PRESERVING PRIVACY IN INTERNET OF THINGS DEVICES: A SURVEY

Mr. Rahul Sadashiv Kumbhar, Assistant Professor & I/C HOD, Dept. Of Computer Engineering (Poly), D.Y. Patil Technical Campus, Faculty of Engineering & Faculty of Management, Talsande, Kolhapur, Maharashtra, India 415412.

Abstract

The proliferation of IoT devices has contributed to the widespread adoption and familiarity of the Internet of Things, enhancing convenience in people's daily lives. However, cloud-based IoT devices often encounter significant network delays as they need to transmit a large number of photos to distant cloud servers. The emergence of edge computing has provided a solution by allowing data owners to upload their photos to nearby edge servers, addressing issues related to photo viewing and searching. This approach enables edge servers to efficiently receive and process the uploaded photos, resulting in substantial reductions in transmission time and bandwidth consumption. Various techniques have been developed to rapidly interpret visual data captured by IoT devices.

Keywords: — IOT devices, Machine Learning.

I. Introduction

With the emergence of retrieval services, individuals with limited resources can now store encrypted images on remote servers and access them whenever needed. However, existing randomized image search techniques, primarily designed for cloud computing scenarios, have certain drawbacks such as excessive utilization of data transmission resources and network latency. These limitations make them unsuitable for Internet of Things (IoT) devices operating in an edge computing environment. To address this issue, we propose a Secure and Verifiable Multi-key Image Search (SVMIS) framework within a cloud-assisted edge computing setting. Firstly, image feature vectors are extracted using a pre-trained Convolutional Neural Network (CNN) model to enhance search accuracy. Furthermore, a key distribution algorithm is designed to replace encoded records between different owners.

II. Literature

The Internet of Things (IoT) empowers us to establish connections among physical objects, spanning from smart buildings to portable devices like IoT wearables. The ability to remotely gather data and effectively manage and monitor objects represents the key advantages of IoT wearable devices. These capabilities can be harnessed in various ways, such as facilitating network connections, device discovery, user authentication, privacy protection, data sharing, and serving as the primary focus of the proposed research. Data sharing, due to its facilitation of collaboration and provision of services to individuals or entities, has become significantly prevalent in our everyday lives. This encompasses diverse scenarios, including user-to-user, user-to-device, and device-todevice interactions. Within this context, the environment of a user or an IoT device, characterized in this paper as broadcast signals, stands as one of the factors that enable data exchange. This work implements an IoT data sharing method based on something that is in a user's or an IoT device's surroundings using broadcast signals to measure RSSI[1] values and Machine Learning (ML) models. Through experimental testing employing multiple ML models, the proposed approach demonstrates a peak accuracy of 97.78%. Confidence in the security and privacy measures implemented in IoT smart devices to safeguard personal IoT data is lacking among many IoT consumers. Moreover, assessing the level of trust that end consumers have in their smart devices has become increasingly challenging. This article presents a research study aimed at identifying privacy concerns of end users regarding IoT smart devices. To ascertain users' privacy apprehensions, we conducted a survey and examined various smart devices. Additionally, we construct and apply five IoT privacy-preserving (IoTPP) [2] control strategies to compare the privacy protections put in place by a variety of wellknown smart devices. The findings from this study indicate that over 86% of respondents express either a high or very high level of concern regarding security. In the ecosystem of the Internet of Things (IoT), identity authentication has become an essential component of access control. Various IoT devices, including commercial banking smart cards, incorporate fingerprint authentication mechanisms to address the vulnerabilities associated with passwordbased verification. However, due to resource constraints on IoT devices, simplistic authentication methods are often employed, leading to significant degradation in system performance. Moreover, in these existing approaches, adequate protection for fingerprint templates is not ensured. To address these issues, we propose a privacy-preserving fingerprint authentication method specifically tailored for IoT applications. The proposed system comprises four key components: first, the extraction of minutiae points; second, the generation of a cancelable binary template[3] using the minutia cylindercode (MCC) approach, enhanced by our suggested normalized random projection technique; third, the construction of a lightweight privacy-preserving template through innovative pairwise Boolean operations; and fourth, fingerprint matching. Our method effectively mitigates attacks such as hill-climbing and preimage attacks. For prototyping the proposed system, we utilize the widely adopted open-source platform, Open Virtual Platforms. The effectiveness of our IoT-centric fingerprint authentication system has been extensively evaluated using eight benchmark datasets. Additionally, our system achieves authentication accuracy comparable to unprotected fingerprint authentication systems used in resource-rich, non-IoT environments. The Internet of Things (IoT) enables the connectivity of various devices to the internet, facilitating intelligent applications through the analysis of device data. In this context, edge computing serves as a typical IoT strategy, employing a three-tier architecture to reduce connections and enhance efficiency. Edge nodes play a crucial role in gathering and aggregating device data, while sending processed results to the cloud for further analysis. The privacy of device data will be compromised by the data aggregation mechanism. In this work, we presented PMDA [4], We propose an efficient privacy-preserving approach for aggregating multidimensional data in the context of IoT. This strategy employs a homomorphic encryption technique that preserves linear homomorphic properties for each dimension. By leveraging the Chinese remainder theorem, a multidimensional small integer vector is encrypted into a single ciphertext. The increasing number of IoT network attacks has led to a significant surge in the population of vulnerable IoT devices. Existing security systems suffer from challenges such as high energy consumption, long processing times, and a lack of real-time decision-making capabilities. To address these issues, we introduce the innovative Low-Latency Fogbased Framework called FogFed, which combines federated learning (FL) and fog computing to enhance the security of IoT applications. FL enables collaborative learning among IoT devices while protecting their privacy, while the fog component provides security mechanisms in close proximity to IoT devices, thereby reducing communication delays. FogFed integrates fogbased IoT attack detection utilizing binary FL classifiers [5] and cloud-based IoT attack detection using multiclass FL classifiers. Through extensive testing involving prominent IoT attacks, malware, and the UNSW-NB15 dataset, our approach demonstrates remarkable accuracy (99%) and detection rates (99%), surpassing centralized ML/DL models. Furthermore, it significantly reduces latency, ensuring privacy protection. As the usage of smart devices in various IoT applications continues to surge, security remains a major concern. Robust multifactor device authentication techniques are essential to ensure device security. Authentication failures can lead to the introduction of erroneous data into the system and expose vulnerabilities to malicious attacks. Therefore, secure authentication protocols are imperative for IoTenabled devices. In this study, we introduce the Rabin Cryptosystem based Biometric Privacy-Preserving User Authentication Scheme (RCBP2U-AS) [6], a novel method for user authentication. Our proposed approach demonstrates superior performance in terms of authentication and security compared to other existing schemes. We evaluated its effectiveness using the AVISPA (Automated Validation of Internet Security Protocols and Applications) simulation tool, and the results show that the system exhibits resilience against replay attacks, man-in-the-middle attacks, impersonation attacks, password guessing attacks, and various other assault scenarios. We also assessed the computation, communication, storage overhead, and overall calculation time of the proposed approach.

