**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# A SECURE GSM-BASED SMS BANKING SYSTEM: ANALYSIS, DESIGN, AND IMPLEMENTATION

**Zahraa Ibrahim kadhim sultan**

Middle Technical University ,Institute of Administration Rusafa-Baghdad

zahraa_ibrahim@mtu.edu.iq

## Abstract

Mobile banking has now become a critical platform of financial access, particularly in areas where smartphone and internet access are still low. Nevertheless, conventional SMS based banking is plagued by serious security failures such as plaintext transport, GSM cryptographic defects, SIM-SWO, and message disclosure within the SMSC. This puts a critical requirement of a superior, safe and dependable SMS banking application that has the ability to run on simple mobile phones. In this work, the author suggests the analysis, design, and implementation of a secure SMS-based banking system with a layered cryptographic model. The modelling technique is a mixture of the MERISE modelling approach and a hybrid framework of security, which is founded on RSA session initiation, SHA-derived session keys, and AES-256 message confidentiality. The implementation of the system utilised an SMS gateway and a SQL-based back end to facilitate common banking operations. Experimental findings show proper functional operation of all services, the average round-trip time of SMS is 712 seconds and consistent behaviour in the case of network congestion as a result of GSM store-and-forward reliability. Resistance to interception as well as spoofing, replay and SIM SWAP attacks is verified through security evaluation. In general, the results indicate that secure and efficient SMS banking can be realized and can offer an inclusive solution to the financial requirements of a mobile internet environment, where mobile internet services are not always reliable or accessible.

**Keywords**: Secure SMS Banking, GSM Vulnerabilities, End-to-End Encryption, Mobile Financial Services, MERISE System Modeling.

## 1. Introduction

Mobile telecommunications and GSM networks have now become mainstream in personal communication, and SMS is proving to be one of the strongest and most ubiquitous services in the exchange of short text messages. SMS commercial launch began in the early 1990s and nowadays maintains billions of messages daily internationally. Due to its simplicity, cheap nature and the ability to use simple smartphones, SMS has been embraced in most value-added services, such as e-government, notifications, alerts, and mobile banking. SMS based service usage in the banking industry enables customers to view their account balance, transaction notifications, and, in certain implementations, perform simple operations like transfers or payments through one or two simple text commands. To a great number of

Received: August 08, 2025

Volume 38 No.12s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

customers, particularly in areas with a poor or slow Internet connection, SMS banking is better than web banking since only a GSM handset and a mobile subscription are required.

Despite popularity, standard SMS has several security weaknesses:

- The mobile station (MS) communicates with the Short Message Service Centre (SMSC) through the transmission of messages as plain text.
- Only the radio connection between the MS and the base station is encrypted with GSM (A5/1, A5/2, A5/3), and does not ensure end-to-end implementation.
- SMSs could be intercepted, stored and sent to intermediaries (e.g., SMSCs and network operators).
- -Eavesdropping, spoofing, and unauthorized access by attackers can be done, which is unacceptable when the messages contain account numbers, balances, PINs, or transaction instructions.

Those that operate SMS to carry out sensitive operations thus put their clients at risk of confidentiality and integrity unless an extra security measure is enforced. The existing GSM security mechanisms cannot be considered good enough to get an end-to-end secure communication. The main objectives of this work are:

- Examine the security characteristics and attacks of GSM/SMS concerning mobile banking.
- Develop a safe SMS-banking design that is implemented on a wear application-layer cryptographic (public-key and symmetric encryption, hash-based session keys).
- Develop the banking system with the MERISE methodology to come up with uniform conceptual, logical and physical model data.
- Install a test version of an SMS based banking system, complete modules (account, customer, credit, payment, withdrawal, users, messaging) are built in with secure SMS processing.

The following contributions are made in this paper, based on the MSc thesis:

- In-depth discussion on the security levels of the GSM/SMS, such as A5 encryption, IMSI/IMEI-based authentication, and vulnerabilities that are well known in the SMSC processing and GSM ciphers.
- A secure SMS-banking architecture which makes use of: RSA public key cryptography of initial safe key exchange, AES as the symmetric encryption key of messages, and SHA hashing session keys based on user credentials (PIN, Salt, username).
- A system model (based on MERISE) including context diagrams, conceptual data model, logical data model, and physical data model, based on the SMS banking operations.

