**UNIT 4**

Privacy-Preserving Internet of Things: Techniques and Applications

**I. INTRODUCTION**

Internet of Things (IoT) has risen as an predominant technology in the recent decade. It attracted the technology world for its easy and automatic nature of providing essential services to the users by sensing the environment. Number of devices and sensor connected together to form the IoT network in order to provide the service. Though it has numerous merits for its widespread usage in automatic management of household things, monitoring healthcare and transportation control, it has considerable security and privacy issues. Every node in IoT generates lot of data. It contains sensitive information about the users behavior. Hence, it is important to protect such information from leakage. Storage of IoT data is another important issue. It needs proper authentication and access control mechanism to protect the data. The data collected from IoT has rich insights for academics and research purpose. Analyzing the data without removing personal sensitive information would lead to privacy breach. So, it is important to preserve the privacy of the users before presenting the data for analysis. The privacy of the users can be preserved at various stages such as data collection, data storage and data analysis. Anonymous data collection methods have become popular since it hides the identity of the user and IoT nodes. Cloud based data storage is generally used to store the IoT data. The privacy of the data can be ensured during data storage through various encryption techniques. Homomorphic encryption techniques are used to protect privacy during data analytics and retrieval.

**SECURITY MANDATE IOT APPLICATIONS**

**A. IoT in Home Automation**

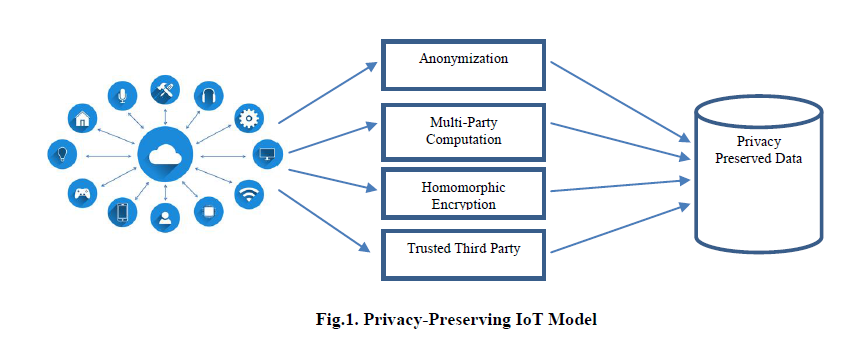
Smart Homes (SH) are equipped with different types of sensors and RFID to monitor and efficiently use the resources. The IoT devices are connected via wireless connection forming a network and share the data via edge networks[1]. The home automation system collects information about the daily usage of power and other user behaviors. Such data are highly sensitive and should not be revealed. Hence, it is important to develop an efficient privacy preserving home automation system. Privacy preserving home automation system protects the user identity, location privacy and daily behavior.

**B. IoT in Health Care**

IoT health care applications consists of wearable sensors, smart pill box [2], smart bed etc., to remotely monitor the patients’ health. However, it has various security and privacy concerns as it collects patient health related information. IoT devices utilizes fog based system or cloud based systems to store the health care information. Patients healthcare applications should collect the user data anonymously and the sensitive health related information must be removed. Such privacy preserved data is a rich resource of disease diagnosis and health care systems. So, developing health care application with privacy concern has become a mandate.

**C. IoT in Fog & Cloud Computing**

The ubiquitous nature of cloud and pervasive nature of IoT together called as cloudIoT [3]. Cloud computing based IoT system collects information from IoT sensors and it stores data in the cloud. The cloud computing offers different services to the IoT system such as storage, service, computation etc. It reduces the computation burden of IoT devices. Fog computing is also called as edge computing which is an extension of cloud



computing. Fog computing differs from cloud computing in the distributed network. Fog computing is a network of edge smart devices connected with cloud. Having fog nodes in the edge network eases the burden of cloud servers and improves ubiquity. Fog enabled IoT applications consists of fog nodes which performs routing, data collection and aggregation. The data are then transmitted to cloud for storage.

**D. IoT in Blockchain**

Blockchain is another emerging technology which is used in transaction and interactions. Blockchain for IoT applications can build the trust between the devices, reduces the computational costs, and accelerate transactions. Blockchain in IoT provides solution for the data synchronization among thousands of IoT devices. Traditional client server model fails to synchronize huge number of IoT devices [4].

**III. PRIVACY PRESERVING APPROACHES IN IOT**

The privacy breach in an IoT system can be preserved by different cryptographic and anonymization techniques. Fig.1 shows the privacy preserving IoT model to preserve the privacy of the IoT generated data. The privacy preserved data can be utilized for academics and research purposes.

This section describes the various privacy preserving approaches in IoT system. They are anonymization technique, multi-party computation, trusted third party computation and homomorphic encryption.

**A. Anonymization Techniques on IoT**

The sensitive information over IoT nodes are secured through aggregation of the information. However, there arises others problems such as computational delay, invalid results, software bugs etc. A public verifiable aggregation scheme is proposed in [5]. This scheme collects the data from untrusted nodes and then performs aggregation. The trustworthiness of the data can be verified publicly using the proposed tuple algorithms. Nevertheless some data owners have been dropped out in this scheme.

