A Multi-factor Security Protocol Utilizing Mobile Devices for Wireless Payment-Secure Web Authentication

Submitted in partial fulfillment of the requirement for the degree

of

MASTER OF TECHNOLOGY

INFORMATION TECHONOLOGY

UNDER THE GUIDANCE OF

Dr. Santosh Soni

&

Dr. Pankaj Chandra

SUBMITTED BY

NEHA DWIVEDI

(4th SEMESTER)

Roll No.: 23037103

Enrolment No.: GGV/18/1181

DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF STUDIES OF ENGINEERING & TECHNOLOGY

GURU GHASIDAS VISHWAVIDYALAYA, BILASPUR (C.G.) – 495009

INDIA

MAY-2025

CERTIFICATE

This is to certify that the dissertation entitled "**A Multi-factor Security Protocol Utilizing Mobile Devices for Wireless Payment-Secure Web Authentication**" is an authentic record of dissertation writing done by **Neha Dwivedi** a student **of M. Tech. (Information Technology)**, 4th Semester, Department of Information of the university.

Signature of Student

NEHA DWIVEDI
(4th SEMESTER)
Roll No.: 23037103
Enrolment No.: GGV/18/1181

This is to certify that the above statement made by the student(s) is correct to the best of my knowledge.

Signature of supervisor

DR. SANTOSH SONI

Signature of co. supervisor

DR. PANKAJ CHANDRA

Signature of Head of the Department
Dr. Manoj Kumar
(Professor)
HEAD
Department of Information Technology
SoS, Engg. & Technology
Guru Ghasidas Vishwavidyalaya
(Central University) Bilaspur (C.G.)

ABSTRACT

TICs are unique, pseudo-randomly generated codes issued by financial institutions to their customers. Each TIC is valid for a single transaction and is deactivated upon use, thereby mitigating the risk of replay attacks. TICs can be alphanumeric and are stored securely on the user's mobile device, encrypted with a symmetric key derived from a local password. The financial institution maintains a record of issued TICs and validates them during transaction processing to ensure authenticity. To protect the confidentiality and integrity of TICs, the system employs symmetric-key encryption. In symmetric-key encryption, the same key is used for both encryption and decryption, ensuring that only authorized parties can access the encrypted data. The encryption algorithm utilizes an iterated block cipher, which processes fixed-size blocks of data through multiple rounds of transformation, enhancing security by increasing the complexity of potential attacks. SMS serves as an out-of-band communication channel to authenticate transactions. Upon initiating a transaction, the system sends an SMS containing a one-time code to the user's registered mobile number. The user must respond to the SMS to confirm the transaction, providing an additional layer of security by verifying the user's possession of the mobile device. The proposed system incorporates two-way authentication to further enhance security. In this process, both the user and the financial institution authenticate each other, ensuring mutual trust. This approach mitigates the risk of man-in-the-middle attacks and ensures that both parties are legitimate before proceeding with the transaction. While SMS-based authentication provides an additional layer of security, it is susceptible to certain vulnerabilities, such as interception and SIM swapping. To address these risks, the system employs end-to-end encryption for SMS messages and implements measures to detect and prevent unauthorized SIM card changes. Additionally, the use of iterated block ciphers in the encryption of TICs enhances resistance to cryptographic attacks. The integration of TICs, symmetric-key encryption, iterated block ciphers, and SMS-based two-way authentication offers a robust framework for securing mobile-based online banking and purchasing transactions. By addressing the limitations of traditional authentication methods, this system provides enhanced security against a range of cyber threats, ensuring the confidentiality and integrity of user transactions.