop a software that will ensure total encryption and decryption across all the message servers and hosting devices. This has been accomplished by;

1. Implementation of strong authentication mechanism.
2. Assurance of information privacy through unique and personalized Credentials.
3. Guarantee of data integrity through integrity-checker mechanism.

BACKGROUND LITERATURE

When examining previous research on encryption and decryption, we major our focus on the manner that was utilized to ensure that; privacy, non-repudiation, authorization and safety are upheld. Therefore we considered zhou, X., & Tang, X. (2011, august) who made a well-researched work on the same. In their publication, they acknowledged the key features that encryption and decryption has brought about. These include; information confidentiality, digital signature, authentication, secret sub-storage, system security, integrity of information and certainty, to prevent information from tampering, forgery and counterfeiting among other functions.

They further explained that encryption and decryption algorithm's security depends on the algorithm while the internal structure of the rigor of mathematics, it also depends on the key confidentiality**. Key in the encryption algorithm has a pivotal position, once the key was leaked, it means that anyone can be in the encryption system to encrypt and decrypt information, it means the encryption algorithm is useless.** And since they established that the encryption private key plays a critical role and its careless handling could mess up every effort, they suggested an implementation of a complete and practical RSA encrypt/decrypt solution based on the study of RSA public key algorithm. Though their proposal helps to solve problems like interception of messages on transit. User where not considered in the event that communication device get misplaced or even leave their devices unattended to. They can be exposed to a lot of attacks. Therefore our project aims to mitigate all that were left behind by embracing the current encryption and decryption methods along with adding new feature to ensure that all messaging platform are well covered. Our idea makes a tradeoff between security usability in the interest of minimally affecting the users' workflow and maintain universal accessibility.

METHODOLOGY

Knowledge from machine learning models and natural language processing techniques dominated the entire project e.g. Levenshtein distance and cosine similarity. They were used to ensure the integrity of the data. Our own encryption algorithms were used in conjunction with the cipher and pycrypto module in Python to provide intervallic encryption and decryption of messages. The use of the cipher and pycrypto modules helped ensure the robustness and effectiveness of the encryption and decryption processes. Additionally, techniques such as Levenshtein Distance and Cosine Similarity were used to ensure the integrity of the data. If the integrity of the data was compromised, the ML algorithm would raise a red flag. This combination of methods provided a highly secure means of communication for users of the application.

On initial usage of the application, users are required to verify their identity through either biometric features e.g. Fingerprint or by providing password/passcode before being able to view specific message. Once verified, the encrypted message displayed in the chat screen is decrypted and displayed in plain text for a period of 10 seconds before it is encrypted again. An algorithm also checks the integrity of the messages every 2 seconds to ensure that they have not been tampered with. Additionally, for additional security, the encryption key changes every 5 seconds.

RESULTS / OUTPUTS

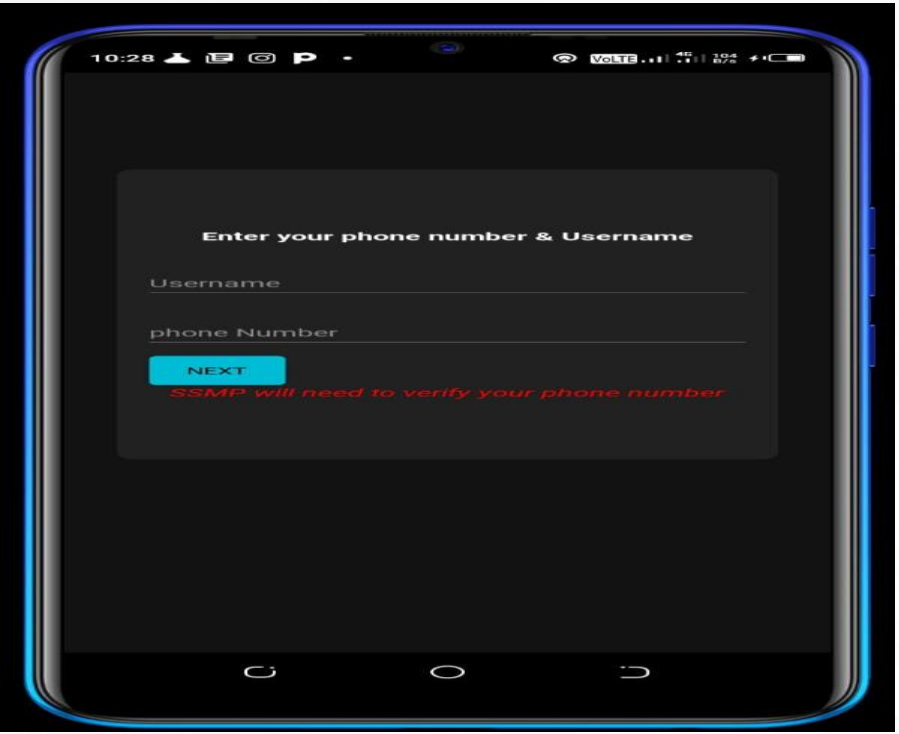
Our project yielded an application that is compatible with most of the operating systems; android, windows among others. On deployment, One is prompted to enter their registration details that is; username and the desired phone number. On clicking the registration section, the phone number initially entered is verified and a specific code is sent to it so as to facilitate successful registration. During the deployment of the app, the chats if any will by default be in encrypted form. Therefore to decrypt, encryption can be disabled in the settings. Further, the setting option provides a wide range of features. Among the features are; login function that apply both the passcode and fingerprint features also changing username and the login mechanism is provided in the settings. Among the most essential toolbars we have is key icon that on clicking on it, a user is prompted to choose a decryption mechanism they would prefer to use. This applies to either single message or entire chat. We also have integrity checker that is shown by the colors that constantly changes; blues is the standard color, green shows that the message is in its original form thus confirms that there was no interception, red signals that alteration was made while on transit.

