FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 8 No. 2, April, 2024, pp 46 - 58
DOI: https://doi.org/10.33003/fjs-2024-0802-2339

BANKS SHORT MESSAGE SERVICE THREATS NOTIFICATION SYSTEM ON ANDROID BASED PHONE

***Muhammad, Ishaq Umar, Muhammad Mukhtar Liman, Joshua Abah, Timothy Moses and J. Agushaka**

Department of Computer Science, Faculty of Computing, Federal University of Lafia, Nigeria

*Corresponding authors' email: muhammadishaqumar@gmail.com

ABSTRACT

This research is carried out for the development and implementation of an end-to-end encrypted Short Message Service (SMS) App, utilizing a hybrid cipher algorithm, driven by the notable insecurity observed in SMS communications on mobile devices. SMS is a widely used communication method, and the primary goal of this study is to create a system (App) for end-to-end encrypted SMS. Loss of phones is becoming vulnerable for threats, because we store vital records in android and these records are secret such that no other third party is required to see them, such as Bank SMS, Event Notification etc. Also this information can be compromised if android phone is been lost and found by the criminals. Kidnapping activity is serious case happening in northern part of Nigeria, so if a phone is being lost and discovered how financed he is (the device holder), there is any means of bank account compromisation as that would allow the bank to give some information about the account because of the registered SIM card inserted in android devices (phones). This system is aimed to secure Bank SMS by not allowing an unauthorized person to views the banks SMS, but all other SMS can be view. Whenever the Banks SMS is received by the Android phone, the system will encrypt it and can only be viewed if using correct decryption key, a notification will be sent to the owner other phone if more than two attempt to view the message is made, using a Hybrid Cipher Algorithm on the Android Operating System. Hybrid encryption is an approach that combines both asymmetric and symmetric encryption methods, leveraging the advantages of each to enhance overall encryption effectiveness. The study discusses various encryption algorithms and relies on secondary sources for collecting pertinent data. In this research, three methodological approaches are used: Structured System Analysis Design Methodology (SSADM), Object Oriented Analysis Design Methodology (OOADM), and prototyping. The application of three cryptographic algorithms—Message Digest 5 (MD5), Blowfish, and Rivest-Shamir-Adleman (RSA)—ensures integrity, confidentiality, authentication, and security of the messages. The encryption provided by the developed application is designed to be resistant to brute force attacks. The implementation of this system is carried out using the Java programming language. To achieve this aim, we deployed the Java cipher-cryptography algorithm.

Keywords: Android Device, Bank SMS, Authentication, Notification, Security

INTRODUCTION

In the contemporary era, where technology is rapidly evolving, and digital transactions have become the norm, the importance of secure communication channels, particularly in the banking sector, is paramount (Sandhu & Arora, 2022). The integration of Short Message Service (SMS) into banking systems has provided customers with unparalleled convenience and flexibility, but it has also introduced new vulnerabilities and security challenges (Raharja & Ashari, 2021).

The ubiquity of mobile phones, especially Android devices, has led to their widespread use in various domains, including banking (Ferm & Thaichon, 2021). Traditionally, banks have used SMS for notifications, transaction alerts, one-time passwords (OTPs), and other critical communications (Agwanyanjaba, 2020). However, the SMS protocol, inherently, was not designed with strong security features, making it susceptible to various forms of attack such as interception, eavesdropping, and SMS phishing (Priya et al., 2023).

As cyber threats evolve and become more sophisticated, the need for more secure SMS communication systems becomes urgent (Kim et al., 2023). The vulnerabilities in the current SMS-based banking communications can lead to significant risks, including financial fraud, identity theft, and unauthorized access to sensitive banking information (Menard & Bott, 2020). Therefore, enhancing the security of SMS communication for banking purposes is not just a matter of protecting individual users, but it's also crucial for maintaining the integrity and trustworthiness of the banking system as a whole (Raharja & Ashari, 2021).

This paper explores the design and implementation of a cutting-edge system tailored for securing bank SMS on Android platforms. By amalgamating advancements in mobile technology with state-of-the-art security protocols, this system aims to fortify the traditional SMS channel against potential vulnerabilities and threats. Through the integration of encryption, authentication, and other security mechanisms, the proposed system strives to establish a robust defense against unauthorized access and interception of sensitive banking information transmitted via SMS.

Furthermore, this research builds upon existing literature, drawing insights from seminal works such as (Ekwonwune & Enyinnaya, 2020) and (Raharja & Ashari, 2021), which emphasize the critical importance of fortifying SMS-based banking services. These works underscore the vulnerabilities inherent in conventional SMS communication and advocate for the implementation of innovative security measures to protect against evolving cyber threats. The new system works; it will not just encrypt the entire SMS but only a function of the SMS (Banks SMS), it allows all other messages to be viewed but encrypt Banks SMS unlike how the conventional system does, and will send notification if an attempt to view Bank SMS on the device is done; and this can be done if more than one attempts is done.

As we delve into the intricacies of the proposed system, it is essential to consider the dynamic landscape of mobile banking, where user experience and security must strike a delicate balance. Through a comprehensive examination of existing security frameworks and a critical analysis of their efficacy, this research aims to contribute valuable insights towards the development of a robust, user-friendly, and secure system for bank SMS on Android-based phones.

In summary, the development of a Secured Bank SMS System for Android-based phones is a critical step towards fortifying the security of mobile banking communications. By addressing the vulnerabilities inherent in traditional SMS, this system not only protects users against emerging cyber threats but also strengthens the overall trust in digital banking services. As we move forward, the adoption and continual enhancement of such security measures will be essential in navigating the evolving landscape of digital banking and communication technology.

Literature review

(Rihan et al., 2019) conduct an investigation into the Comparative Performance of Cryptographic Algorithms. In their examination, they evaluated the efficiency of established cryptographic techniques such as RSA, AES, Blowfish, DES, Elliptic Curve, MD5, SHA, and RSA algorithms. Their experimental findings confirmed that the MD5 algorithm has the shortest encryption time, whereas RSA has the longest encryption time. Additionally, they discovered that the decryption process of the Blowfish algorithm surpasses that of other algorithms. Notably, hashing-based algorithms do not necessitate decryption.

(Sagheer et al., 2019) designed a model to ensure confidentiality and integrity of SMS data by utilizing a hybrid cryptographic approach. This approach melds the Advanced Encryption Standard (AES) for encryption and decryption tasks with the RC4 algorithm for key expansion and generation, aiming to bolster security significantly. The model was developed using the Java programming language, specifically on the NetBeans platform. To validate its effectiveness, their system underwent testing on various mobile devices, including the Nokia 5233. The outcomes were promising, with each process completing in under a second. The swift performance, coupled with effective mobile compatibility, positions their system favorably when compared to existing solutions in the field.

As a means of curbing cybercriminals from pilfering transaction details, (Fletcher, 2019) suggests implementing a system wherein transaction information is encrypted, allowing access only to those possessing the appropriate decryption key. Their study was accomplished through the use of the ECC (Elliptic Curve Cryptography) asymmetric algorithm, involving the exchange of public keys between the bank and the customer. The data is subsequently encrypted using both the public key and private key. In this process, the customer receives a QR code containing the encrypted transaction details. To decrypt and view the information, an Android application scans the QR code. Notably, the generation of asymmetric keys is facilitated by the ECDSA (Elliptic Curve Digital Signature Algorithm), and both encryption and decryption follow the ECIES (Elliptic Curve Integrated Encryption Scheme) standard. This approach ensures a secure and efficient method for safeguarding transaction details from unauthorized access.

