# A Secure and Robust Architecture based on Mobile Healthcare Applications for Patient Monitoring Environments

Shaik Shakeel Ahamad, Majed Alowaidi
Department of Information Technology, College of Computer and Information Sciences
Majmaah University, Al-Majmaah, 11952, Saudi Arabia

***Abstract*—The recent outbreak of COVID-19 pandemic realized the importance of patient monitoring environments, Mobile Healthcare Applications (MHA) plays very crucial role in the successful implementation of patient monitoring environments. Existing MHA's in the realm of patient monitoring environments are prone to repackaging attacks; do not ensure security, application security and communication security. This paper proposes a secure and robust architecture for mobile healthcare applications in patient monitoring environments ensuring end to end security ensuring all the security properties by overcoming repackaging attacks which are very vital for success of mobile healthcare applications. We implemented our proposed protocol in Android Studio, Kotlin is designed to interoperate fully with Java. ECDH Key exchange algorithm is used for key exchange between MHA in patient's smart phone and MHA in the hospital TPM. We created an EC key pairs (NIST P-256 aka secp256r1) at patient's MHA and MHA of hospital TPM by using ECDH and we created a shared AES secret key. AES with GCM mode used for encryption and decryption of patient data.**

***Keywords*—Mobile healthcare applications (MHA); UICC (universal integrated circuit card); Kotlin language; android studio; ECDSA (elliptic curve digital signature algorithm); GCM mode; end to end security**

## I. Introduction

The speedy development of information and communication technology (ICT) infrastructures are playing very important role in offering innumerous opportunities for efficient and affordable mobile health solutions. Mobile health solutions help in delivering healthcare anywhere and at any time overcoming geographical barriers, these services are a boon for the patients living in remote areas where health care facilities are not accessible. Mobile Healthcare Applications (MHAs) plays vital role in the successful implementation of mobile health solutions. Many Mobile Healthcare Applications (MHAs) are available in the market helping hospitals, doctors and patients. MHAs are available to assist hospitals, doctors in managing and in monitoring patients and in making clinical decisions. Smartphones and MHAs provide the following benefits to all the stakeholders especially patients, doctors and hospital staff as they ensure accuracy and efficiency. The author in [1] systematically assessed the consequences of cyber threats on health care. The security of user privacy information is very important for system deployment and operation [2]. The authentication process of Telecare Medical Information Systems (TMIS) occurs in a public channel, which is prone to attacks. Attackers can disrupt the authentication process through eavesdropping, interception, and forgery method, and launch malicious attacks such as forgery attacks, replay attacks, and side-channel attacks. These attacks can lead to malicious access and loss of data. Future MHAs are expected to include larger databases helping in making clinical decisions. COVID-19 pandemic realized the importance of patient monitoring environments, Mobile Healthcare Applications (MHA) plays very crucial role in the successful implementation of patient monitoring environments. During COVID-19 pandemic health information system became the primary target of cybersecurity attacks [3]. The health care industry should be prepared to overcome cyberattacks. The system can be protected from attacks by designing a secure identity authentication scheme and intrusion detection technology [4]. Among the main concerns in health monitoring frameworks are: reliability in making clinical decisions and security and privacy of data. Existing MHA's in the realm of patient monitoring environments do not ensure application security and communication security. Existing mobile healthcare monitoring solutions does not ensure Application security and communication security, Patient's privacy, not compliant with HIPAA standard and prone to repackaging attacks. This article's organization is as follows: In Section II discusses related work in the realm of secure mobile healthcare. Section III proposes a Secure Mobile Healthcare framework. Section IV presents an experimental setup and results, and Section V compares our proposed work with the related works. Section VI provides discussion of the proposed framework, and Section VII concludes the paper.

## II. Related Work

[5] monitors blood pressure, with a unique look and feel for monitoring heart health, which communicates with Bluetooth, so it is easy to share and store patient's records. The Omron HeartAdvisor mobile app [6] allows to transfers blood pressure readings smartphone based healthcare application. But both the solutions have the following limitations

*a)* End to End security is not ensured.

*b)* Patient's privacy is not ensured.

*c)* Not compliant with HIPAA standard.