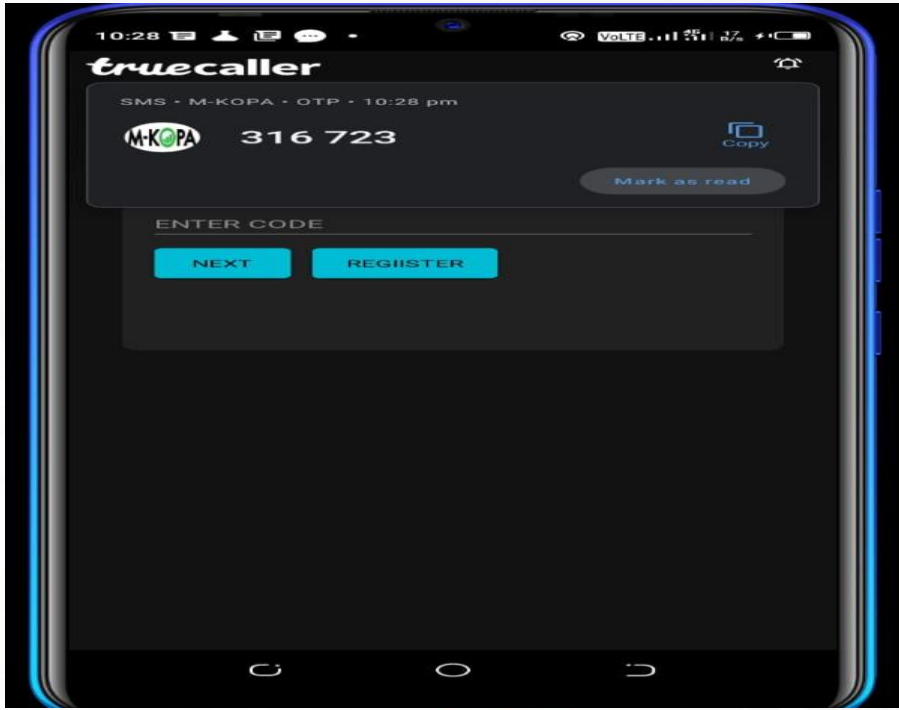
When a message is being send from say X to Y, the message is encrypted. Initial encryption key at the sending end is stored in the server. On the receiving end, the message will also be in encrypted form with a different key also stored in the server, to decrypt it, the server is prompted and it does the matching and decrypt it intelligently. Hence no one can tell the key for any message. This guarantees confidentiality has been upheld. About section gives briefing on what our application is all about. developer section tells more about each of us and our contributions to the entire application. The log out section does the existing function. Share provides an invitation to other users without the application. All these results are shown in the screenshots below:

DISCUSSION

1. **LOGIN/REGISTRATION -** This is first screen module to appear when the application is being deployed in users' device for the first time. The user is required to register by filling all the parameters. **For username and phone number is a must**
2. **VERIFICATION SECTION** - The modules verifies the user details e.g. Phone number. A 4 digit code is sent to the user's phone number to verify that he/she owns the phone number.
3. **MAINSCREEN MODULE** – This module ushers in entire modules that include the developer, setting, chat and contact section as will be shown below.

1 DISCUSSION

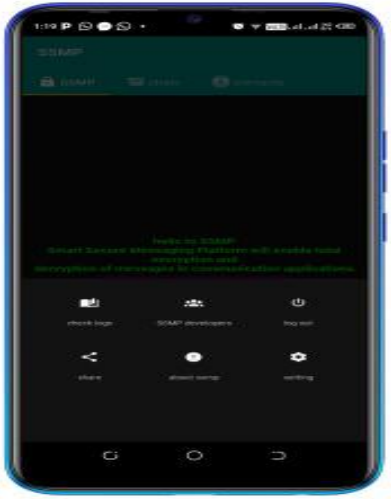




3.

MAIN SCREEN
This is the main screen after the user have logged in into the application.
The screen provide a user with an interface to navigate to different modules like developers module,setting,chats and contact module etc

Setting module

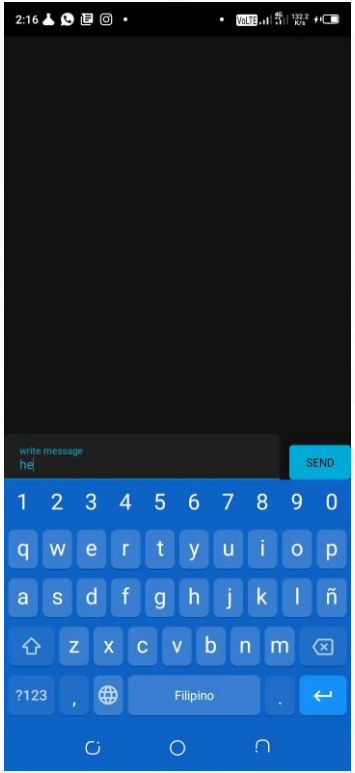


Main menu to access other Modules [check logs,ssmp devs,about ssmp,setting etc]

About Module

ENCRYPTION & DECRYPTION

INTEGRITY CHECKING



CONCLUSIONS AND FUTURE WORKS

The proposed messaging application addresses the security concerns related to data integrity, privacy and authentication mechanisms. We have solved the issues arising through; encryption that utilizes machine learning and natural language processing algorithm. These implemented security measures provide a secure communication experience for users and can be used as a starting point for further research and development in the field.

THANK YOU!