JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Survey on Privacy Preserving using IoT Devices

Shradha Vishwanath Nikam
D.Y. Patil College of Engineering

Prof. G. A Patil
D.Y. Patil College of Engineering

***Abstract*— The rapid growth of smart devices (IoT) has helped the Internet of Things become more well-known and regularly used. Because of this, people's daily lives are now very convenient. Cloud-based IoT devices are always prone to substantial network delays since they must transfer a sizable number of photographs to far-off cloud servers. With the development of edge computing, data owners can now upload photos to a nearby edge server to alleviate problems with viewing and searching for photos. The amount of photos that upload can be quickly received and processed by edge servers and data owners, significantly reducing the amount of time and bandwidth used for transmission. In order to swiftly evaluate visual data produced by IoT sensors, many techniques have been developed.**

Keywords*— *IOTBased devices, Machine Learning,

I. INTRODUCTION

With the development of reclaiming services, customers with limited resources will frequently store scrambled images on remote servers and search them anytime, whenever. In any event, current plans for randomised image search are suggested for cloud registering scenarios, but they have a few flaws, such as excessive information transmission , resource utilisation or organisation latency, which make them inappropriate for Internet of Things (IoT) devices in an edge figuring environment. In order to address this, a Secure and Verifiable Multi-key Image Search (SVMIS) plot in cloud-assisted edge registering is widely used. Pictures including vectors are removed using the pre-prepared Convolutional Neural Network (CNN) architectural mode in order to increase search precision. Keywise based circulation convention is used to switch out the encoded records of different owners.

II. IMPLEMENTATIONS USING IOT DEVICES THAT INCLUDE PRIVACY PRESERVING

The Internet of Things (IoT) gives the ability to engage present items, varying from intelligent structures to portable gadgets like IoT wearables. The capacity to remotely collect data and the ability to manage and monitor objects are the main benefits of IoT wearable devices. These attributes find application in various contexts, including networking, device discovery, user authentication, privacy protection, data sharing, and comprehensive technique exploration. Data sharing has gained prominence in daily life, facilitating collaboration and service provision between users and devices, encompassing user-to-user, user-to-device, and device-to-device scenarios. Research by A. S. AlQahtani, H. Alamleh, and R. Alrawili [1] highlight the role of the user's or IoT device's environment, referred to as broadcast signals, as a facilitating variable for data exchange. This research introduces an IoT data sharing methodology that leverages broadcast signals from the surroundings of users or IoT devices, utilizing Received Signal Strength Indicator (RSSI) [1] values and Machine Learning (ML) models for data exchange. Empirical validation of this approach using multiple ML models attains an impressive accuracy of up to 97.78%. The concerns regarding the security and privacy of personal data in IoT smart devices are frequently raised by numerous IoT consumers. Additionally, assessing the extent of confidence that users invest in their smart devices proves to be a complex undertaking.

Author D. Joy, O. Kotevska and E. Al-Masri [2] provides a study that identifies end users' privacy issues related to IoT smart devices. In order to determine users' privacy concerns, author looked at a number of smart devices and performed a survey. Additionally, author constructed and applied five IoT privacy-preserving (IoTPP) [2] control strategies to compare the privacy protections put in place by a variety of well-known smart devices. The findings from this study indicate that over 86% of the respondents express either high or very high levels of concern regarding security. In the

Internet of Things (IoT) ecosystem, identity authentication is now a crucial part of access control. Numerous contemporary Internet of Things (IoT) gadgets (like smart cards for commercial banking) come equipped with fingerprint authentication systems to address the inherent vulnerabilities of password-dependent verification. However, due to the resource constraints of IoT devices, uncomplicated authentication methods are employed, leading to substantial degradation in system performance.

Furthermore, in these current approaches, fingerprint templates are not safeguarded. S. Wang, J. Hu X. Yin and M. Shahzad [3] developed a fingerprint authentication approach for the Internet of Things that prioritizes privacy protection. The proposed system consists of four essential components in total: The initial phase involves the extraction of minutiae, succeeded by the generation of a cancellable binary template based on minutia cylinder-code (MCC), utilizing the proposed normalized random projection technique. The following stage involves creating a privacy-conscious template using novel pairwise Boolean operations. Subsequently, the fingerprint matching procedure is carried out. Potential attacks such as hill-climbing and preimage attacks can be mitigated effectively using a method specified by the author. To construct a prototype of the proposed system, an extensively employed open-source platform called Open Virtual Platforms is utilized. The effectiveness of the suggested fingerprint authentication system tailored for IoT is rigorously evaluated on eight benchmark datasets. Moreover, the authentication accuracy of the system is akin to open-source fingerprint authentication techniques utilized in scenarios not specific to IoT, where ample resources are available.The Internet of Things (IoT) enables terminal devices to connect to the Internet and provides a number of intelligent applications by analyzing device data.