*d)* Does not ensure application security

*e)* Does not ensure Communication security

*f)* These solutions are vulnerable to repackaging attacks

The author in [7] proposes an authentication scheme in Telecare Medical Information System (TMIS) based on Physical Unclonable Function (PUF) and Elliptic Curve Cryptography (ECC) technology. But this solution has no clarity:

*a)* How the ECC technology can encrypt the messages in the real time.

*b)* How the healthcare application overcomes reverse engineering attacks?

The author in [8] proposes healthcare systems with mutual authentication protocol thereby ensuring location privacy with low computation and storage costs, but this work also does not ensure application security and communication security. The author in [9] proposes a Cloud-IoT based healthcare system that uses a lightweight user authentication scheme, but this work do not ensure end to end security and prone to repackaging attacks. According to market watch, the Application Security Market will cross US$ 11 billion by 2024 globally [10]. According to marketsandmarkets IoT medical devices are will reach USD 63.43 billion by 2023 globally [11]. IoT medical devices are being used by many patients all around the globe as they make the life of patients easy and is evident from the predictions from marketsandmarkets [12], but these devices should be made secure right from the manufacturing phase of these devices which is the responsibility of the manufacturer. IoT medical devices use healthcare applications and applications need to be portable and secure, the security of these applications is the responsibility of the hospitals and the government. Healthcare data is kept in the hospital database and it is the responsibility of the hospitals and the government to keep the data secure thereby ensuring HIPAA regulations. In order to be HIPAA complaint network security should be ensured, i.e. protecting data at rest and during transit. This is the core motivation for this work. PhysioDroid [13] is an advanced system for remote monitoring of patient's health. The PhysioDroid system has the following:

*1)* A monitoring device transmits the collected readings.

*2)* A smartphone, data collector application for medical diagnosis and for health alerts.

*3)* Stores data from multiple sources.

The author in [14] discusses transport issues in the mobile Healthcare applications, proposes a platform for testing and finally proposes solutions to overcome these attacks. The author in [15] discusses server side security concerns and vulnerabilities in the mHealth apps and compares with the applications in other realms. The author in [16] proposes a data encryption solution for mobile health apps (DE4MHA). Following are the limitations of the existing research works in the realm of Mobile Healthcare Applications (MHA):

*a)* Application security and communication security is not ensured

*b)* Data in the hospital is not secure.

*c)* Patient's privacy is not ensured.

*d)* Not compliant with HIPAA standard.

*e)* Does not ensure application security

*f)* Does not ensure Communication security

*g)* Existing MHA's are vulnerable to repackaging attacks

The author in [17] proposes a new self-defending code (SDC) approach which encrypts parts of the app code at compile time and dynamically decrypts the ciphertext code at run-time but this work does not ensure the security of keys.

Following are the contributions made by our research work:

*a)* We have proposed a secure architecture from the UICC (Universal Integrated Circuit Card) of the patient's smart phone and hospital server and a secure protocol is proposed in the realm of Patient Management and Monitoring.

*b)* In our proposed healthcare framework MHAs overcomes repackaging attacks code obfuscation, code attestation and by enabling self-signing restrictions.

*c)* We have proposed a secure healthcare protocol ensuring all the security properties.

*d)* Compared our proposed healthcare system with the existing real time Mobile Healthcare Application solutions and existing research works in mobile healthcare and found to be better than these solutions and

*e)* We successfully implemented our proposed protocol in Android Studio and found to be better than the existing solutions.

*f)* Proposed healthcare framework overcomes known attacks.