The rest of this paper will be structured in the following way: Section 2 will be a review of SMS technology, GSM architecture, SMS security issues, and secure SMS and mobile

Received: August 08, 2025

Volume 38 No.12s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

banking solutions. Section 3 provides the methodology of the research, the MERISE-based modelling, system architecture and cryptographic model along with straightforward mathematical formulas. Section 4 explains how the SMS banking application will be implemented and the key functional modules of the application, giving an account of the advantages and disadvantages of the methodology. Section 5 is the conclusion of the paper and provides directions for future work.

## 2. Literature Review

### a. SMS and GSM Network Architecture

It consists of a GSM network made of the mobile station (MS), base transceiver station (BTS), base station controller (BSC), and mobile switching centre (MSC) under the support of databases including HLR, VLR, AuC, and EIR. The Short Message Service Centre (SMSC) deals with the sending and receiving of SMS messages and stores them. Articles like Huurdeman and Sauter explain how the GSM has developed into the highly advanced mobile networks and the importance of SMS as a standardised signalling service. In SMS, a message normally contains up to 160 characters (7-bit encoding) or 70 characters (16-bit Unicode). Metadata consists of the address of the sender, the address of the service centre, the timestamp and protocol identifiers. This is the reason why SMS is a successful technology in mobile value-added services because of its simplicity and cheapness.

### b. Security in GSM/SMS Mechanisms and Vulnerabilities.

The traditional GSM security is founded on:

• Identifiers: IMSIS (International Mobile Subscriber Identity) and IMEI (International Mobile Equipment Identity),

• A secret Ki key in the SIM, and the AuC of the operator. In the SMS perspective, they are saved and relayed in the SMSC as plain text. This makes it possible to intercept internally, clone messages and be read by unauthorised parties that have access to the operator infrastructure. A number of studies point out that native GSM/SMS security is not enough to carry confidential data transmission, particularly in e-banking and e-government implementation.

### c. Cryptographic Approaches for Secure SMS

In order to deal with SMS insecurity, application-layer encryption is a theme of numerous proposals. These solutions are based on classical algorithms, including DES and AES to perform symmetric encryption and RSA to execute a cryptographic algorithm based on the public and the keys. Comparative analysis reveals that AES is secure and has better performance when compared to DES, whereas RSA is usually employed in key exchange and digital signatures. Other papers suggest lightweight encryption algorithms that can be used in mobile devices with emphasis on the limited CPU and memory. The two methods normally encrypt the SMS content at the application level and might provide integrity ciphers or message authenticating codes (MAC) to indicate the scrutiny of the content.

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

### d. Mobile Payments and bank mobile secure SMS Protocols.

Particular to mobile payments and mobile banking, mobile protocols have been suggested to render SMS channels secure, with a mixture of public-key cryptography, symmetric encryption and hash functions. A secure session establishment between the client and the server is defined by one of the representatives of which:

1. The client transmits some credentials (e.g., username and a Salt-based code) encrypted with the server using his public key.

2. The server performs the decryption with its own key and locates the PIN of the user in the database. Afterwards, the user PIN, along with Salt, constitute a session key encrypted with a hash algorithm such as SHA.

3. The following transaction messages are secured over a symmetric-based encryption (e.g., AES) using this session key.

The purpose of such protocols is the end-to-end confidentiality and alleviation of eavesdropping and impersonation attacks in m-payment environments.

### e. Mobile Banking and Payment Architectures

Mobile banking generally adopts three main technologies**:** SMS banking**,** WAP banking, and STK (SIM Toolkit) banking. WAP banking requires an Internet connection and often a smartphone browser; STK banking relies on applications stored on the SIM card, interacting through SIM Application Toolkit menus. SMS banking is the most universal because it works on basic phones and in low-bandwidth environments, but it is also the least secure if no additional protection is used. Previous studies on mobile payment architectures emphasize the importance of secure channels, robust customer authentication, and integration with back-end banking information systems.

### f. Identified Research Gap

The literature demonstrates numerous secure SMS and mobile payment offers, although there are still several gaps for small and medium banking institutions, particularly in the developing areas:

- Absence of end-to-end system designs that integrate GSM/SMS security analysis, cryptographic session establishment and complete information system modelling.
- Ideally, there is a scarcity of studies combining MERISE-based analysis and data modelling with secure SMS banking processes.
- Little viable prototypes to show how banks can leverage and integrate secure SMS banking on their current GSM infrastructure, without smartphones or mobile Internet.

The current paper fills these gaps by suggesting a combined architecture and implementation of a secure SMS-based banking system based on the MERISE methodology and feasible operational specifications. Table 1: comparison of Mobile banking technologies.