(Salim et al., 2019) In their research, a secure system for mobile banking was developed, comprising three main components: the client-side (associated with the bank), the server, and the application running on a mobile device. The model employed the proposed Elliptic Curve Integrated Encryption Schema (ECIES) for securely exchanging confidential data between the client (the mobile application) and the server. The ECIES implementation utilized the Elliptic-curve Diffie–Hellman (ECDH) as the key agreement algorithm, the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) known as AES-GCM for encryption, and the MAC-384 as the Message Authentication Code (MAC) function. Additionally, hash functions (SHA512 and SHA384) were applied in the key derivation process. Moreover, the proposed system incorporated a secondary password authentication step when conducting a money transfer transaction.

A study conducted by (Garba, 2019) aimed to develop a messaging application that balances optimal functionality and code processing speed, along with the capacity for rapid architectural improvements without incurring significant resource costs. The initial version of this messenger included essential features like registration, account login, user online status checking, messaging, and hash encoding for secure internet communication. The findings demonstrated a notable potential for enhancing the application's architecture in any segment of the code while maintaining minimal impact on its other functions. This resulted in a more stable performance compared to messengers developed using Android or JavaScript frameworks. However, achieving a higher code processing speed, in comparison with other Android or web-based applications, was a challenge. To address this, a specific method was designed and implemented to boost the processing speed of the code. This new approach showed significant improvements in processing speeds for the messenger, making it more efficient compared to other Android or web-based messaging systems.

(Yusuf et al., 2019) conduct a study to enhance the authentication processes used in mobile devices. The proposed authentication system integrates both fingerprint and facial recognition methods to verify the user of the mobile device. Access to the device is contingent upon the successful verification through both these methods. The process initiates with fingerprint authentication, followed by facial recognition. If either of these methods is unsuccessful, the device remains inaccessible. It is important to note that the facial recognition component depends on a connection to Microsoft's servers.

(Ekwonwune & Enyinnaya, 2020) Conduct a study to develop an Android-based software application that provides end-to-end encryption for SMS messages. This application utilizes a Hybrid Cipher Algorithm, which combines the strengths of both asymmetric and symmetric encryption, to secure messages during transmission between mobile devices. The study explores various encryption techniques, drawing on secondary data sources for information. To achieve this, the research employs three distinct methodologies: Structured System Analysis Design Methodology (SSADM), Object-Oriented Analysis Design Methodology (OOADM), and prototyping. The security features of the application are bolstered by the integration of three cryptographic algorithms: Message Digest 5 (MD5), Blowfish, and Rivest-Shamir Adleman (RSA). These algorithms ensure the integrity, confidentiality, authentication, and overall security of the messages. Moreover, the application is designed to be resistant to brute force attacks. The development of this software involved programming in Java.

A study conducted by (Grandis & Yunanto, 2020) focuses on creating a mobile banking system that incorporates Near Field Communication (NFC) for client authentication and security. This system enables various banking functions such as checking account balances, viewing transaction history, transferring money within the same bank and to other banks associated with ATM Bersama, and paying electricity bills.

The system is developed using the Java programming language, with Android Studio as the development tool. For server access, PHP is used alongside MySQL for database management, with IdWebHost providing hosting services. Data output is formatted using JSON. Data for the study is gathered through interviews and literature reviews. The development approach is based on the Rapid Application Development (RAD) methodology. The system's effectiveness is evaluated through unit testing and user acceptance testing. The final outcome is a secure mobile banking application that employs NFC technology, PIN verification, and AES encryption for enhanced security.

(Mabruri, 2020) carried out a study focused on the application of a dynamic AES algorithm featuring an S-BOX in an Android messenger chat application. This application was developed using Java and utilized a hierarchical database structure for storing data. The outcomes of the study showed that the algorithm was effective, successfully encrypting and decrypting messages. The research stands out for its adaptability, demonstrating potential for application across a variety of file formats, including but not limited to text messages, documents, images, and videos. Additionally, the study proposes a noteworthy suggestion for future research endeavors: the integration of the AES algorithm with other cryptographic algorithms, aiming to bolster encryption security across diverse types of files.

(Otor et al., 2020) designed and simulated an enhanced security model for USSD in banking operations within Nigeria. The existing USSD platform's security was bolstered by introducing a secret question as an additional authentication layer, aimed at reducing the risk of identity theft. During new account openings, customers register a secret question with the bank, while existing customers update their details in the bank's database before enrolling in USSD services. This process mirrors the way customers verify their ATM PIN in the bank, ensuring that only the customer knows the answer. The model was implemented using PHP on the XAMPP platform and simulated using the Hubtel USSD mocker. Results demonstrated that the proposed system's security was strengthened with the introduction of an additional layer of authentication through the secret question.

The study was conducted by (Chin et al., 2020) aim to develop a messaging application that balances optimal functionality and code processing speed, along with the capacity for rapid architectural improvements without incurring significant resource costs. The initial version of this messenger included essential features like registration, account login, user online status checking, messaging, and hash encoding for secure internet communication. The findings demonstrated a notable potential for enhancing the application's architecture in any segment of the code while maintaining minimal impact on its other functions. This resulted in a more stable performance compared to messengers developed using Android or JavaScript frameworks. However, achieving a higher code processing speed, in comparison with other Android or web-based applications, was a challenge. To address this, a specific method was designed and implemented to boost the processing speed of the code. This new approach showed significant improvements in processing speeds for the messenger, making it more efficient compared to other Android or web-based messaging systems.

(Bekkem Sumanth Reddy, 2021) In their research on Secure End-to-End Encrypted SMS System, the author introduces a model that enables the sender to encrypt messages before they are transmitted via the internet. This encryption process utilizes the Advanced Encryption Standard (AES) as its cryptographic algorithm. The application designed in this study allows the user to input a key and a message they wish to encrypt. Consequently, this results in the generation of encrypted messages that can be decrypted and read by the recipient. The encryption method, specifically the use of AES in the application, ensures that the encrypted texts are resistant to Brute-Force attacks, thereby enhancing the security of the messages sent.

(Logunleko et al., 2021) develop a model that provides a platform-agnostic solution for secure money transfers, employing data masking and an advanced base64 algorithm to move funds between accounts. The study enhances current financial transaction systems by creating a secure mobile money transfer system. It protects financial details through encryption and masking, both within the mobile app and in the SMS notifications (Text Message Notification) sent to users. This approach significantly reduces the likelihood of third-party interception and comprehension of sensitive financial information.

(Lei et al., 2021) conduct a comprehensive and first-of-its-kind study focusing on how malicious local applications can illicitly access SMS OTP (one-time password) messages on contemporary mobile operating systems. Their investigation reveals several new attack vectors, primarily emerging from mechanisms originally designed to enhance the usability and security of SMS-based authentication. Ironically, these mechanisms have inadvertently opened up new avenues for attacks. To gauge the real-world implications of these vulnerabilities, there engaged in both user studies and an extensive analysis involving 140,586 applications. This extensive survey uncovered 36 apps, collectively installed by hundreds of millions of users, that are susceptible to these newly identified attacks. Notable among these vulnerable applications are widely used messaging platforms like Telegram and KakaoTalk.