## III. Proposed Healthcare Framework

In order to overcome the existing MHA and research works in the realm of Mobile Healthcare we propose a secure interaction between the MHA in the UICC of the patient's smartphone and the TPM of the hospital. Patient (P), Doctor (D), Hospital (H), Sensor (S), MHA in sensor, UICC in Smartphone and MHA in the UICC are the entities involved in the proposed framework. Existing MHAs are installed in the smart phone which can be compromised by malware, so we propose our secure framework in the SE of the patient's smartphone referred as UICC. Sensor (S) contains a SE, SE contains MHA collecting health information. This Sensor (S) MHA shares a symmetric key with the MHA in UICC of the patient's smartphone as shown in [12] and MHA of patient's smartphone shares a symmetric key with the MHA of TPM at hospital. UICC and MHAs in the UICC of the patient's smartphone are personalized by the TPM at hospital as shown in [18] Over-The-Air (OTA). TPM of the hospital is personalized by the hospital. Fig. 1 shows the interaction between the Patient's MHA (which is in the UICC of smartphone) and MHA of Hospital (which is in the Hospital TPM). There are nine layers at the both sides i.e. MHA, HTTPS (HTTPS Request and HTTPS Response), TLS, TCP, IP, BIP, SCP 102 223, SCP 102 221 and ISO 7816-3/4. MHA of patient's smartphone encrypts the messages with a symmetric key shared between MHAs of patient's smartphone

and TPM at hospital. HTTPS encrypts all the messages exchanged between patient's smartphone and TPM at hospital. Communication security is ensured using TLS a secure tunnel is established between patients.

UICC of smartphone and Hospital TPM, TCP ensures end to end reliability, IP is a protocol used at the network layer and BIP is a mechanism at the interface between the UICC and the smartphone providing access to the data bearers supported by the smartphone. ISO and the IEC jointly manages ISO/IEC 7816 standard. By using our proposed secure architecture end to end security and reliability is ensured in the information exchange between the patient and the hospital. Table I shows the notations used in the paper. Fig. 2 shows the steps involved in patient monitoring protocol.

Step 1: Sensor (S) collects patient's readings and sends it to the UICC of the patient's smartphone at regular intervals via Bluetooth Low Energy (BLE); in order to overcome BLE vulnerabilities, MHA in Sensor (S) encrypts the data sent to the MHA in the UICC of the smartphone (patient (P)). Patient's readings are encrypted with the shared symmetric key between the MHA of the Sensor (S) and MHA in UICC (P). Our proposed framework overcomes BLE vulnerabilities as our MHA's code is obfuscated by the MHA manufacturer and attested by the Certifying Authority (CA) and imposes self-signing restrictions, in addition to these data transmitted from the sensor (S) is encrypted using the symmetric key shared between sensor's MHA and the MHA of the patient (P). Data encryption prevents MITM and eavesdropping attacks. A secure link is established between the sensor's MHA and MHA in the UICC of the patient ensuring application security (symmetric key) and communication security (using SSL/TLS).

$$S \rightarrow P: \{PD, T_S, N_S, ID_P, ID_S, LOC_P\}SK_{PS}$$

Step 2: UICC (P) forwards the received message to the hospital's Trusted Platform Module (TPM) after decrypting the received message.

$$P \rightarrow H: \{PD, LOC_P, T_P, N_P, ID_P, ID_H\}SK_{PH}$$

Step 3: If the readings are abnormal then "H" shares patient's location to the ambulance

$$H \rightarrow D: \{PD, ID_P, LOC_P, T_H, N_H, ID_H\}SK_{HD}$$

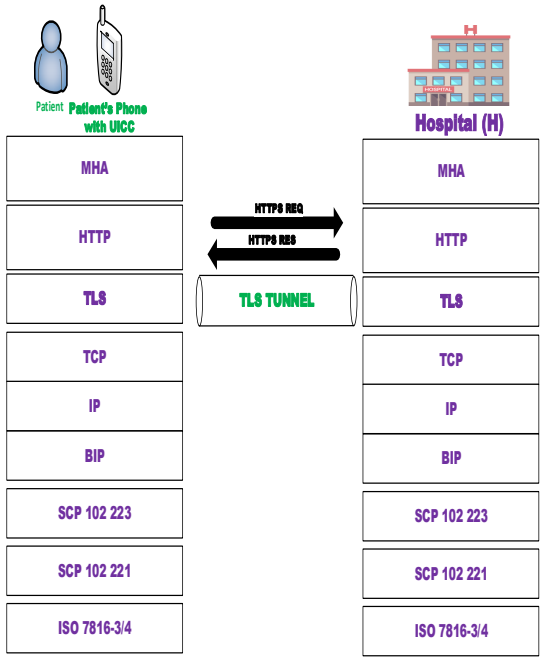


Fig. 1. Interaction between the Patient and Hospital.