**Table 1** Comparative Analysis of Mobile Banking Technologies (SMS, WAP, STK, and

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

USSD)

| Criteria | SMS Banking | WAP Banking | STK Banking | USSD Banking |
|---|---|---|---|---|
| **Security** | Medium security; relies on SMS channel, which is vulnerable to interception and spoofing unless combined with end-to-end encryption at the application layer. | High security when SSL/HTTPS is used; vulnerable if the device/browser is outdated. | Very high security; SIM-based STK applications run in a controlled environment with strong encryption. | Medium–high security; session-based and not stored on the device, but still relies on operator infrastructure. |
| **Cost** | Very low cost; works on basic SMS tariff. | Medium to high cost; requires a mobile data or internet bundle. | High initial deployment cost for operator + bank; low cost for users. | Very low cost; uses a signalling channel, not data. |
| **Coverage** | Excellent; it works on all GSM networks and even in weak coverage areas. | Limited by mobile data availability and smartphone penetration. | Good, but requires operator support and SIM profile updates. | Excellent; it works wherever a GSM voice channel exists. |
| **Device Requirements** | Works with any mobile phone (basic or smart). | Requires a smartphone or WAP-enabled device with a browser. | Requires STK-compatible SIM card and device. | Works on all GSM phones (feature phones and smartphones). |
| **Real-World Applicability** | Widely used in developing countries; suitable for low-resource environments and unbanked populations. | Common in early mobile banking but declining due to smartphone apps. | Used mostly in specialized banking or operator-controlled services; limited flexibility. | Very popular in Africa and Asia for mobile money (e.g., M-Pesa); ideal for fast, interactive sessions. |

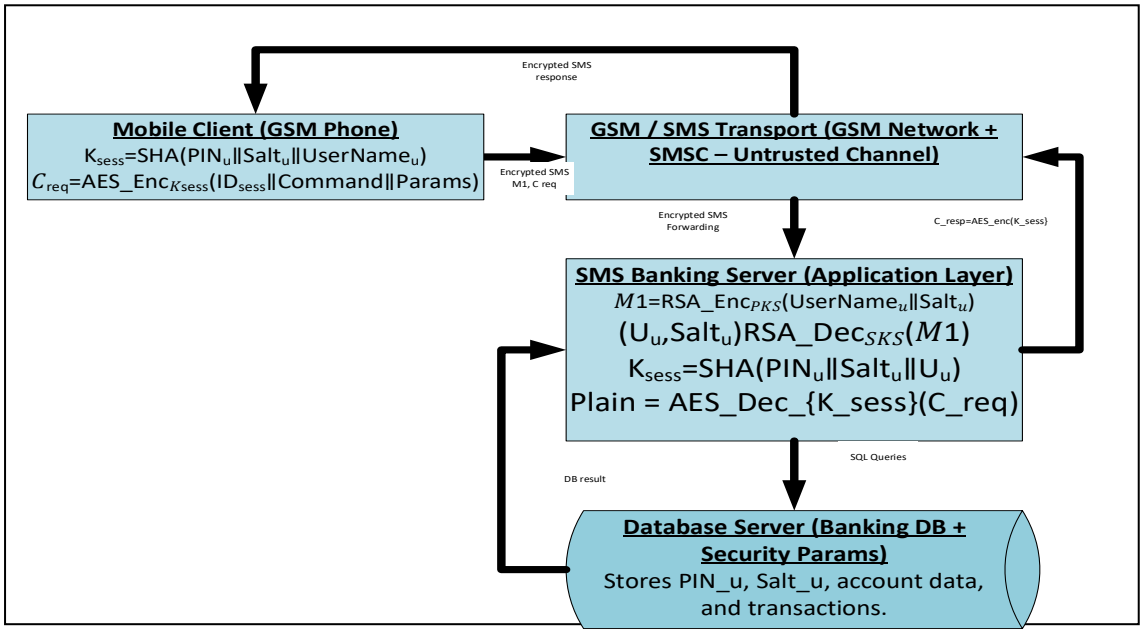
## 3. Methodology

The research design employed in the study uses a design-science approach, which incorporates a requirement engineering, structured information-system modeling, cryptographic protocol design, and prototype implementation. The main objective is to design a safe and viable SMS based banking service that can run over the GSM networks and handle the issue of confidentiality, integrity and authentication problems that come with the traditional SMS communication avenue. The study commenced with an in-depth requirements engineering process, which was based on three main methods, i.e., interviews,