(Raharja & Ashari, 2021) Conduct a study on SMS Banking security protocol, the research runs through two steps. The first step is the transmission of the transaction request, and the second step is the transaction process. The encipherment is conducted using 3DES symmetric cryptography. Digital signature and data integrity are conducted using ECDSA asymmetric cryptography. The key exchange is conducted using ECDH. The test result showed that the implementation of the protocol could conduct an SMS Banking service and provide protection over the PIN. In general, this protocol has fulfilled X.800 security services.

(Enyinnaya et al., 2021) conduct a study to explores the implementation of end-to-end encrypted Short Message Service (SMS) through the utilization of a hybrid encryption algorithm. In this secure SMS system, messages undergo encryption during their transmission between devices, and only the intended recipient's device can decipher the unreadable message using a secret key. Hybrid encryption, involving the integration of two or more encryption systems, is employed to enhance security. The research employs Structured System Analysis and Design Methodology (SSADM) and Object-Oriented Analysis and Design Methodology (OOADM) as the chosen methodologies. The use of Rivest-Shamir Adleman (RSA) and Data Encryption Standard (DES) Algorithm ensures the achievement of message integrity, confidentiality, authentication, and overall security. The software development process is executed using the Java programming language.

A study conducted by (Sari et al., 2022) on cryptographic algorithms for an SMS security system on Android. The study compared three cryptographic algorithms: AES (Advanced Encryption Standard), RSA (Rivest Shamir Adleman), and

TEA (Tiny Encryption Algorithm). The aim was to identify the algorithm that provides better security for an Android-based SMS security system. According to the findings of the study, TEA (Tiny Encryption Algorithm) was determined to be the best algorithm for this specific application. Without the details of the study or the specific characteristics compared, it's challenging to delve deeper into the reasons why TEA was considered the most suitable choice. However, TEA is known for its simplicity and efficiency in resource-constrained environments, making it potentially suitable for mobile devices like Android smartphones. It's a symmetric key block cipher with a focus on simplicity and speed, and it is often used in applications where code size and processing power are critical factors.

(Onuwabhagbe OGBEIDE et al., 2023) conduct a study to explore the extent of security awareness among users of mobile banking applications and whether this awareness translated into improved security measures. One key aspect investigated was the security risk associated with users granting access to third parties. The survey results indicated a limited level of security awareness, with only 14.4% of respondents acknowledging security as a significant consideration. This underscores a general lack of awareness among users, with 58.2% expressing serious concerns about their privacy, particularly in relation to the risky behavior of granting access to third parties. The study further highlighted that a majority of users perceived current security measures in mobile banking as inadequate. To analyze the collected data, the research employed an empirical survey with quantitative descriptive analysis. The primary data collection tool was a structured questionnaire, and the Statistical Package for Social Science (SPSS) was used to code and analyze the data.

(Akande et al., 2023) introduces a mobile application designed to identify and thwart smishing attacks through a rule-based SMS service. The mobile application is equipped with a feature that intercepts incoming SMS messages to the smartphone. These intercepted messages are subsequently sent via an Application Programming Interface (API) to a rule-based machine learning model. This model employs meticulously chosen rules to assess the content of the received message, determining whether it is spam or legitimate (ham). The analysis results are relayed back to the mobile application through the API. Importantly, the user is given the final decision-making authority on whether to keep or discard the identified spam or legitimate message after receiving a notification.

A Comparative Study of Cryptographic Algorithms was conducted by (Thabit et al., 2023), to evaluated the effectiveness of various cryptographic methods, including RSA, AES, Blowfish, DES, Elliptic Curve Cryptography, MD5, and SHA. The findings revealed that among these, the MD5 algorithm required the least time for encryption, whereas RSA had the longest encryption time. Additionally, it was discovered that the Blowfish algorithm outperforms others in terms of decryption efficiency. It was also noted that hashing-based algorithms, like MD5 and SHA, do not necessitate decryption.

(Scholar & RGMCET, 2023) Introduced is a novel Secure SMS Messaging Protocol (SSMS) designed for M-payment. Functioning as an application layer protocol, it is specifically crafted for GSM users, serving as a secure conduit within the M-payment system. The protocol adopts an elliptic curve-based public key solution, employing the public key as the secret key for symmetric encryption. Furthermore, distinct keys are utilized for both encryption and decryption processes.

Table 1: Related review work

Authors	Algorithm	Findings	Tools Used	Limitations
(Grandis & Yunanto, 2020)	AES Encryption	Robust text security; efficient performance	Android Studio, Java	Key management complexity; potential processing overhead
Enyinnaya et al., (2021)	RSA Encryption	High security for key exchange	Android Studio, OpenSSL	Slower compared to symmetric algorithms; larger key sizes
Lei et al., (2021)	2FA (OTP)	Effective access authentication	Google Authenticator, SMS APIs	Dependency on user's phone; potential for OTP interception
Salim et al., (2019)	HMAC (HOTP)	Strong authentication for transactions	Java, SMS APIs	Less user-friendly; synchronization issues
Fletcher, (2019)	ECC	Excellent security with faster performance	Bouncy Castle, Java	Implementation complexity; less common
Otor et al., (2020)	Blockchain	Tamper-proof transaction records	Ethereum Platform, Solidity	Scalability issues; high computational and energy requirements
Rihan et al., (2019)	Machine Learning	Effective fraud detection	Python, TensorFlow	High false positives; requires extensive training data
Chin et al.,(2020)	Biometric (Fingerprint)	High user convenience; difficult to spoof	Android Biometric APIs	Hardware dependency; vulnerability to spoofing
Thabit et al., (2023),	SSL/TLS	Secure data transmission standard	OpenSSL, Android Networking Libraries	Vulnerability to certain attacks; requires proper certificate management

Authors	Algorithm	Findings	Tools Used	Limitations
Yusuf et al., (2019)	TOTP	Time-based access authentication	Java, Android SDK	Time synchronization issues; user action required
Sari et al.,(2022)	SMS Encryption with Hashing	Enhanced SMS security	Java, Android SDK	Slightly slower due to hashing; potential for replay attacks
Raharja & Ashari, (2021)	Digital Certificates	Trusted identity assurance	OpenSSL, Java	Complex certificate management; cost
Bekkem Sumanth Reddy, (2021)	End-to-End Encryption (E2EE)	Ensures privacy of message content	Signal Protocol, Java	Complexity; reliance on user's security practices

Problems Statement

The current SMS-based banking services accessible on Android platforms face susceptibility to a range of security risks (Kalipi, 2023). Unauthorized interception of SMS messages, unauthorized access to user information, and manipulation of transaction data by hackers pose significant threats, potentially resulting in financial losses for customers (Vishnuvardhan et al., 2020). The absence of a strong security mechanism emphasizes the need to confront these vulnerabilities. In the realm of mobile banking, the reliance on Short Message Service (SMS) for critical communications such as transaction notifications, account alerts, and One-Time Passwords (OTPs) is widespread (Prince et al., 2023). While SMS offers convenience and accessibility, its integration into the banking sector has exposed several significant security vulnerabilities, particularly in the context of Android-based smartphones, which hold a substantial share of the global mobile market.