TABLE I. NOTATIONS

| Notation | Full Form/Meaning | Notation | Full Form/Meaning | Notation | Full Form/Meaning |
|---|---|---|---|---|---|
| MHA | Mobile Healthcare Application | **OTA** | Over The Air | **$ID_P$** | Identity of Patient |
| HTTPS REQ | Hypertext Transfer Protocol Secure Request | **AES** | Advanced Encryption Standard, | **PD** | Patient Data |
| HTTPS RES | Hypertext Transfer Protocol Secure Response | **ECDH** | Elliptic-curve Diffie–Hellman | **P** | Patient |
| TLS | Transport Layer Security | **ECDSA** | Elliptic Curve Digital Signature Algorithm | **$ID_H$** | Identity of Hospital |
| IP | Internet Protocol | **SE** | Secure Element | **ACK** | Acknowledgment |
| BIP | Bearer Independent Protocol | **UICC** | Universal Integrated Circuit Card | **$SK_{PH}$** | Symmetric Key shared between Patient and Hospital |
| SCP 102 223 | Smart Card Platform 102 223 | **GCM** | Galois/Counter Mode | **$SK_{HD}$** | Symmetric Key shared between Hospital & Doctor |
| SCP 102 221 | Smart Card Platform 102 221 | **NIST** | National Institute of Standards and Technology | **$SK_{PS}$** | Symmetric Key Shared between Patient & Sensor |
| ISO 7816-3/4 | International Organization for Standardization (ISO) | **EC Key Pair** | Elliptic Curve Key Pair | **$T_P$** | Timestamp generated by Patient |
| **H** | Hospital | **HIPAA** | Health Insurance Portability and Accountability Act | **$T_H$** | Timestamp generated by Hospital |
| **P** | Sensor | **IoT** | Internet of Things | **$T_S$** | Timestamp generated by Sensor |
| **D** | Doctor | **IV** | Initialization Vector | **$N_P$** | Nonce generated by Patient |
| **$N_S$** | Nonce generated by Sensor | **$N_H$** | Nonce generated by Hospital | **$LOC_P$** | Location of the Patient |

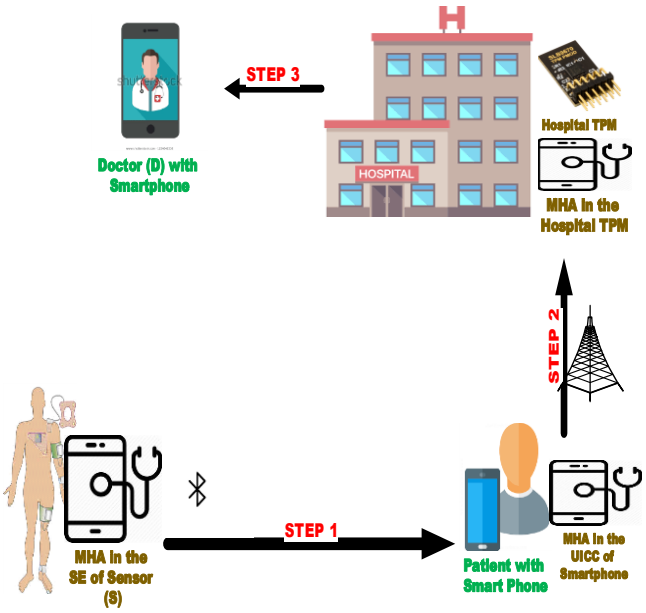


Fig. 2. Proposed Healthcare Protocol.

## IV. Experimental Setup and Results

We implemented our proposed protocol in Android Studio using Kotlin language; it was designed to interoperate fully with Java. ECDH Key exchange algorithm is used for key exchange between MHA in patient's smart phone and MHA in the hospital TPM. ECDSA, digest algorithm used is SHA-256 and AES symmetric encryption algorithm are used to ensure all the security properties. We created an EC key pairs (NIST P-256 aka secp256r1) at patient's MHA and MHA of hospital TPM by using ECDH and we created a shared AES secret key. AES with GCM mode used for encryption and decryption of patient data, Fig. 3 and 4.