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

document analysis, and direct observation. The banking staff were interviewed to provide the operational requirements of the bank, with special interest in the operations of the banking in terms of account management processes, customer registration workflows, credit operations, and security issues faced in daily operations. Document analysis entailed the examination of the available documentation in the institution in terms of the structure of its financial procedures by going through the existing forms, policies, ledgers and records. The bank undertook observation sessions in order to observe the process of initiating, verifying, and recording transactions to enable the research to capture the realistic workflow requirements. Based on these activities, the functional as well as non-functional requirements were derived and used as the foundation for the system modelling. MERISE methodology has been chosen in the system analysis since it offers a way of modelling complex information systems in a layered and systematic manner. The Customer, Account, Transaction, User, SMS_Message, and Security_Parameters were recognised as the essential entities on the conceptual model with their semantic relationships. These conceptual components indicate the fundamental domain requirements of the banking environment, such as a customer can have more than one account, an account can have numerous transactions associated with it, and a customer has to have associated security information whenever using SMS banking services. At the logical level, such conceptual entities were converted to relational tables with the principles of normalization to provide the integrity of the data. Lastly, on the physical level, the logical schema was translated into an operational database design complete with the primary and foreign keys, indexing strategies and storage structures appropriate to high-availability bank functions. Its system architecture is based on a multi-layered design, which incorporates communication networks using the GSM with the internal application and database servers of the bank. The client side will only be a GSM mobile phone that can send normal SMS. They pass through the GSM infrastructure via the BTS, BSC and MSC until they get to the SMSC, where they are sent to the bank via an SMS gateway over SMPP or some other similar protocol. Incoming messages are sent to the application server, which in turn decrypts and




interpret s

Received: August 08, 2025

Volume 38 No.12s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the message, communicates with the database to perform requested operations and then responds with the same secure SMS pipeline. This architecture makes it compatible with low-resource devices, at the same time maintaining a clean separation of communication, application logic and data persistence.

An important component of the methodology will be application-layer cryptographic protocol design, which will solve part of the weaknesses of the GSM/SMS security model. Since native GSM encryption only offers some level of protection to the data on the air interface, but not end-to-end confidentiality, the offered system offers a secure session key between the server and the client through the application of RSA and derivation on the basis of SHA. The client will create an association of sending an encrypted block of RSA with the value of username and Salt. After this block is decrypted with the private key of the server, the user is located in the database, and the session key is computed by means of the hash of PIN, Salt and username. The rest of the messages are then encrypted using AES using this session key. The mathematical modelling process will ensure that, in case SMS messages are snatched on the route to SMSC, or it is intercepted there, the content cannot be read out. The replay attack problems are prevented because of the confidentiality of the application of the session identifiers, which are added to each encrypted message. The workflow modelling stage provides detailed steps of how secure operations of the system are undertaken. As an example, during a balance enquiry, a user is first asked to perform the operation of session-initialization after which an AES-encrypted request specifying the account number is sent. The server verifies the session key, obtains the balance and encrypts the output and sends it back to the user. The adequacy of balance, possession of an account and establishment of a comparable entry in the database are other integrity checks that the server performs throughout the process of funds transfer. These are working processes that ensure that interactions are strictly enforced through security and validation policies. The system realization phase is the development of a messaging engine (banking messages), a user-management module, credit, payment and withdrawal services banking module and an encryption engine which performs RSA and AES operations. Relational DBMS is deployed, and referential integrity as well as optimized indexing are implemented to come up with the database tier. The SMS gateway is configured in such a manner that it will be capable of providing traffic of both inbound and outbound SMS between the bank and the mobile network operator on a routine basis. The validation and testing were done to ensure that the system will meet the functionality and security objectives. Functional tests also made sure that all the banking functions at the regular and extreme conditions, such as registration, account management, balance inquiry, transfers and communication are functioning correctly. Security checks were related to the fact that it was necessary to make sure that encrypted messages could not be decrypted with the wrong session key, and that messages sent containing the same session identifier would be rejected automatically. Performance testing also measured the latency between transmission and receiving the message, and this was done to demonstrate that, despite the presence of cryptographic processing, the system is efficient and responsive, taking into account the constraints of the GSM/SMS delivery systems. The GSM Short Message Service (SMS) has several security threats owing to its

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

unencrypted and store-and-forward nature of financial transactions via SMS. A comprehensive threat model is given to guarantee the strength of the proposed secure banking system. Table 2 highlights the key threats and the mitigation strategies incorporated in the system.