The fundamental design of the SMS protocol lacks robust end-to-end encryption, making it susceptible to interception and unauthorized access. This vulnerability is particularly concerning for sensitive banking information transmitted over SMS, There is also a growing trend in SMS phishing (smishing) attacks, where fraudsters impersonate banks to trick customers into revealing sensitive information. The existing SMS infrastructure offers limited authentication mechanisms to counter such threats. Many banking SMS systems do not integrate 2FA, relying solely on the security of the SMS itself, which is no longer sufficient in the current cyber threat landscape. Consequently, the objectives of this study is to create a system that offers a secure SMS banking service on Android phones by encrypting Bank SMS to cipher-text and decrypted to normal text when using correct key. This system aims to mitigate prevailing security issues, guaranteeing the privacy and integrity of user information.

MATERIALS AND METHODS

Analysis of the System

System overview

The recommended system is a smooth safety system with verification for safety to encrypt Banks SMS with GSM alert report for threats notification. It drive function as a means for providing safety to our Bank Short Message Service on Android based phone. The work also recommends observing issues that have a progressive impact on encryption of Bank SMS, this effort entails of a microcontroller that will be used to stimulate a signal and send reports via text messages to the Android device owner. This safety encryption system uses the keypad that allows users to enter a code on a keypad to encrypt as the best certification tool as shown in a Front-end design block App in Figure 1.0 below. It also works as both smart and wireless approaches foe safety of the systems to provide an improved system with better safety features.

Figure 1: The recommended system diagram.
Source: (Design by the authors)

Design Algorithm

Algorithm is the finite sequence of solving a well-defined problem; in this work we proposed the algorithm below;

Step1: StartStep 2: Enter (Input Password)
Step 3: Confirm the Chiper-text using MD5 algorithm
Step 4: Compare with SQLite Database
Step 5: If yes Login Successful, Else Login Fail and Generate a Message
Step 6: Compare the Hash Code with the user details
Step 7: If code match then login successful, else send alert to the Device holder
Step 8: Stop

System Description

Various approaches of designing an android based safety system are observed, in this work password is deployed in other to decrypts the Banks Short Message Service. The system is model sensibly to report the crime attempts in real-time. The system is designed into two module of functions, where each module in the diagram represent a section of the circuit to conveys a specific function; Encryption Section and Decryption Section as shown in Figure 2 below.

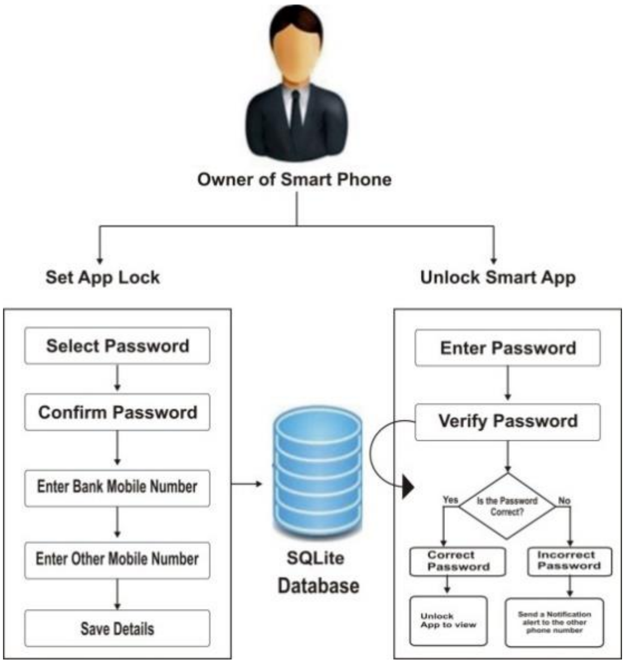


Figure 2: The system model

The architecture presents the procedure for setting of encrypting/decrypting the Bank SMS. All the specifications must be certain; like password, contact numbers, etc., are stored in SQLite database which must be verified through the App while encrypting the Banks Short Message Service, these details are verified from SQLite database and if the password is correct then BSMS will be decrypted and the user can view it. If the password is incorrect, then report will be sent to the device owner through his other phone number that is recorded by the App, further procedure is explained in workflow given in section 4 (figure 10). If user fails to decrypt the App to view the Bank SMS within three attempts then the report will be sent to the device owner and further action can be carryout, this can be done, using random number selection.

System Flow Chart

The system flow-chart diagram shown in Figure 3. Section 1; The incoming message sent by Bank (encrypted) through the SIM to which the message will be received and the device make (Android), if the device make is android, the message; to verify whether the message is from Bank or not, if the message is from bank it will encrypt and requires to be authenticate. Section 2; for the authorized person who has a valid password, the user will input password, is password correct? The system will check for the password authenticity if valid it will decrypt otherwise remains encrypted, after three unsuccessful trials, the system will send a crime attempt SMS to the owner through is secondary mobile number as shown in fig. 2 above.

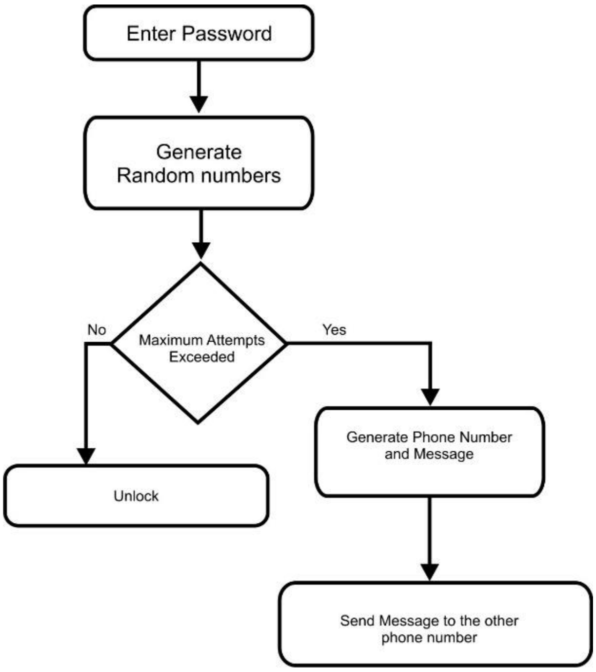

Enter Password
Generate Random numbers
Maximum Attempts Exceeded
No
Yes
Unlock
Generate Phone Number and Message
Send Message to the other phone number

Figure 3: The Flowchart of the system

Setup and Analysis of the proposed system

In this section, the user is required to download the new secure Bank SMS App (Proposed), so during installations, the terms and procedure for setup is mandatory. Since we are using tools to execute parameters, the installations must appreciate both of them sequentially. The procedure are as follows;-

i. Download prerequisites packages via the command line (Google Playstore).
ii. During installation, type-in the password.
iii. Verification of the Password; this is done by SQlite database and store.
iv. Scan; which will take some time.
v. Give the phone number of your choice.
vi. Give the second phone number for the threads report.
vii. Confirm and save.

Password Authentication

When the user opens the app, the prompt page appears for user to access by a password for authentication which ensures that unauthorized access is denied. When the user enters the right password, only then the app gives the access for decryption to the Bank Message enabling feature. Whereas if wrong password is entered, an error message will generate, if more than two attempts are made, threats notification will be sent to the device owner via his second line.