Edge computing offers a three-tier architecture as a typical IoT strategy to cut down on connections and boost productivity. Edge nodes are specifically in charge of gathering and agglomerating device data, and sending processed results to the cloud for further analysis. The privacy of device data will be compromised by the data aggregation mechanism. In this research, author presented a privacy conserving multi-dimensional data aggregation scheme for IoT [PMDA] [4], an effective IoT multidimensional data aggregation approach that protects privacy. The strategy creates a homomorphic encryption technique that retains linear homomorphic features per dimension while encrypting a multidimensional small integer vector into a single ciphertext using the Chinese remainder theorem. IoT network assaults are rapidly increasing, which is driving a sharp increase in the number of unsecured IoT devices. Existing security systems have several issues, such as high energy consumption, protracted processing times, and a lack of real-time choices. In this line, the author introduced the FogFed novel Framework that is Fog-based and Low in Latency to safeguard IoT applications integrating fog computing with federated learning (FL). In order to eliminate communication lags, the fog supplies security features close to IoT devices, while the Federated Learning (FL) facilitates interactive education between IoT while maintaining their privacy.

FogFed combines multiclass FL classifier-based stored in the cloud IoT attack detection with binaries federated learning [FL] classifier-based [5] fog-based IoT attack detection.The UNSW-NB15 dataset and well-known IoT attacks were used in the trials, and the results show an accuracy level of ninety percent and detection rate of 99%, outperforming centralised Machine Learning [ML]/ Data Learning [DL] models while significantly reducing latency and protecting privacy. Smart device utilisation has recently expanded quickly as a result of the wide variety of IoT-based applications. Security is one of the key problems with IoT applications and devices. Device security can only be ensured by reliable multi-factor authentication methods. Incorrect data being fed into the system and harmful attacks could result from an authentication failure.

IoT enabled devices need safe authentication protocols. This paper suggests a user authentication technique called the Rabin Cryptosystem which is on Biometric Privacy-Preserving User Authentication Scheme (RCBP2U-AS) [6]. The proposed approach performs authentication and security quite a little better than other schemes. It is discovered using the simulation tool AVISPA (Automated Validation of Internet Security Protocols and Applications).Using the Automatic Verification of Internet Security Protocols and Applications (AVISPA) simulation tool, it was discovered that the system is immune to man-in-the-middle attacks, replay,password guessing attacks, impersonation attacks, and many other assaults. The computation, communication, storage overhead, and overall calculation time of the suggested approach are assessed.

III. FINDINGS

This paper mainly focuses on different approaches that are used for privacy preserving which involves use of IOT based devices and systems .Different ways and means were studied and conclusion was drawn .

IOT characteristics:

- IOT is a versatile device based mechanism that contains different techniques such as were searchable symmetric encryption(SSE),Content-based image retrieval (CBIR),asymmetric scalar-product-preserving encryption (ASPE),Harris method.facial-based authentication systems.
- Human re-identification systems, and public safety surveillance camera systems are just a few of the real-world IoT applications that have made facial recognition (FR) more crucial.Hence facial recognition is one of the assets of IOT.
- Face photos' privacy has come under increasing scrutiny, both in terms of the gathered face datasets stored on cloud platforms and in terms of their regular use.

Edge computing using IOT characteristics:

While ignoring the privacy issue in end devices of IOT, the majority of existing approaches (such as deep learning with differential privacy [7]) use the saved face data to create analytics models that maintain privacy. They propose a novel, efficient, and resource-efficient facial reconstruction approach in the Blooms filtering domain in this study that can satisfy the requirements of IoT devices. Our approach makes it possible to perform analytics on facial data representation while ensuring high data utility and privacyThis investigation proposes an approach to collect location data while ensuring local differential privacy compliance, effectively addressing these challenges to uphold user privacy. The Internet of Things (IoT) has been hampered by low data processing efficiency due to network transmission delays. Edge computing emerges as a solution to counteract this limitation, offering the potential to decrease data transmission lag and enhance processing speed. However, edge computing often involves processing and storing user data by reputable but potentially untrustworthy authorized entities, potentially compromising user privacy. To mitigate this, the study employs a Voronoi diagram generated by the Delaunay method to divide the road network space, identifying Voronoi grid regions [8] encompassing edge nodes. These regions' original position data undergoes perturbation using a random disturbance technique, ensuring local differential privacy compliance. Comparative tests validate the efficacy of this privacy-preserving approach [8], which not only aligns better with users' privacy requirements compared to existing methods but also enhances data availability. The prevalent trend of data sharing in daily life fosters collaboration between entities such as user-to-user, user-to-device, and device-to-device, offering services to both or either party. A key facilitator of data exchange is the user's or IoT device's environment, as discussed in this paper within the context of broadcast signals. This study implements an IoT data sharing mechanism that leverages broadcast signals from users' or IoT devices' surroundings, employing Received Signal Strength Indicator (RSSI) [9] values and Machine Learning (ML) models. Empirical assessments of this strategy utilizing multiple ML models yield a remarkable maximum accuracy of 97.78%.