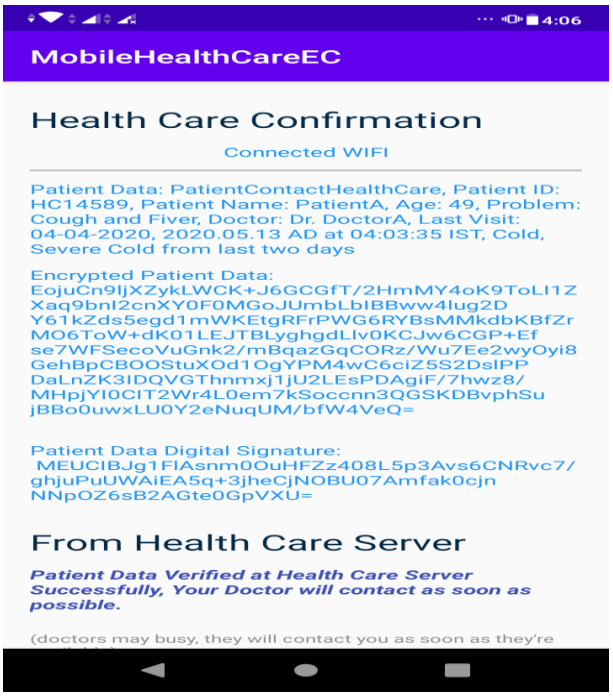


Fig. 3. Encrypted Patient's Data Transferred to Hospital.


Fig. 4. Confirmation of Patient Data at Hospital.

## V. Comparison with Related Work

We have proposed a secure architecture from the UICC of the patient's smart phone and hospital server and a secure protocol is proposed in the realm of Patient Management and Monitoring. Proposed healthcare framework MHAs overcomes repackaging attacks code obfuscation, code attestation and by enabling self-signing restrictions. In addition to these proposed secure healthcare protocol ensuring all the security properties. Finally, we have carried out our experiments in Android Studio and found to be better than the existing solutions by overcoming all the known attacks. This section highlights the comparative analysis of the proposed system with the eight existing real time MHA solutions and existing research works. Table II compares our proposed framework with the existing research works in this realm with the following features and found to be better than the existing research works.

*a) Confidentiality*: Confidentiality is ensured using a symmetric key at the application level which is shared between the entities.

*b) Authentication*: MHAs are authenticated using their respective certificates and moreover symmetric keys are shared among the entities involved in the framework.

*c) Overcomes Tampering of Messages*: Messages are encrypted using the shared symmetric key and data is hashed thereby ensuring the integrity of the exchanged messages.

*d) Compliant to HIPAA Standard*: Messages are encrypted using the shared symmetric key and communication security is also ensured using SSL/TLS protocol

*e) Application Security*: MHAs in both the sensor and UICC (of the patient) are protected by password. In addition to this MHAs are protected from repackaging attacks by implementing code obfuscation, code attestation and by enabling self-signing restrictions.

TABLE II. COMPARATIVE ANALYSIS WITH RELATED WORK

| **Research Works Features** | **[5]** | **[6]** | **[13]** | **[14]** | **[15]** | **[16]** | **Our Proposed** |
|---|---|---|---|---|---|---|---|
| Confidentiality | No | No | No | Yes | Yes | Yes | Yes |
| Authentication | | | | Yes | Yes | Yes | Yes |
| Overcomes Tampering of messages | No | No | No | Yes | Yes | Yes | Yes |
| Compliant to HIPAA standard | No | No | No | No | No | No | Yes |
| Ensures Application Security | No | No | No | No | No | No | Yes |
| Ensures Communication Security | No | No | No | Yes | Yes | No | Yes |
| Overcomes Heartbleed Vulnerability | No | No | No | Yes | Yes | No | Yes |
| Overcomes BLE vulnerabilities | No | No | No | No | No | No | Yes |
| Overcomes Replay Attacks | No | No | No | No | No | Yes | Yes |
| Overcomes Man-In-The-Middle Attacks | No | No | No | No | No | No | Yes |
| Overcomes Impersonation Attacks | No | No | No | No | No | No | Yes |
| Overcomes reverse engineering attacks | No | No | No | No | No | No | Yes |

*f) Communication Security*: TLS protocol at the communication layer ensures communication security.