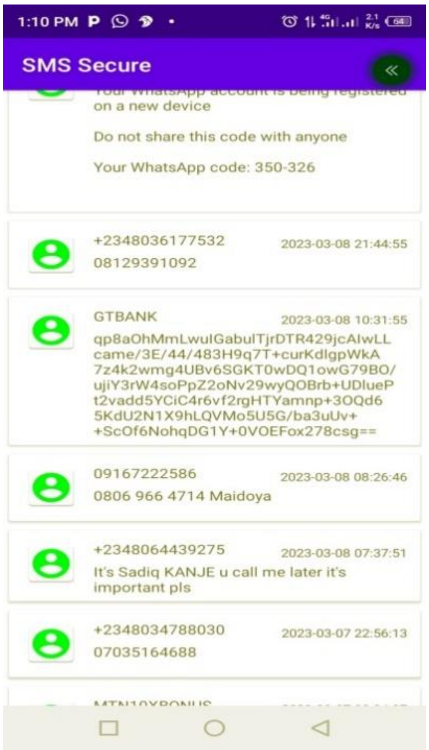
RESULTS AND DISCUSSION

The system model in fig. 2 is aimed at bringing solutions to threats on android based devices and the objectives are the tools that are used to driven the processes for the achievement of the anticipating result. See figure 1 above.

Figure 4: This Figure showed the screen of an android phone, indicating a hand locating the message App to view Messages.

Figure 5: This figure shown, indicate the various messages (Inbox, Sent Message, Draft Box, etc) after the message App is selected and type-on.

After launching the message App, having displayed various segments (Inbox, Sent Message, Draft Box, etc), all messages can be view but a bank Messages are encrypted, and shall always require password before one can be able decrypts to view the message. See the figure 6 below.



Your WhatsApp account is being registered on a new device

Do not share this code with anyone

Your WhatsApp code: 350-326

+2348036177532 2023-03-08 21:44:55
08129391092

GTBANK 2023-03-08 10:31:55
qp8aOhMmLwulGabulTjrDTR429jcAlwLL
came/3E/44/483H9q7T+curKdlgpWkA
7z4k2wmg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+UDlueP
t2vadd5YCiC4r6vf2rgHTYamnp+3OQd6
5KdU2N1X9hLQVMo5U5G/ba3uUv+
+ScOf6NohqDG1Y+0VOEFox278csg==

09167222586 2023-03-08 08:26:46
0806 966 4714 Maidoya

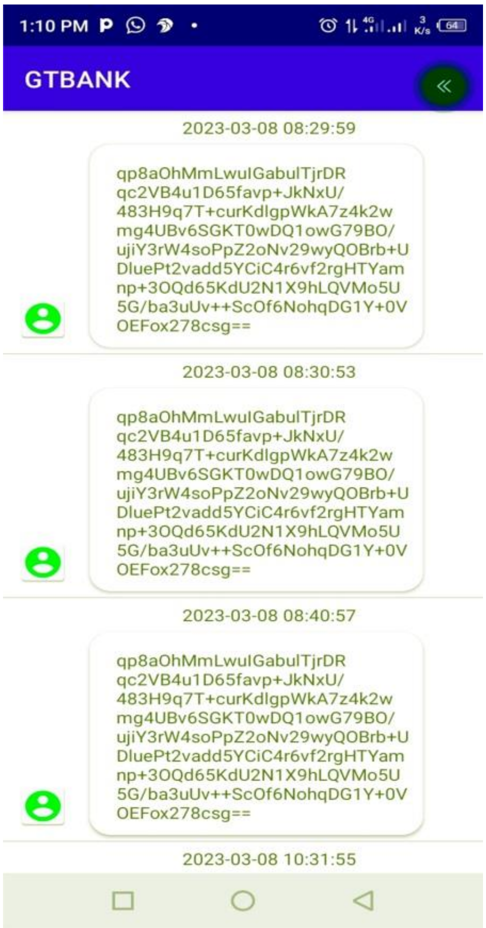
+2348064439275 2023-03-08 07:37:51
It's Sadiq KANJE u call me later it's important pls

+2348034788030 2023-03-07 22:56:13
07035164688

MTN10XBONUS

Figure 6: Displayed Message indicating Bank SMS encrypted

Figure 6: showed all the messages contains on the device, but indicating Banks SMS encrypted, if a person click on the Banks SMS, it will be presented as indicated in the fig. 7 below.



2023-03-08 08:29:59

qp8aOhMmLwulGabulTjrDR
qc2VB4u1D65favp+JkNxU/
483H9q7T+curKdlgpWkA7z4k2w
mg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+U
DluePt2vadd5YCiC4r6vf2rgHTYam
np+3OQd65KdU2N1X9hLQVMo5U
5G/ba3uUv++ScOf6NohqDG1Y+0V
OEFox278csg==

2023-03-08 08:30:53

qp8aOhMmLwulGabulTjrDR
qc2VB4u1D65favp+JkNxU/
483H9q7T+curKdlgpWkA7z4k2w
mg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+U
DluePt2vadd5YCiC4r6vf2rgHTYam
np+3OQd65KdU2N1X9hLQVMo5U
5G/ba3uUv++ScOf6NohqDG1Y+0V
OEFox278csg==

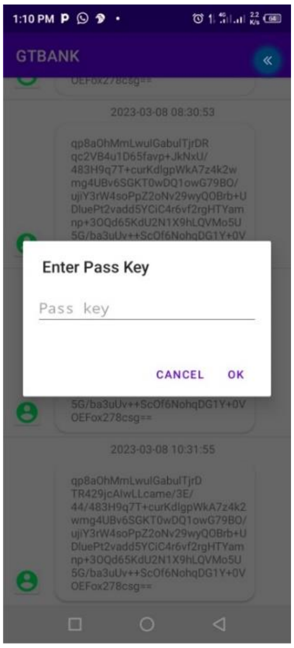
2023-03-08 08:40:57

qp8aOhMmLwulGabulTjrDR
qc2VB4u1D65favp+JkNxU/
483H9q7T+curKdlgpWkA7z4k2w
mg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+U
DluePt2vadd5YCiC4r6vf2rgHTYam
np+3OQd65KdU2N1X9hLQVMo5U
5G/ba3uUv++ScOf6NohqDG1Y+0V
OEFox278csg==

2023-03-08 10:31:55

Figure 7: Showing encrypted Banks SMS

Only an authorized person can decrypt the SMS by having password for authorization, as at when the person strike-on the banks Message the dialog box display, requesting the person to put-in decryption key before the access shall be granted see fig. 8 below.



OEFox278csg==

2023-03-08 08:30:53

qp8aOhMmLwulGabulTjrDR
qc2VB4u1D65favp+JkNxU/
483H9q7T+curKdlgpWkA7z4k2w
mg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+U
DluePt2vadd5YCiC4r6vf2rgHTYam
np+3OQd65KdU2N1X9hLQVMo5U
5G/ba3uUv++ScOf6NohqDG1Y+0V

Enter Pass Key

Pass key

CANCEL OK

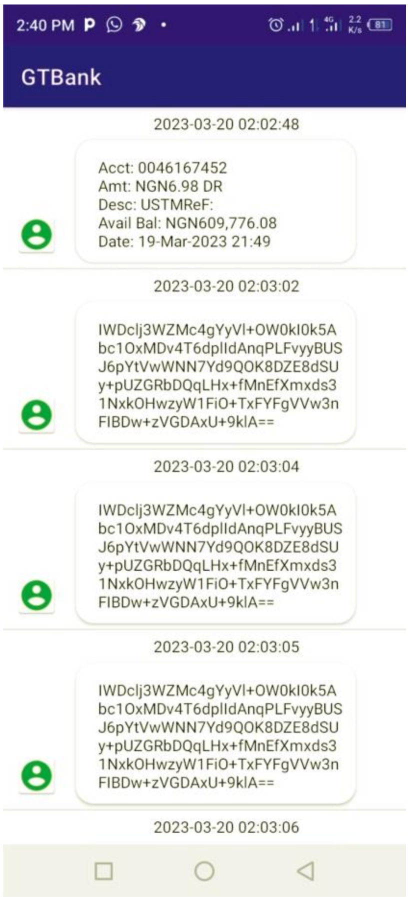
5G/ba3uUv++ScOf6NohqDG1Y+0V
OEFox278csg==

