Fuzzy Systems and Soft Computing
ISSN : 1819-4362

SECURE CLOUD-BASED HEALTH MONITORING SERVICES BY USING SVM CLASSIFICATION

[1]Gantambotla Harika, [2]Katakam Rohith, [3]Ranga Shreya, [4]Sana Tabassum, [5]Pavan Kumar Panakanti

[1,2,3,4]UG Scholar, Department of CSE (AI&ML)

[5]Associate Professor, Department of CSE (AI&ML)

CMR Institute of Technology, Hyderabad, Telangana, India-501401

ABSTRACT: Present smart applications with smart medical equipment, generating more data and it needs to be processed and trained locally for decision making, and also need to prevent privacy leaks. The storage and computing capabilities of smart devices are limited, so the storage needs to be outsourced and it must be secured. Cloud computing provides all requirements to support medical data and heath monitoring service with more security. In cloud-based health monitoring services, we propose a verifiable and secure SVM classification scheme (VSSVMC) for cloud-based health monitoring services in a malicious setting where the cloud server may return invalid decisions. By constructing verifiable indexes, VSSVMC ensures the verifiability of medical decisions, which enables clients to detect whether the cloud server returns incorrect or incomplete medical decisions. Symmetric key encryption is leveraged to ensure the confidentiality of the medical decision model and medical data with computational efficiency. We give security and verifiability definitions, and provide formal security and verifiability proofs for VSSVMC.

INTRODUCTION The new trends in the lifestyle leading to unhealthy eating habits, etc. have caused the potential diseases particularly of the heart and vascular to increase dramatically. Moreover, it is seen that the younger generation has also started suffering from heart problems [1]. Most of the deaths caused across the globe are because of the coronary heart disease. Thus, any progress leading to improved early diagnosis in a patient is always welcomed by medical community. The growth of chronic diseases and the elderly have significantly raised the costs of medical services [2]. With the proliferation of artificial intelligence and wearable devices, numerous medical institutes provide health monitoring services to reduce skyrocketing healthcare costs and improve the quality of medical decision services [3]. Coupled with the recent advances of cloud computing, cloudbased health monitoring services are

http://doi.org/10.36893/FSCC.2024.V09I01.099-108

new options to further reduce computational and storage costs in health monitoring systems [4], [5]. In particular, cloud-based health monitoring services involve three entities, i.e., a medical institute, a cloud server, and clients [6]. Specifically, the medical institute outsources a medical decision model to a cloud server, and later clients submit their medical features to the cloud server periodically and receive their real-time medical decisions based on the outsourced model. Such a procedure brings many benefits for health monitoring services, such as ease of management, ubiquitous access, and scalability. Apart from the well-known advantages, cloud-based health monitoring services may lead to critical privacy concerns as the cloud server may not behave honestly [7], [8]. From the perspective of medical institutes, the medical decision model, which is trained from a significant amount of sensitive medical records, is a valuable knowledge asset. Due to intellectual property protection issues, the confidentiality of the medical decision model should be ensured [9]. From the perspective of clients, both medical features and medical decisions are sensitive medical data for them. Accidental exposure of med-ical data may increase health insurance costs when a client has chronic diseases. In order to ensure the confidentiality, many secure SVM classification schemes have been proposed [10]. The existing schemes are mainly designed based on homomorphic encryption (HE), bilinear pairing [11]-[14], secure multi-party computation (MPC) [12],. Furthermore, the aforementioned schemes assume that the cloud server is an honest-but-curious adversary Unfortunately, this assumption does not always hold in real-world applications, because the cloud server may deviate from the prescribed scheme. Therefore, it is desirable to achieve the verifiability of the returned decisions in secure SVM classification for constructing trustworthy and privacy-preserving health monitoring services.

LITERATURE SURVEY To ensure the confidentiality of both medical models and medical data in cloud-based health monitoring services, a significant amount of secure SVM classification schemes have been proposed. The existing schemes can be categorized as ho-momorphic encryption (HE)-based schemes [15]–[17], bilinear pairing-based schemes [18], secure multi-party computation (MPC)- based schemes [19], [20], order-preserving encryption (OPE)-based schemes [21], matrix transformation (MT)-based schemes [22], and randomized Bloom filters-based

http://doi.org/10.36893/FSCC.2024.V09I01.099-108

schemes.[23]. Due to time-consuming operations in HE, MPC, and pairing, some of these schemes may incur prohibitive computational costs [15]–[18] or communication costs [19], [20] to resource-limited body sensors and wearable devices used in cloud-based health monitoring services. Both OPEbased [21] and MT-based [22] schemes are lightweight in terms of computational, communication, and storage overheads. Yet, OPE-based schemes may leak the numerical orders of data [21] and MT-based schemes may reveal the distribution of data [22]. Thus, both OPE-based schemes [21] and MT-based [22] schemes may incur privacy leakage in cloud-based health monitoring services. The randomized Bloom filter-based scheme in [23] protects the confidentiality of medical data with computational and communication efficiency. However, Bloom filter techniques inevitably introduce false positive to the medical decisions, which may lead to misdiagnosis issues