The edge perception layer of the electric Internet of Things (eIoT) encompasses a significant amount of user data, which includes sensitive information such as identity and location, making it vulnerable to privacy breaches. To address this issue, a novel solution is presented: an eIoT model based on edge IoT agents is formulated, coupled with the introduction of a dynamic privacy-preserving method that employs Multi-identity-based Fully Homomorphic Encryption (MIBFHE) [10].This mechanism departs from the limitations of previous designs, allowing simpler key management, revocation, and user-generated secret key generation based on identity. The system is dynamically fault-tolerant, ensuring uninterrupted calculations even when a device is introduced or malfunctions. IoT systems predominantly comprise embedded devices with restricted computational capabilities, accompanied by a cloud component for data processing and transmission to end users. The access IoT devices have to users' private information underscores the need for a robust security solution, considering both usability and scalability. This study explores an authentication service designed for Internet of Things (IoT) applications in smart home devices. The method utilizes QR codes and attribute-based cryptography (ABC) [11], with smartphones serving as security anchors. Considering the possible lack of reliability in specific IoT devices and cloud

elements within the IoT environment, a protocol for attribute-based access control is introduced to ensure privacy during device authentication within cloud services. This is achieved by extending the FIDO UAF protocol to include a privacy-preserving attribute-based component, thereby augmenting the security of smartphone-centered authentication in conjunction with the cloud element.

Proposed Work:

Depending on the above survey of different systems research and analysis a system can be generated for solving an issue of image upload and retrieval which will preserve privacy which is lacking in the IOT based devices and systems.

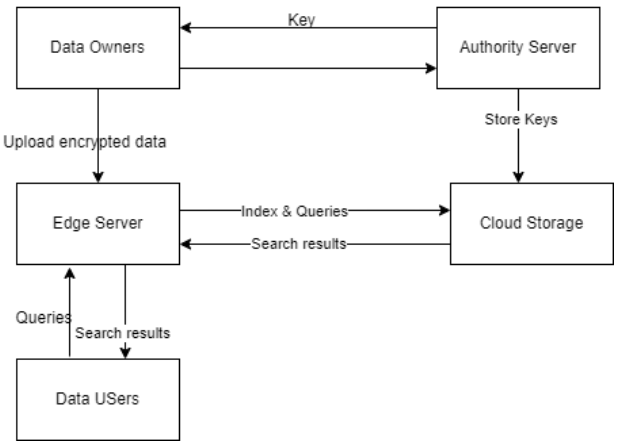

Fig. 1 Proposed Model for SVMIS

Figure 1 shows a system that will be a Secure and Verifiable Image Search (SVMIS). SVMIS achieves exceptional execution and great security. In the meantime, SVMIS prepares keywise dissemination convention to help the establishing and supplies an indisputable component to confirm the correctness of inquiry items in cloud-based edge registering framework.

Summary:

In summary, the burgeoning growth of IoT-enabled devices has significantly impacted the widespread adoption of the Internet of Things, enhancing daily convenience. Nevertheless, cloud-based IoT devices often face significant network delays when transmitting numerous images to distant cloud servers. The advent of edge computing offers a solution, enabling images to be uploaded to nearby edge servers, effectively addressing issues related to photo viewing and searching. This approach significantly reduces transmission time and bandwidth consumption. Diverse methods have emerged to rapidly interpret visual data from IoT devices, leveraging methods like detectable symmetric encryption (SSE), content-based image retrieval (CBIR), and facial-based authentication systems. These advancements have potential applications in privacy-preserving authentication, data sharing, and multidimensional data aggregation. Privacy concerns surrounding IoT devices have prompted the development of innovative privacy-preserving techniques that ensure data security while maintaining usability. Security is further improved by the use of attributes and biometric-based strategies, such as attribute-based cryptography and QR codes. Overall, this study outlines the evolving landscape of IoT-related privacy-preserving methodologies and suggests the potential of a Secure and Verifiable Image Search (SVMIS) system to address image upload and retrieval challenges while prioritizing data privacy.

IV. REFERENCES

1. 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 Low-Latency 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. M. Bi, Y. Wang, Z. Cai and X. Tong, "A privacy-preserving mechanism based on local differential privacy in edge computing," in China Communications, vol. 17, no. 9, pp. 50-65, Sept. 2020, doi: 10.23919/JCC.2020.09.005.
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. R. 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.