2023-03-08 10:31:55

qp8aOhMmLwulGabulTjrD
TR429jcAlwLLcame/3E/
44/483H9q7T+curKdlgpWkA7z4k2
wmg4UBv6SGKT0wDQ1owG79BO/
ujiY3rW4soPpZ2oNv29wyQOBrb+U
DluePt2vadd5YCiC4r6vf2rgHTYam
np+3OQd65KdU2N1X9hLQVMo5U
5G/ba3uUv++ScOf6NohqDG1Y+0V
OEFox278csg==

Figure 8: Authentication phase

Hence, if the attempt to decrypt the message is done successful with the right decryption key, the Bank SMS shall decrypted, see fig 9 below.



2023-03-20 02:02:48

Acct: 0046167452
Amt: NGN6.98 DR
Desc: USTMReF:
Avail Bal: NGN609,776.08
Date: 19-Mar-2023 21:49

2023-03-20 02:03:02

```
IWDclj3WZMc4gYyVl+OW0kI0k5A
bc1OxMDv4T6dplIdAnqPLFvyyBUS
J6pYtVwWNN7Yd9QOK8DZE8dSU
y+pUZGRbDQqLHx+fMnEfXmxds3
1NxkOHwzyW1FiO+TxFYFgVVw3n
FIBDw+zVGDAxU+9kIA==
```

2023-03-20 02:03:04

```
IWDclj3WZMc4gYyVl+OW0kI0k5A
bc1OxMDv4T6dplIdAnqPLFvyyBUS
J6pYtVwWNN7Yd9QOK8DZE8dSU
y+pUZGRbDQqLHx+fMnEfXmxds3
1NxkOHwzyW1FiO+TxFYFgVVw3n
FIBDw+zVGDAxU+9kIA==
```

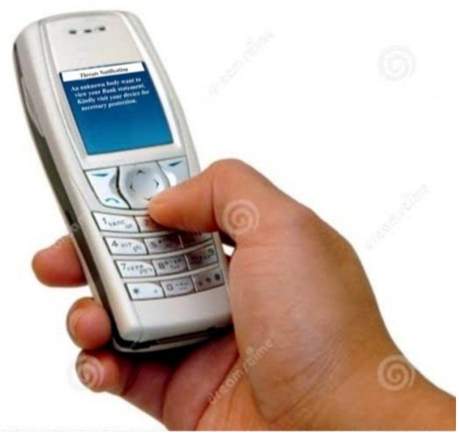
2023-03-20 02:03:05

```
IWDclj3WZMc4gYyVl+OW0kI0k5A
bc1OxMDv4T6dplIdAnqPLFvyyBUS
J6pYtVwWNN7Yd9QOK8DZE8dSU
y+pUZGRbDQqLHx+fMnEfXmxds3
1NxkOHwzyW1FiO+TxFYFgVVw3n
FIBDw+zVGDAxU+9kIA==
```

2023-03-20 02:03:06

Figure 9: Showing decrypted Bank SMS

And if attempts of more than two times are done, the system sends the threat notification through the other cell phone number for immediate respond. See the figure 10 below.



Threats Notification

An unknown body want to view your Bank statement. Kindly visit your device for necessary protection.

Figure 10: Threats notification

The figure above indicated that, the other cell phone number received the threats notification via the attempt made by the unknown body to view the Banks SMS alert on the android phone device.

Discussion

The recommended policy for Banks Short Message Service on Android based safety system App with keypads lock and GSM alert report system. This App system also ensures that the device owner get reports in the form of text messages (TM) from the Android Device by the system (App) after certain conditions are met.

- The Banks SMS: this is the subject matter of threads, where the problem is identified, and the system is design to protect the Bank alert received by android based phone from the view of third party.

- Authentication: this is done by the back-end process, to synchronize and ensure the correctness and uniqueness of the password to enable access or denial of access at wrong password.
- Notification: this phase is the point at which the message of crime reports is sent by the device owner for immediate action after more than three wrong attempts were made.

Scope

This work incorporates on Android platform. So, it can be used on some device which runs on Android operating system. This application can be used in companies for securing data transfer. The purpose of this application is to secured data transfer between Bank and Customer (the devices holder).

Operational principles

This proposed effort; it comprises modules as shown in Figure 1 and Figure 2. The operation of each of these modules is described below;

- Select Password Module: this will allows the user to put random numbers of choice for locking and unlocking.
- Confirm Password: this Module will enable the system to verify whether the above random numbers are the same as the recent for synchronization.
- Bank Mobile Number (Alert Line): this is the receiving alert-number for which the bank sends transaction notification and also keeps track of customer records.
- Other Mobile Number: this is the secondary number which the system sent notification on crime attempts to the device owner.
- Save Details: this is the phase or module for which the information given is stored in the database.
- Enter Password: this module is for selected random numbers entry for unlocking the system.
- Verify Password: in this module, the password is checked to ensure the correctness of the password for authentication.
- Encrypt/Decrypt: This phase is achieved after a successful password is log in; it is the module that determines reliability of the password to grant access (means allow access to the user or denial of access after password is log in).
- Send Notification: This module will send a report to the device owner for any wrong attempts to the system for action and will not allow the user to access the Bank SMS and view.

CONCLUSION

The android based system is widely in use today, more are been produced daily with different modifications, there is a high demand for the android security with the best features. This work incorporates a Bank Short Message Service secure-App on android based phone; this system is developed to carry out the functions discussed in segments of this work above. However, there are some limitations to others Make of phones; Apple, Symbian etc., these other aspects of phone makes is recommended for further research.

RECOMMENDATIONS

i. Upon reviews, we recommend that Android users should embrace the security awareness at all the time.
ii. Researchers should look into this proposed security model and make more research for other phone make (Apple, etc.) jh

REFERENCES

Abah, J. (2022). *Mobile Security: A Review 1*. *6*(1), 601004.

Abiodun, M. K., Imoize, A. L., Awotunde, J. B., Lee, C.-C., Adeniyi, A. E., Chioma, U., & Li10, C.-T. (2023). Analysis of a Double-stage Encryption Scheme Using Hybrid Cryptography to Enhance Data Security in Cloud Computing Systems. *Journal of Library and Information Studies*, *21*(2), 1–26.

Agwanyanjaba, W. O. (2020). *Enhanced Mobile Banking Security: Implementing Transaction Authorization Mechanism Via USSD Push.* University of Nairobi.

Ahmad, Z., Ong, T. S., Gan, Y. W., Liew, T. H., & Norhashim, M. (2022). Predictors of Employees' Mobile Security Practice: An Analysis of Personal and Work-Related Variables. *Applied Sciences (Switzerland)*, *12*(9). https://doi.org/10.3390/app12094198

Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O., & Fatokun, A. (2023). SMSPROTECT: An automatic smishing detection mobile application. *ICT Express*, *9*(2), 168–176.