III. Conclusion

This paper focuses primarily on exploring different approaches used for privacy preservation in IoT-based devices and systems. Various techniques such as Searchable Symmetric Encryption (SSE), Content-based Image Retrieval (CBIR), Asymmetric Scalar-ProductPreserving Encryption (ASPE), the Harris method, facialbased authentication systems, human re-identification systems, and public safety surveillance camera systems are examined. The increasing importance of facial recognition (FR) in real-world IoT applications raises concerns about the privacy of face photos, both in terms of stored face datasets on cloud platforms and their regular use. Existing approaches often overlook privacy concerns on end devices and instead utilize saved face data to create privacy-preserving analytics models, such as deep learning with differential privacy. In this article, a novel and resource-efficient face representation strategy in the Bloom filter space is proposed to meet the specific requirements of IoT devices. This technology enables analytics on face data representation while ensuring privacy and maintaining data utility. The study also suggests a mechanism for collecting location data that adheres to local differential privacy, addressing privacy issues and safeguarding users' privacy. The low data processing efficiency of IoT due to network transmission delays can be mitigated by edge computing, which reduces data transmission lag and improves data processing speed. However, in edge computing, user data is typically processed and stored by trusted but potentially suspicious authorized organizations, posing a risk of personal data leakage. In this study, we employ the Delaunay method to create a Voronoi diagram, which divides the road network space. By identifying the Voronoi grid region [8] containing the edge nodes, we establish the basis for our privacy-preserving technique. To ensure local differential privacy, we introduce a random disturbance technique to perturb the original position data within each Voronoi grid. The effectiveness of this privacy-preserving technique is confirmed through comparison tests, demonstrating its superiority in meeting users' privacy needs and providing higher data availability compared to existing approaches. The increasing need for data sharing in various contexts, such as user-to-user, user-to-device, and device-to-device interactions, has become widespread in our daily lives. In this regard, we propose an IoT data sharing method based on the surrounding environment of users or IoT devices, leveraging broadcast signals to measure RSSI [9] values and employ Machine Learning (ML) models. Experimental testing of this strategy using multiple ML models shows a maximum accuracy of 97.78%. The electric Internet of Things (eIoT) edge perception layer involves a substantial amount of user data, including sensitive information like identity and location, making it susceptible to privacy breaches. To address this concern, we introduce an edge IoT agent-based eIoT model and propose a dynamic privacy-preserving method utilizing Multi-identity-based Fully Homomorphic Encryption (MIBFHE) [10]. Unlike previous designs, our mechanism eliminates the constraint of a single secret key, simplifying key management, revocation, and usergenerated secret key generation based on identity. Furthermore, our system exhibits dynamic fault tolerance, allowing calculations to proceed smoothly even in the presence of device introductions or failures. Considering that IoT systems consist of embedded devices with limited computing power and a cloud component for data processing and transmission, it is crucial to ensure strong security solutions that prioritize usability and scalability. In this work, we present an IoT authentication service for smart home devices utilizing QR codes, attribute-based cryptography (ABC) [11], and a smartphone as a security anchor. Recognizing the potential unreliability of certain IoT devices and cloud components within the IoT ecosystem, we propose an attribute-based access control protocol that safeguards privacy during device authentication for cloud services. By augmenting the FIDO UAF protocol with an attributebased privacy-preserving component, our solution provides enhanced security in smartphone-centric authentication to the cloud component.