*g) Overcomes heartbleed vulnerability*: Our proposed system uses newer versions of TLS certificates signed by the Certifying Authority (CA). Patients' private keys are secure which is vital to overcome this vulnerability. So our proposed system overcomes Heartbleed vulnerability.

*h) Overcomes BLE Vulnerabilities*: Sensor (S) and the UICC of the smartphone communicates at regular intervals through Bluetooth Low Energy (BLE). Our proposed framework overcomes BLE vulnerabilities as our MHA's code is obfuscated by the MHA manufacturer and attested by the Certifying Authority (CA) and imposes self-signing restrictions. So our proposed system overcomes BLE vulnerabilities.

*i) Overcomes Replay Attacks*: Encrypted messages containing timestamps and nonce helps in s overcoming replay attacks

*j) Overcomes Man-in-The Middle Attacks*: Encrypted messages containing timestamps and nonce helps in s overcoming MITM attacks.

*k) Overcomes Impersonation Attacks*: Our proposed system overcomes an impersonation attack as the attacker will be unsuccessful in generating session keys.

*l) Overcomes Reverse Engineering Attacks*: MHAs are protected from repackaging attacks by implementing code obfuscation, code attestation and by enabling self-signing restrictions on MHAs.

## VI. DISCUSSION

Health care industry is the main target of attackers as the existing healthcare solutions are very vulnerable. MHAs are updated through unreliable sources, so the security of these solutions is compromised putting patent's data in risk. So MHAs should be personalized and updated by the hospital after authenticating each other. Following are the recommendations for secure patient monitoring environments:

*a)* Healthcare solutions should ensure all the security properties.

*b)* Healthcare solutions should be compliant to HIPAA standard.

*c)* MHAs should withstand reverse engineering attacks

*d)* MHAs should encrypt the patient's data/information

*e)* Healthcare solutions should overcome all the known attacks.

*f)* Healthcare solutions should overcome BLE and heart-bleed vulnerabilities.

## VII. CONCLUSION

Health care industry became the primary target of attackers during COVID-19 pandemic, so health care industry should overcome all the cybersecurity attacks. This paper proposes a secure and robust architecture for mobile healthcare framework in patient monitoring environment which is compliant to HIPAA standard, ensures all the security properties. Mobile Healthcare Applications (MHA) in our proposed healthcare framework overcomes reverse-engineering attacks. We implemented our proposed protocol in Android Studio, Kotlin using Kotlin language. ECDH Key exchange algorithm is used for key exchange between MHA in patient's smart phone and MHA in the hospital TPM. ECDSA, digest algorithm used is SHA-256 and AES symmetric encryption algorithm are used to ensure all the security properties. We created an EC key pairs (NIST P-256 aka secp256r1) at patient's MHA and MHA of hospital TPM by using ECDH and we created a shared AES secret key. AES with GCM mode used for encryption and decryption of patient data. Our proposed mobile healthcare framework overcomes all the known attacks.

## ACKNOWLEDGMENT

The authors gratefully acknowledge the editor and the reviewers' helpful comments and suggestions, which have improved the presentation.

Funding: Dr. Shaik Shakeel Ahamad would like to thank the Deanship of Scientific Research at Majmaah University for supporting this work under Project No.R-2022-19.

*Competing interests*: The authors have declared that no competing interests exist.

REFERENCES

[1] D. W. Kim, J.Y. Choi and K.H. Han, "Risk management-based security evaluation model for telemedicine systems," *BMC Medical Informatics Decision Making*, vol.20, no.1, pp.1-14,2020. [doi: 10.1186/s12911-020-01145-7] [Medline: 32522216].

[2] S. Zhang, T. Yao, V.K.A. Sandor, T.H. Weng, W. Liang *et al.,* "A novel block chain-based privacy-preserving framework for online social networks," *Connection Science*, vol.33, no.3, pp.555-575, 2020 [doi: https://doi.org/10.1080/09540091.2020.1854181].

[3] C.M. Williams, R. Chaturvedi and K. Chakravarthy, "Cybersecurity Risks in a Pandemic," *Journal Medical Internet Research*, vol.22, no.9: e23692,2020 [FREE Full text] [doi: 10.2196/23692] [Medline: 32897869].