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Abdelhag, M. (2018). Mobile Cloud Computing: Challenges and Future Research Directions. *Proceedings - International Conference on Developments in ESystems Engineering, DeSE*, *February 2018*, 62–67. https://doi.org/10.1109/DeSE.2017.21

Almomani, I. M., & Khayer, A. Al. (2020). A Comprehensive Analysis of the Android Permissions System. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.3041432

Alsaffar, M., Aljaloud, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Almurayziq, T. S., Alshammari, G., & Alshammari, A. (2022). Detection of Web Cross-Site Scripting (XSS) Attacks. *Electronics (Switzerland)*, *11*(14), 1–13. https://doi.org/10.3390/electronics11142212

Altulaihan, E., & Almaiah, M. A. (2022). *Cybersecurity Threats , Countermeasures and Mitigation Techniques on the IoT : Future Research Directions*. 1–41.

Anmulwar, S., Srivastava, S., Mahajan, S. P., Gupta, A. K., & Kumar, V. (2019). Rogue access point detection methods: A review. *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*, *July 2018*. https://doi.org/10.1109/ICICES.2014.7034106

Aqel, M. J., Naqshbandi, O. A., Sokiyna, M., & Valentyn, P. (2020). *Messaging System Design Based on Using Servers and Encoding System*. *14*(10), 107–127.

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*(February 2019), 55–69. https://doi.org/10.1016/j.tele.2019.03.003

Bekkem Sumanth Reddy, M. S. P. H. S. S. K. (2021). IRJET-Android based Secure End to End Encrypted SMS System. *Irjet*, *8*(4), 2982–2988.

Bongard-Blanchy, K., Sterckx, J. L., Rossi, A., Distler, V., Rivas, S., & Koenig, V. (2022). An (Un)Necessary Evil - Users' (Un)Certainty about Smartphone App Permissions and Implications for Privacy Engineering. *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022*, 173–180. https://doi.org/10.1109/EuroSPW55150.2022.00023

Callanan, C. (2021). *User tolerance of privacy abuse on mobile Internet and the country level of development*. *September 2019*. https://doi.org/10.1177/0266666915571171

Chin, Amita; Jones, Beth; Little, P. (2021). *A Comparative Analysis of Smartphone Security Behaviors and Practices Amita Chin Virginia Commonwealth University , United States Beth Jones Western Carolina University , United States Philip Little*. *17*(3), 57–80.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2020). Measuring user confidence in smartphone security and privacy. *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*, *1*. https://doi.org/10.1145/2335356.2335358

Ciaramitaro, B., & Pavlov, V. (2011). Mobile security. In *Mobile Technology Consumption: Opportunities and Challenges*. https://doi.org/10.4018/978-1-61350-150-4.ch013

David-West, O., Oni, O., & Ashiru, F. (2022). Diffusion of innovations: Mobile money utility and financial inclusion in Nigeria. Insights from agents and unbanked poor end users. *Information Systems Frontiers*, *24*(6), 1753–1773.

Ekwonwune, E. N., & Enyinnaya, V. C. (2020). Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm. *Journal of Software Engineering and Applications*, *13*(03), 25–40. https://doi.org/10.4236/jsea.2020.133003

Elueze, C. N., & Obasi, C. U. (2022). *5G and The Industry: A Case of the Nigerian Financial Technology Sector*.

Elvira Cruz, I. (2023). *Design of a methodology for the selection of mobile payment technologies in developing countries*.

Enyinnaya, V. C., Ekwonwune, E. N., Osuagwu, O. E., Agbakuru, A. O., & Amanze, B. C. (2021). *Applications of End-to-End Encrypted Short Message Service (SMS) using Hybrid Encryption Algorithm*. *12*(6), 176–181.

Evans. (2018). Improved financial performance without improved operational efficiency: The case of Nigerian firms. *Forum Scientiae Oeconomia*, *6*, 25.

Ferm, L.-E. C., & Thaichon, P. (2021). Customer pre-participatory social media drivers and their influence on attitudinal loyalty within the retail banking industry: A multi-group analysis utilizing social exchange theory. *Journal of Retailing and Consumer Services*, *61*, 102584.

Fletcher, B. (2019). *Application using ECC algorithm and QR.pdf*.

Frik, A., Kim, J., Sanchez, J. R., & Ma, J. (2022). *Users ' Expectations About and Use of Smartphone Privacy and Security Settings*.

Garba, F. A. (2019). TextFort: An Efficient Hybrid Short Message Service Encryption Scheme for Mobile Devices. *Scientific and Practical Cyber Security Journal*.

Ghadirli, H. M., Nodehi, A., & Enayatifar, R. (2019). An overview of encryption algorithms in color images. *Signal Processing*, *164*(September 2018), 163–185. https://doi.org/10.1016/j.sigpro.2019.06.010

Grandis, mohamad regiana, & Yunanto, R. (2020). Jurnal Teknik Informatika, Vol. 12, No. 2, April 2020. *Jurnal Teknik Informatika*, *12*(2), 46–51. https://www.researchgate.net/profile/Rio-Yunanto/publication/344596492_Perancangan_Sistem_Informasi_Iuran_Bulanan_Santri_Pada_Pondok_Pesantren_Sukamiskin_Bandung_Berbasis_Mobile_Web/links/5f832989299bf1b53e1e3d5d/Perancangan-Sistem-Informasi-Iuran-Bulanan

Gupta, B. B., & Narayan, S. (2020). A survey on contactless smart cards and payment system: Technologies, policies, attacks and countermeasures. *Journal of Global Information Management (JGIM)*, *28*(4), 135–159.

Hatamian, M., Wairimu, S., Momen, N., & Fritsch, L. (2021). A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. In *Empirical Software Engineering* (Vol. 26, Issue 3). Empirical Software Engineering. https://doi.org/10.1007/s10664-020-09934-4

Jameaba, M.-S. (2022). *Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Industry and Beyond*.

Kalipi, A. (2023). *Exploring the awareness of security threats associated with short-message service (sms) and protective measures against sms security threats amongst students at the University of Namibia (UNAM)*. University of Namibia.

Kim, Y., Oh, T., & Kim, J. (2023). Analyzing User Awareness of Privacy Data Leak in Mobile Applications. *Mobile Information Systems*. https://doi.org/10.1155/2015/369489

Krupp, B., Sridhar, N., & Zhao, W. (2017). SPE: Security and Privacy Enhancement Framework for Mobile Devices. *IEEE Transactions on Dependable and Secure Computing*, *14*(4), 433–446. https://doi.org/10.1109/TDSC.2015.2465965

Lei, Z., Nan, Y., Fratantonio, Y., & Bianchi, A. (2021). *On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices*. *February*. https://doi.org/10.14722/ndss.2021.24212

Liu, E., Rao, S., Havron, S., Ho, G., Savage, S., Voelker, G. M., & McCoy, D. (2023). No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. *Proceedings on Privacy Enhancing Technologies*, *2023*(1), 207–224. https://doi.org/10.56553/popets-2023-0013

Logunleko, A. M., Logunleko, K. B., Lawal, O. O., Ezugwu, O. O. D., & Akinyemi, O. S. (2021). A Secured Mobile Money Transaction Using Data Masking and Enhanced Base64 Algorithm. *Int. J. Recent Contributions Eng. Sci. IT*, *9*(1), 17–32.