References

[1] A. A. S. AlQahtani, H. Alamleh and R. Alrawili, "Privacy-preserving IoT Data Sharing Scheme," 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0428-0432,doi: 10.1109/IEMCON56893.2022.9946495.

[2] D. Joy, O. Kotevska and E. Al-Masri, "Investigating Users' Privacy Concerns of Internet of Things (IoT) Smart Devices," 2022 IEEE 4th Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2022, pp. 70-76, doi: 10.1109/ECICE55674.2022.10042926..

[3] X. Yin, S. Wang, M. Shahzad and J. Hu, "An IoT-Oriented Privacy-Preserving Fingerprint Authentication System," in IEEE Internet of Things Journal, vol. 9, no. 14, pp. 11760-11771, 15 July15, 2022, doi: 10.1109/JIOT.2021.3131956.

[4] C. Peng, M. Luo, H. Wang, M. K. Khan and D. He, "An Efficient Privacy-Preserving Aggregation Scheme for Multidimensional Data in IoT," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 589-600, 1 Jan.1, 2022, doi: 10.1109/JIOT.2021.3083136.

[5] Z. A. El Houda, L. Khoukhi and B. Brik, "A LowLatency Fog-based Framework to secure IoT Applications using Collaborative Federated Learning," 2022 IEEE 47th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 2022, pp. 343-346, doi: 10.1109/LCN53696.2022.9843315.

[6] D. Naidu and N. K. Ray, "Rabin Cryptosystem Based Biometric Privacy-Preserving User Authentication Scheme for IoT Devices over Cloud," 2022 OITS International Conference on Information Technology (OCIT), Bhubaneswar, India, 2022, pp. 409-414, doi: 10.1109/OCIT56763.2022.00083.

[7] W. Xue, W. Hu, P. Gauranvaram, A. Seneviratne and S. Jha, "An Efficient Privacy-preserving IoT System for Face Recognition," 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), Sydney, NSW, Australia, 2020, pp. 7-11, doi: 10.1109/ETSecIoT50046.2020.00006.

[8] Anitha, P.; Chakravarthy, T. Agricultural Crop Yield Prediction using Artificial Neural Network with Feed Forward Algorithm. Int. J. Comput. Sci. Eng. 2018, 6, 178–181.

[9] A. A. S. AlQahtani, H. Alamleh and R. Alrawili, "Privacy-preserving IoT Data Sharing Scheme," 2022 IEEE 13th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2022, pp. 0428-0432,doi: 10.1109/IEMCON56893.2022.9946495.

[10] Prasath, J.S.; Jayakumar, S.; Karthikeyan, K. Real-time implementation for secure monitoring of wastewater treatment plants using internet of things. Int. J. Innov. Technol. Explor. Eng. 2019, 9, 2997–300R. Qiu, J. Yu, F. Zheng, L. Liang and Y. Li, "Electric IoT Perception Layer Data Privacy-preserving Using Multi-identity-based Fully Homomorphic Encryption," 2020 IEEE 3rd International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), Shenyang, China, 2020, pp. 30-34, doi: 10.1109/AUTEEE50969.2020.9315709.

[11] M. Togan, B. -C. Chifor, I. Florea and G. Gugulea, "A smart-phone based privacy-preserving security framework for IoT devices," 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Romania, 2017, pp. 1-7, doi: 10.1109/ECAI.2017.8166453.

[12] A. V. Dastjerdi, H. Gupta, R. N. Calheiros, S. K. Ghosh, and R. Buyya, 'Fog computing: Principles, architectures, and applications,'' 2016,arXiv:1601.02752. [Online]. Available: http://arxiv.org/abs/1601.02752.

[13] V. Himthani, V. S. Dhaka, M. Kaur, D. Singh and H. -N. Lee, "Systematic Survey on Visually Meaningful Image Encryption Techniques," in IEEE Access, vol. 10, pp. 98360-98373, 2022, doi: 10.1109/ACCESS.2022.3203173.

[14] Q. -X. Huang, W. L. Yap, M. -Y. Chiu and H. -M. Sun, "Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images," in IEEE Access, vol. 10, pp. 66345-66355, 2022, doi: 10.1109/ACCESS.2022.3185206.

[15] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra and F. Khalifa, "A Robust Chaos-Based Technique for Medical Image Encryption," in IEEE Access, vol. 10, pp. 244-257, 2022, doi: 10.1109/ACCESS.2021.3138718.

[16] R. Ismail Abdelfatah, "Quantum Image Encryption Using a Self-Adaptive Hash Function- Controlled Chaotic Map (SAHF-CCM)," in IEEE Access, vol 10, pp. 107152-107169, 2022, doi: 10.1109/ACCESS.2022.3212899.