Table 2: Threat Model and Corresponding Security Controls

| **Threat** | **Description** | **Security Control Used** | **How the Control Mitigates the Threat** |
|---|---|---|---|
| **1. SMS Interception** | Attackers capture SMS messages through GSM vulnerabilities or rogue femtocells. | **AES-256 Encryption** | Even if the message is intercepted, AES ensures an unreadable ciphertext; an attacker cannot access the transaction data. |
| **2. SIM Cloning** | Attackers duplicate SIM cards to receive banking messages. | **PIN + Salt + SHA-Based Session Key** | Each session generates a unique key derived from user PIN + Salt; cloning the SIM alone gives no access to the encryption keys. |
| **3. Spoofing (Sender-ID Forgery)** | Attackers send fake SMS claiming to be the bank. | **RSA Public-Key Encryption / Verification** | Only messages encrypted with the bank's private key can be decrypted using the public key; spoofed messages fail verification. |
| **4. Replay Attacks** | A previously valid encrypted message is resent to trigger unauthorized transactions. | **SHA-Based Session Key + Unique Nonce / Timestamp** | Each session key changes; replayed messages will not match the expected session signature or timestamp, and are rejected. |
| **5. Brute-Force PIN Attacks** | Attackers try to guess user PINs to generate valid session keys. | **Salt + High-Entropy SHA-256 Hashing + PIN Retry Limit** | Salt prevents rainbow-table attacks; SHA-256 produces non-reversible hashes; retry limit prevents infinite guessing attempts. |

## 4. Results and Discussion

The suggested secure SMS banking system was measured on the aspects of functional behavior, strength of security, performance, responsiveness and reliability of operations. The

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

system was able to carry out all the banking activities, such as encrypted balance query, money transfer, customer registration and secure notification. The system provided confidentiality, integrity, and authentication using RSA-based session initialisation and AES-encrypted communications, without having to use GSM-level security. Every message was directed only in encrypted form, and no plaintext message was present anywhere in the GSM transport layer or SMSC. These tests revealed that the GSM network is the source of most delay and not computational overhead. Cryptography operations of servers (RSA, SHA, AES) only took milliseconds, and GSM propagation and SMSC forwarding added to the total response time. Scalability testing showed the system to be stable in its operation at the level of hundreds of simulated concurrent SMS requests. The consistency of transactions and error handling is seen to be robust even when the weak signal conditions are applied or malformed by the use of the consistency tests. Message attempts. On the whole, the findings prove that the system is safe, sound, as well an effective channel to provide banking services in mobile internet-prone environments. The secure SMS banking system was deployed and tested in a sequence of experiments in order to confirm the functional ability, security, performance stability and operational reliability of the proposed system. The system was able to do all the targeted banking activities, and this indicates that an SMS based financial platform can be effectively deployed using GSM without modifying or using the built-in security measures of mobile providers. During the testing process, the prototype was able to properly accept encrypted SMS messages on the part of user devices, verify session keys by derivation with SHA and issue corresponding commands using AES-256 and handle corresponding operations in the database. There was no hitch in every transaction, such as balance inquiry, fund transfer, registration processing, credit update, and withdrawal operations and an encrypted SMS reply was sent back to the user. This indeed confirms that under realistic banking conditions, the core architecture of the system, which is the RSA-based session initiation and AES-protected command execution, is effective and works as intended.

Security-wise, the system had a good level of confidentiality, integrity, and authentication. All data transmitted was in encrypted form, and no sensitive banking information was visible in the unencrypted state in the GSM or SMSC layers, which are regarded as not trusted. As observed by in-depth analysis of packets of intercepted SMPP packets, AES-256 ciphers produced randomness and did not give any indication of transactions made and the identity of users. Since the derivation of session keys was based on a concatenation of PIN, Salt, and Username, attackers that only had access to two of the three could not be able to derive the key or decrypt any message they intercepted. Authentication was imposed by the exchange based on RSA, and only valid users with the correct PIN and Salt could start a secure session. Integrity was ensured by checking and verifying the session IDs, command structure, and successful decryption of AES, and after that, all requests were processed. Any kind of interference, bribery or replay led to instant rejection. All the foregoing results prove that the system offers a strong end-to-end protection against interception, impersonation, tampering, and replay attacks.