[4] W. Liang, L. Xiao, K. Zhang, M. Tang, D. He *et al.,* "Data fusion approach for collaborative anomaly intrusion detection in block chain-based systems," *IEEE Internet of Things Journal*, pp 1-1, 2021 [doi: https://doi.org/10.1109/JIOT.2021.3053842].

[5] Connected Omron Healthcare Products and Apps, 2021. [Online]. Available: https://omronhealthcare.com/service-and-support/connected-health/ [accessed 2021-07-02].

[6] HeartAdvisor, 2021. [Online]. Available: https://omronhealthcare.com/service-and-support/faq/omron-heartadvisor/ [accessed 2021-07-02].

[7] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo *et al.,* "A lightweight authentication scheme for telecare medical information system," *Connection Science,* vol.33, no.3, pp.769-785, 2021 [doi: 10.1080/09540091.2021.1889976].

[8] A. Tewari and B.B. Gupta, "An internet-of-things-based security scheme for healthcare environment for robust location privacy," *International Journal of Computational Science and Engineering*, vol.21, no.2, pp.298-303, 2021 [doi:10.1504/IJCSE.2020.105742].

[9] G. Sharma and S. Kalra, "A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services," *Iranian Journal of Science and Technology Transactions of Electrical Engineering,* vol.43, pp.619-636, 2019. [doi:10.1007/s40998-018-0146-5].

[10] Application Security Market Size will reach US$ 11 Billion by 2024 - MarketWatch. [Online]. Available: https://www.marketwatch.com/press-release/application-security-market-size-will-reach-us-11-billion-by-2024-2019-05-06. [Accessed: 18-June-2021].

[11] S. Singh. IoT Medical Devices Market worth $63.43 Billion by 2023. [Online]. Available: https://www.marketsandmarkets.com/PressReleases/iot-medical-device.asp. [Accessed: 18-June-2021].

[12] S. Kungpisdan, B. Srinivasan and P.D. Le, "Lightweight Mobile Credit-Card Payment Protocol," in *Proc. 2003 INDOCRYPT*, New Delhi, India, pp. 295–308, 2003 [doi: https://doi.org/10.1007/978-3-540-24582-7_22].

[13] O. Banos, C. Villalonga, M. Damas, P. Gloesekoetter, H. Pomares *et al.,* "PhysioDroid: Combining Wearable Health Sensors and Mobile Devices for a Ubiquitous, Continuous, and Personal Monitoring," *The Scientific World Journal*. Volume 2014, Article ID 490824, 11 pages [doi: http://dx.doi.org/10.1155/2014/490824].

[14] J. Müthing, T. Jäschke and C. M. Friedrich, "Client-Focused Security Assessment of mHealth Apps and Recommended Practices to Prevent or Mitigate Transport Security Issues," *JMIR Mhealth Uhealth*, vol.5, no.10: e147, 2017 [doi: 10.2196/mhealth.7791].

[15] J. Müthing, R. Brüngel and C.M. Friedrich, "Server-Focused Security Assessment of Mobile Health Apps for Popular Mobile Platforms," *Journal Medical Internet Research,* vol.21, no.1*:* e9818, 2019 [doi: 10.2196/jmir.9818].

[16] B.M. Silva, J.JPC. Rodrigues, F. Canelo, I.C. Lopes and L. Zhou, "A Data Encryption Solution for Mobile Health Apps in Cooperation Environments," *Journal Medical Internet Research,* vol.15, no.4*:* e66, 2013 [doi: 10.2196/jmir.2498].

[17] K. Chen, Y. Zhang and P. Liu, "Leveraging Information Asymmetry to Transform Android Apps into Self-Defending Code Against Repackaging Attacks," *IEEE Transactions on Mobile Computing,* vol.17, no.8, pp. 1879-1893, 2018 [doi: 10.1109/TMC.2017.2782249].

[18] S.S. Ahamad, V.N. Sastry and S.K. Udgata, "Secure mobile payment framework based on UICC with formal verification," *International Journal of Computational Science and Engineering*, vol.9, no.4, pp. 355-370, 2014 [doi: 10.1504/IJCSE.2014.060718].