Ma, S., & Chen, C. (2023). Are digital natives overconfident in their privacy literacy? Discrepancy between self-assessed and actual privacy literacy, and their impacts on privacy protection behavior. *Frontiers in Psychology*, *14*(June 2022), 1–11. https://doi.org/10.3389/fpsyg.2023.1224168

Mabruri, A. S. (2020). *Data Security System of Text Messaging Based on Android Mobile Devices Using Advanced Encrytion Standard Dynamic*. *October 2000*, 39–46.

Menard, P., & Bott, G. J. (2020). Analyzing IOT users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers and Security*, *95*, 101856. https://doi.org/10.1016/j.cose.2020.101856

Mousavi, S. K., Ghaffari, A., Besharat, S., & Afshari, H. (2021). Security of internet of things based on cryptographic algorithms: a survey. *Wireless Networks*, *27*, 1515–1555.

Noviandy, T. R., Idroes, G. M., Maulana, A., Hardi, I., Ringga, E. S., & Idroes, R. (2023). Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques. *Indatu Journal of Management and Accounting*, *1*(1), 29–35.

Omolara, A. E., Jantan, A., Abiodun, O. I., Dada, K. V., Arshad, H., & Emmanuel, E. (2019). A deception model robust to eavesdropping over communication for social network systems. *IEEE Access*, *7*, 100881–100898.

Onuwabhagbe OGBEIDE, V., OMOROGIUWA, O., & Eturpa SALAMI, E. (2023). an Empirical Survey To Substantiate the Need for a Cyber Security Framework for Smes in Nigeria. *International Journal of Research Publications*, *128*(1), 9–24. https://doi.org/10.47119/ijrp1001281720235221

Otor, S. U., Akumba, B. O., Idikwu, J. S., & Achika, I. P. (2020). An Improved Security Model for Nigerian Unstructured Supplementary Services Data Mobile Banking Platform. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *6*(3), 974–987.

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. *World Bank*, *54*.

Prince, C., Omrani, N., Maalaoui, A., Dabic, M., & Kraus, S. (2023). Are We Living in Surveillance Societies and Is Privacy an Illusion? An Empirical Study on Privacy Literacy and Privacy Concerns. *IEEE Transactions on Engineering Management*, *70*, 3553–3570. https://doi.org/10.1109/TEM.2021.3092702

Priya, D., Reddi, T., Reddy, M. S. T., Khan, M. K., & others. (2023). A Comprehensive Examination of Email Spoofing: Issues and Prospects for Email Security. *Computers \& Security*, 103600.

Radhi, S. M., & Ogla, R. (2023). In-Depth Assessment of Cryptographic Algorithms Namely DES, 3DES, AES, RSA, and Blowfish. *Iraqi Journal of Computers, Communications, Control and Systems Engineering*, *23*(3), 125–138.

Raharja, I. M. S., & Ashari, A. (2021). Enhancing Security System of Short Message Service for Banking Transaction. *International Journal of Computing*, *20*(1), 31–38. https://doi.org/10.47839/ijc.20.1.2089

Rahim Soomro, T., & Irshad, S. (2018). Identity Theft and Social Media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1), 43. https://www.researchgate.net/publication/323185128

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five two-factor authentication methods. *Proceedings of the 15th Symposium on Usable Privacy and Security, SOUPS 2019*, 357–370.

Rihan, S. D., Khalid, A., Eldin, S., & Osman, F. (2019). A Performance Comparison of Encryption Algorithms AES and DES. *International Journal of Engineering Research & Technology (IJERT)*, *4*(12), 151–154. www.ijert.org

Sagheer, A. M., Abdulhameed, A. A., & Abduljabbar, M. A. (2019). SMS security for smartphone. *Proceedings - 2013 6th International Conference on Developments in ESystems Engineering, DeSE 2013*, *February 2015*, 281–285. https://doi.org/10.1109/DeSE.2013.57

Salim, A., Sagheer, A. M., & Yaseen, L. (2019). Design and Implementation of a Secure Mobile Banking System Based on Elliptic Curve Integrated Encryption Schema. *International Conference on Applied Computing to Support Industry: Innovation and Technology*, 424–438.

Sandhu, S., & Arora, S. (2022). Customers' usage behaviour of e-banking services: Interplay of electronic banking and traditional banking. *International Journal of Finance \& Economics*, *27*(2), 2169–2181.

Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Review : Algoritma Kriptografi Sistem Keamanan SMS di Android. *Journal of Information Technology*, *2*(1), 11–15. https://doi.org/10.46229/jifotech.v2i1.292

Scholar, M. T., & RGMCET, N. (2023). *Easy and Secure Smart SMS Protocol on M-Health Environment in Mobile Computing*.

Shen, B., Wei, L., Xiang, C., Wu, Y., Shen, M., Zhou, Y., & Jin, X. (2021). Can systems explain permissions better? Understanding users' misperceptions under smartphone runtime permission model. *Proceedings of the 30th USENIX Security Symposium*, 751–768.

Shuba, A., Bakopoulou, E., & Markopoulou, A. (2018). Privacy Leak Classification on Mobile Devices. *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC*, *2018-June*(i). https://doi.org/10.1109/SPAWC.2018.8445948

Sitkowski, M., & Simulation, D. (2018). *Securely Encrypting Data At Rest*. *February*.

Souppaya, M., & Scarfone, K. (2023). Guidelines for Managing the Security of Mobile Devices in the Enterprise. *NIST Special Publication 800-124, Revision 1*, 1–30.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf%5Cnpapers3://publication/doi/10.6028/NIST.SP.800-124r1

Stirparo, P. (2015). *MobiLeak : security and privacy of personal data in mobile applications*.

Thabit, F., Can, O., Wani, R. U. Z., Qasem, M. A., Thorat, S. B., & Alkhzaimi, H. A. (2023). Data security techniques in cloud computing based on machine learning algorithms and cryptographic algorithms: Lightweight algorithms and genetics algorithms. *Concurrency and Computation: Practice and Experience*, e7691.

Ullah, I., Boreli, R., & Kanhere, S. S. (2023). Privacy in targeted advertising on mobile devices : a survey. *International Journal of Information Security*, *22*(3), 647–678. https://doi.org/10.1007/s10207-022-00655-x

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2016). On the Security and Privacy of Internet of Things Architectures and Systems. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 49–57. https://doi.org/10.1109/SIOT.2015.9

Visconti, A. (2018). *The Dangers of Rooting : Data Leakage Detection in*. *2018*.

Vishnuvardhan, B., Manjula, B., & Lakshman Naik, R. (2020). A study of digital banking: Security issues and challenges. *Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018*, 163–185.

Wang, C., Wang, Y., Chen, Y., Liu, H., & Liu, J. (2020). User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*, *170*, 107118. https://doi.org/10.1016/j.comnet.2020.107118

Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., Haq, M. A., Alhussen, A., & Alharby, S. (2022). Malware Analysis in IoT & Android Systems with Defensive Mechanism. *Electronics (Switzerland)*, *11*(15), 1–20. https://doi.org/10.3390/electronics11152354

Yusuf, M., Gimba, U. A., Bello, A. U., Adamu, A. H., Salisu, S., State, J., & Science, C. (2019). *Two Way Authentication for Android Mobile Phones*. *5*(1), 179–186.

.