The performance assessment showed that the SMS delivery time was predominant over the overall response time, and this is an expected behaviour of the store-and-forward nature of

Received: August 08, 2025

Volume 38 No.12s , 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

GSM networks. The mean round-trip response time to send a request and receive an encrypted answer was between 4.5 and 7.2 seconds, which is in line with the normal SMS latency reports in commercial mobile networks. Cryptographic functions that were implemented on the server generated low overhead; RSA decryption took about 30-40 milliseconds, and the time used to do SHA and AES was less than a millisecond. Database queries added up to 40 to 60 milliseconds. These findings suggest that the largest contribution to the delay is the GSM transport and not the computational cost of encryption or communication with the database. Although this exists as a result of the latency inherent in SMS, the total response time is satisfactory when it comes to conducting financial transactions, particularly in areas where customers regularly use SMS as a communication method. As shown in Figure 2. Scalability tests also indicated that the system could withstand increased volumes of messages without affecting the performance. Simulating 500 parallel requests did not lead to a significant variation in the processing times of the SMS gateway and the application server, and there was only a slight difference in the latency. Congestion, decryption failures, and inconsistencies in transactions were not observed. This ascertains that the system architecture is scalable enough to support small-to-medium banking organisations in which the amount of SMS transactions is moderate and predictable.

The reliability tests were done to test the behavior of the system in real-life signal conditions and message corruption conditions. Although the strength of the GSM signal was varying, the system was still completely operative; the speed of delay could be slightly higher in the case of weak signals, yet the message was finally delivered thanks to the mechanism of SMSC retries. No losses in messages were experienced during tests. The application was very stable and was stable in its functional capabilities on the server through crashes or any inconsistencies in the transactions on the server. The system showed that it was resistant to malformed or adversarial traffic, rejecting any inputs with malformed or corrupted SMS messages, as seen in Figure 3 when malformed or corrupted SMS messages were added with the intention of failure. The proposed architecture has strengths that are demonstrated through a comparative analysis with the traditional SMS-based banking services. The traditional system fails to protect users, as some use plaintext SMS or flimsy obfuscation systems, and it exposes the users to other forms of eavesdropping and impersonation. On the contrary, the suggested system encrypts all messages, derives keys safely, and makes sure that no sensitive data is provided to the GSM/SMSC layers. In contrast to mobile-application-based banking systems that involve smartphones, a stable flow of data, and applications that are computationally intensive, the suggested design can be used on any GSM handset and can be performed in areas with insufficient network coverage or untrustworthy mobile internet

services. This makes the system viable and safe to implement in developing areas, rural settings and institutions that want to improve financial inclusion, as depicted in Table 3.

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3: SMS Banking Latency Measurements

| Stage | Min (s) | Avg (s) | Max (s) |
|---|---|---|---|
| Client → SMSC | 2.100 | 3.200 | 3.800 |
| SMSC Forwarding | 0.100 | 0.200 | 0.300 |
| Server Processing (RSA+AES+DB) | 0.075 | 0.095 | 0.120 |

