Abstract:

The report focuses on the cybersecurity risks of smartphones and digital payments. It focuses on a problem and a research structure of the study. The report includes the various potential cybersecurity threats on smartphones and digital payments. It also includes the possible outcomes and best practices to avoid these potential cyber risks. Smartphones are an integral part of our lives and payments through smartphone shave emerged as the most popular in recent years. The report focuses on the risks in the utilization of the payments through smartphones.

Problem Statement:

The increase in digital payment over the few years has increased security threats. The attacks include mobile malware and viruses, phishing attack, keyloggers, trojan and fraud apps/updates and others. These cyber security risks lead to various adverse consequences such as theft, loss of integrity and leakage of confidential financial information.

Research:

The report consists of a problem system regarding the complication of digital payments and cyber security risks related to it. It also includes a discussion and analysis that consists of the cyber security risk in the payments app and protection techniques. It concludes with some best practices that can be undertaken by smartphone users to avoid cyber-attacks and to complete smooth payments.

Analysis:

The security breaches regarding mobile devices have not yet been systematically discussed in the literature. People need to be aware of such vulnerabilities, possible hazards, and actions they can take to minimise these. Using mobile applications comes with a variety of privacy risks. Some significant security issues in this study were presented to highlight by this research.

People should refrain from relying on just about any hyperlinks received through Text from dubious addresses, in addition to accepting SMS/MMS communications from unknown sources. Update the mobile Operating system as quickly as is practical after the patch is issued. Sensitive material should indeed be kept in safe facilities with good protection, a powerful passcode must be utilized.

Conclusion:

People depend on android smartphones to preserve everywhere from texts, personal documents, contact information, and online network account names to online payments, internet ordering, and general merchandise money transfers. This study looks at numerous cyber threats to smartphone devices including wallets and financial apps. The report focuses on cybersecurity issues in smartphone payment.

The report analyses possible risks and security issues of mobile phone payments and provides the best possible solutions and techniques to avoid these attacks. The outcome of the study is to analyse and evaluate the cybersecuriry risks in mobile phones and digital payments. These cybersecurity risks are based on the threats to the privacy of the users, mobile devices and security of the payments.