PROPOSED WORK we proposed a verifiable and secure SVM classification scheme (VSSVMC) for cloud-based health monitoring services in a malicious setting, which is a stronger threat model than that of previous secure SVM classification schemes. Different from the popular adopted honest-butcurious threat model, the malicious threat model enables a cloud server to forge or delete some of the medical decisions. To design VSSVMC, we first transform the SVM classification functionality to a function of conjunctively querying whether a feature vector is located in a multidimensional interval. Then, we build efficient query indexes for the SVM classifier, which could be expressed by decision rules. Later, we leverage pseudo-random permutations, pseudo-random functions, and symmetric key encryption to encrypt the query indexes and produce pseudo-random strings for decision verification. After that, the verifiable and secure SVM classification could be achieved by querying such encrypted indexes. By ensuring both decision verifiability and data confidentiality, VSSVMC enables trustworthy and secure cloud-based health monitoring services. the system model of cloud-based health monitoring services in Fig. 1, which contains three entities, i.e., a medical institute (MI), a cloud server (CS), and a client (C)

Fig 1: The System Model of Cloud-based Health Monitoring Services

http://doi.org/10.36893/FSCC.2024.V09I01.099-108

Model outsourcing and parameter delivery. In this stage, MI interacts with CS and C only once. Namely, MI outsources the medical decision model to CS and delivers some parameters to C. Medical decision requests and responses. In this stage, C interacts with CS periodically. Namely, C submits multiple medical decision requests to MI and waiting for the corresponding medical decisions, for each request-response round: C submits his medical features to CS and CS returns the corresponding medical decisions by utilizing the medical decision model.. SVM classification scheme, which ensures the confidentiality, verifiability, and efficiency for cloud-based health monitoring services.

1) Confidentiality. Both the medical decision model and the medical data (including medical features and medical decisions) should be protected against CS. With confidentiality, both the intellectual property (medical decision model) of MI and the data privacy (both medical features and decisions) of C are protected in cloud-based health monitoring services, which alleviates both the intellectual property protection and privacy leakage concerns of MI and C, respectively.

2) Verifiability. The invalid (including incorrect or incomplete) medical decisions received from CS should be detected. With verifiability, the cloud-based health monitoring service is secure against malicious adversaries and robust against software errors, which ensures the accuracy of medical decisions for C.

3) Efficiency. Sub-linear computational complexity and microsecond-level execution time should be achieved. With efficiency, the secure cloud-based health monitoring service is lightweight and efficient for resource-limited body sensors and wearable devices.

CONCLUSION We have designed a malicious threat model in cloud-based health monitoring services, and proposed VSSVMC to ensure the verifiability, confidentiality, and efficiency simultaneously. Different from existing secure SVM classification schemes, VSSVMC enables decision verification for detecting CS’s malicious behaviors such as forging or deleting the decisions. VSSVMC can perform verifiable and secure SVM classification with acceptable overhead. Therefore, VSSVMC is a potential option to construct trustworthy, secure, and efficient cloud-based health monitoring services. For the future work, we will improve the computational efficiency and reduce the

http://doi.org/10.36893/FSCC.2024.V09I01.099-108

storage costs of verifiable and secure SVM classification in malicious settings

REFERENCES

(1) J. B. Rubin and W. B. Borden, "Coronary Heart Disease in Young Adults", Curr. Atheroscler Rep., vol 14, no. 2, (2012), pp. 140-149

(2) A. S. Abiodun, M. H. Anisi, and M. K. Khan, "Cloud-based wireless body area networks: Managing data for better health care," IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 55– 59, 2019.

(3) M. W. L. Moreira, J. J. P. C. Rodrigues, K. Saleem, and V. V. Korotaev, "Computational learning approaches for personalized pregnancy care," IEEE Network, vol. 34, no. 2, pp. 106–111, 2020.

(4) A. S. Abiodun, M. H. Anisi, and M. K. Khan, "Cloud-based wireless body area networks: Managing data for better health care," IEEE Consumer Electronics Magazine, vol. 8, no. 3, pp. 55– 59, 2019.

(5) M. W. L. Moreira, J. J. P. C. Rodrigues, K. Saleem, and V. V. Korotaev, "Computational learning approaches for personalized pregnancy care," IEEE Network, vol. 34, no. 2, pp. 106–111, 2020.

(6) J. H. Abawajy and M. M. Hassan, "Federated internet of things and cloud computing pervasive patient health monitoring system," IEEE Communications Magazine, vol. 55, no. 1, pp. 48–53, 2017.

(7) D. B. Neill, "Using artificial intelligence to improve hospital inpatient care," IEEE Intelligent Systems, vol. 28, no. 2, pp. 92–95, 2013.

(8) M. Li, S. S. M. Chow, S. Hu, Y. Yan, C. Shen, and Q. Wang, "Optimizing privacypreserving outsourced convolutional neural net-work predictions," IEEE Trans. on Dependable and Secure Computing, vol. PP, no. 99, pp. 1–1, 10.1109/TDSC.2020.3029 899, 2020.

(9) A. Yang, J. Xu, J. Weng, J. Zhou, and D. S. Wong, "Lightweight and privacy-preserving delegatable proofs of storage with data dynamics in cloud storage," IEEE Trans. on Cloud Computing, accepted 2018, to appear, DOI: 10.1109/TCC.2018.2851256.

(10) J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "Cinema: Efficient and privacy-preserving online medical primary diagnosis with skyline query," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1450–1461, 2018.

http://doi.org/10.36893/FSCC.2024.V09I01.099-108