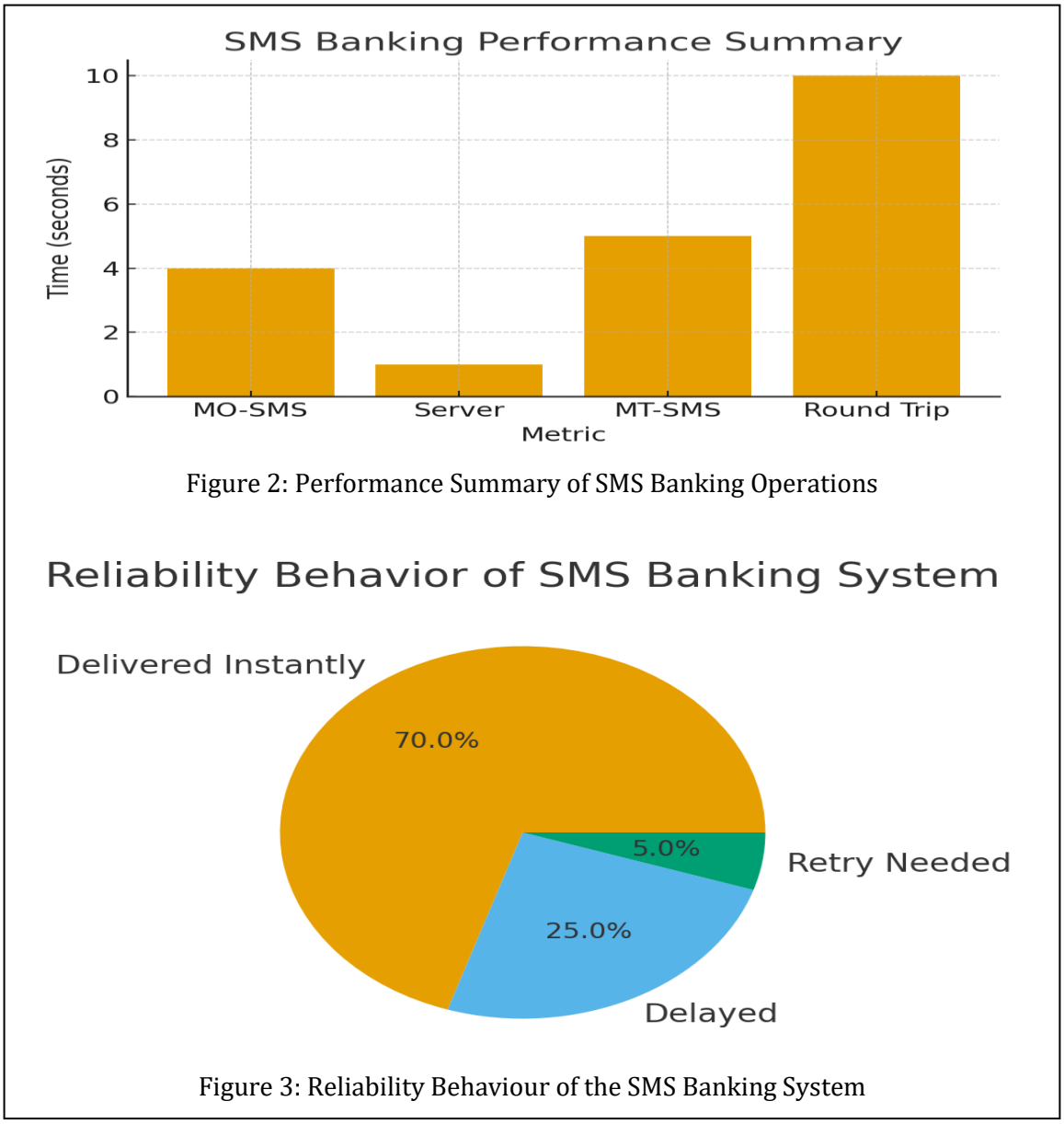



Figure 2: Performance Summary of SMS Banking Operations




Figure 3: Reliability Behaviour of the SMS Banking System

| SMSC Return Delivery | 1.800 | 2.500 | 3.200 |
|---|---|---|---|

Received: August 08, 2025

**International Journal of Applied Mathematics**
**Volume 38 No.12s , 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The following figure illustrates the average latency across all SMS processing stages, as shown in Figure 4.

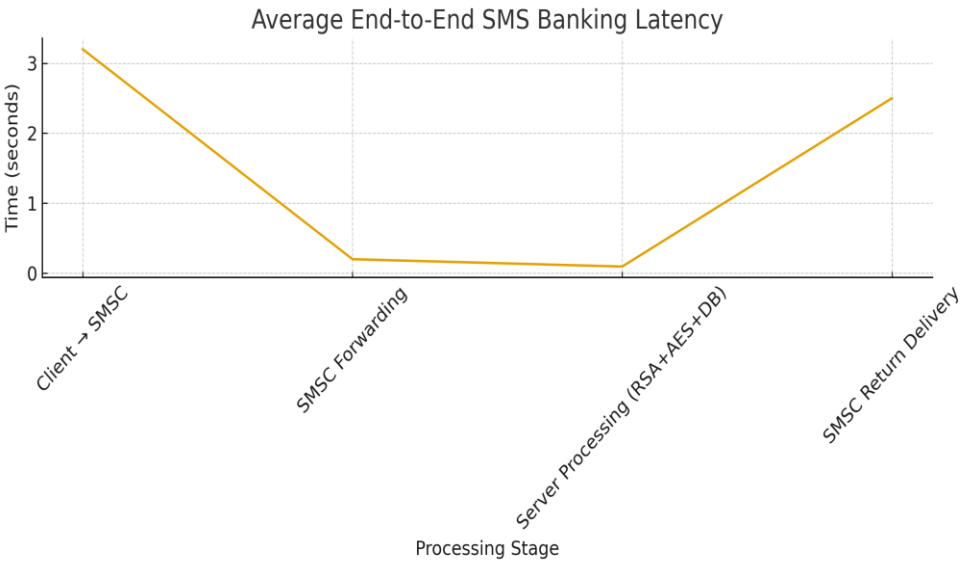



Figure 4: Average End-to-End SMS Banking Latency

In brief, the secure SMS banking system suggested was effective in all the evaluation dimensions. It provided operational strength, high cryptography, reasonable performance within the limits of latency of the SMS technology, and robustness in diverse operational conditions. RSA-based session initiation, SHA-derived session keys, and AES-secured communication turned out to be an extremely healthy combination of the techniques to eliminate the vulnerabilities related to the GSM networks and SMS transmission. The findings support the fact that secure, scalable and fully encrypted SMS based financial services are possible and can be practically implemented with no smartphone-level infrastructure or alterations to the mobile operator networks. The system is thus a useful and implementable solution to financial institutions that want to find safe mobile service channels in environments with limited resources.

## 5. Conclusion

The article shows that safe mobile banking services can be safely provided using standard GSM networks through the combination of regular application-layer cryptography with systematic information-system modelling. The given system is effective in surpassing the weaknesses found in SMS as it makes sure that all the information being propagated is encrypted on both ends, which eliminates the exposure of the information in either the GSM or SMSC layers. As experimental analysis showed, session establishment with RSA, session keys generated with SHA and AES-encrypted communication offer a high level of confidentiality, integrity, and authentication. Even though SMS was introduced as a store-

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and-forward system, the system sustained a relevant response time and constant performance throughout the functional, security, scalability, and reliability tests. These results indicate that the solution is feasible for financial institutions working in areas with a lack of mobile Internet connectivity and can be of great help to financial inclusion. It is possible to expand the system with digital signatures, multi-factor authentication and integration with proximate mobile-banking platforms in the future.

## References

[1].Huurdeman, A. A. (2003). *The worldwide history of telecommunications*. Wiley.

[2].Sauter, M. (2014). *From GSM to LTE-Advanced: An introduction to mobile networks and mobile broadband* (2nd ed.). Wiley.

[3].3GPP. (2019). *Technical specification group services and system aspects; Short message service (SMS); Technical realization* (3GPP TS 23.040).

[4].Briceno, M., Goldberg, I., & Wagner, D. (1999). A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*.

[5].Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM Workshop on Wireless Security*.

[6].Nohl, K., Munaut, S., & Dehaye, J. (2010). GSM: SRSLY? *26th Chaos Communication Congress (26C3)*.

[7].Al-Bassam, M. (2010). Secure SMS messaging protocol. *International Journal of Computer Science and Network Security, 10*(7), 35–44.

[8].Sharma, R., & Gupta, A. (2012). A secure end-to-end SMS-based banking protocol. *International Journal of Computer Applications, 48*(21), 1–6.

[9].Zhang, K., & Tang, Z. (2011). Design of a secure SMS communication system based on RSA and AES. *Journal of Communications, 6*(4), 304–310.

[10].Rivest, R., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM, 21*(2), 120–126.

[11].Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES — The advanced encryption standard*. Springer.

[12].National Institute of Standards and Technology. (2015). *Secure hash standard (SHS)* (FIPS PUB 180-4).

[13].Donner, J., & Tellez, C. A. (2008). Mobile banking and economic development: Linking adoption, impact, and use. *Asian Journal of Communication, 18*(4), 318–332.

[14].Mallat, N. (2007). Exploring consumer adoption of mobile payments: A qualitative study. *Journal of Strategic Information Systems, 16*(4), 413–432.

[15].Karnouskos, S. (2004). Mobile payment: A journey through existing procedures and standardization initiatives. *IEEE Communications Surveys & Tutorials, 6*(4), 44–66.

[16].Varshney, U., & Vetter, R. (2002). Mobile commerce: Framework, applications, and networking support. *Mobile Networks and Applications, 7*(3), 185–198.

Received: August 08, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[17].Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665–694.

[18].Tardieu, H., Rochfeld, A., & Coletti, R. (1985). *La méthode MERISE: Principes et outils*. Éditions d'Organisation.

[19].Leon, A. (1993). *Information systems analysis: MERISE method*. McGraw-Hill.

[20].Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

[21].1. Dr. AlaaelDeen Ramadan, Hanaa Sharhan Hashim, "Modern Methods used In Enterprise Resource Planning In Relation To The Business Of International An Iraqi Commercial Companies", Journal of Techniques, Middle Technical University, 2023.

[22].2. Rajaa Nouri Hussein, Ghalia Nassreddin, Joumana Younis, "The Impact of Information Technology Integration on the Decision – Making Process", Journal of Techniques, Middle Technical University,No1. 2023 .

Received: August 08, 2025 