An anonymous raw data collection scheme for IoT without trusted authority is proposed in [6]. In this scheme the data is neither aggregated nor any noise added, but presented as the raw data for the analysis to get maximum utility of the data. The privacy of the collected data is preserved through obfuscation of data with other participants data in the group and thus it hides the individual privacy. Removal of trusted authority not only reduces the computation power but also unlinks the data with its contributor.

A privacy preserving anonymity and traceability patient’s data medical node of an IoT is proposed in [7]. The privacy of the patients are preserved using attribute based encryption technique (ABE). It controls the access to the medical records by a keyword match access control policy. The proposed system model comprises of trusted authority, medical nodes and cloud platform. The computational cost for this method is comparatively high.

An anonymous authentication protocol for IoT target driven application is presented in [8]. It is a fully decentralized protocol to ensure anonymity and unlinkability of participants and interactions. The proposed anonymous protocol aims to resolve the privacy issues between data holders and data collectors. The protocol used Shamir’s secret sharing scheme to protect the privacy. This protocol is criticized for its ad-hoc nature and insecurity[9]. Adversaries can impersonate as a genuine user to surpass the authentication system and cheat the data collectors.

Location based services of IoT always have a concern about the location privacy of the users. A dummy location privacy preserving algorithm (DLP) to preserve the location privacy of IoT devices is proposed in [10]. In this work they have analyzed the attack algorithm and developed an entropy-based location privacy preservation algorithm. It is designed to resist the colluding and inference attacks with minimal computational costs. It utilizes the greedy approach to select the dummy location until it reaches the k-anonymity.

**B. Secure Multi-Party Computation on IoT**

OppNet records location history of nodes in the network. It maintains a history table to find the best route to send the message from sender to receiver node. History table is prone to attacks and can leak privacy information. Privacy preserving history based routing mechanism is proposed in [11]. It aims to protect the identity and location privacy of the OppNets. It uses multiparty computation method to transfer the message from sender to receiver anonymously. It provides security and privacy by sacrificing some computational overheads. Reference [12] has proposed protocols to solve the privacy issues in smart grids. Smart metering system is an IoT based system which collects consumers data in proper intervals.

Hence, the privacy of the users is at risk. To protect the privacy of the of the users, fully homomorphic encryption (FHE) and secure multiparty computation (MPC) techniques are adapted to develop a protocol for smart grid advanced metering infrastructure. This mechanism addresses the excessive fragmentation problem of FHE and message complexity problem of MPC. The privacy of the users have been protected by using pseudo random number generator to calculate the share privately that are computed by other meters.

**C. Homomorphic Encryption on IoT**

A fog orchestration concept is introduced [13] in order to tackle the response time and service deliver issue due to the security methods in IoT. Fog orchestration allows the network to be self-tailored for the expected service to be delivered with necessary privacy and security solutions. This method utilizes attribute based encryption (ABE) and homomorphic encryption (HE) techniques to protect the privacy of the data with minimal latency and power consumption of IoT devices.

In [14] an anonymous privacy preserving data aggregation scheme for fog enhanced IoT system is proposed in order to protect the sensitive information. This scheme utilized pseudonym method to provide anonymity and authenticity. To preserve the data privacy Paillier algorithm is applied during data aggregation. This scheme is efficient for resource limited devices and real time communication. However, this scheme cannot be applicable for smart grids. A context aware privacy preserving method is proposed in [15]. This method is applied on a software defined networking (SDN) paradigm facilitated smart city IoT.

A context aware privacy preserving method is proposed in [15]. This method is applied on a software defined networking (SDN) paradigm facilitated smart city IoT. The privacy breach of the network is managed by monitoring the data packets flows through the network. SDN controller asdfasd monitors the network and when it finds a highly sensitive data, it divides the data into 70% and 30%. Then the first part of data transmitted over secure route found in the network and the second part transmitted via VPN.

A privacy preserving IoT architecture is proposed in [16]. The architecture protects the IoT sensitive data from disclosure and hacking. Homomorphic encryption scheme is utilized to control the access to sensitive data. The data is aggregated to addends hence the sensitive data are not revealed to the hackers or attackers. It provides an end-to-end privacy preserving data access scheme. The system is further evaluated based on its efficiency of query processing time.

Cognitive IoT extracts meaningful insights from the data collected from IoT devices. However, the trust worthiness of the data collected are verified by truth discovery approaches. It is important to design the truth discovery without breaching the privacy. A lightweight truth discovery framework to preserve privacy of fog based IoT systems called LPTD is proposed [17]. This framework prevents the privacy breach by adopting Paillier cryptosystem and one-way hash chain techniques. It prevents the false data injections and accomplish truth discovery with less computational and communication overhead.

**D. Trusted Third Party on IoT**

Trusted anonymous server based privacy preserving trajectory scheme for mobile IoT devices is proposed in [18]. This scheme protects the users location privacy by satisfying the spatial k-anonymity property for the group users snapshot queries. It resists inference attack on location based service provider and thus protects the location privacy of individual users. For continuous queries, a circular secure areas construction method is also proposed. It utilizes optimal average nearest neighbor method to maintain the distance between the users and hide the users real location information.

An outsourced multi authority access control scheme based on attribute based encryption method is proposed in [19]. Ciphertext-policy attribute-based encryption method provides data confidentiality and fine grained access control. Hence, this method is utilized in the proposed scheme to design a privacy preserving algorithm to transform the attributes anonymous and securely authenticable. The computation burden has been reduced by outsourcing the decryption computation.

**E. Other Techniques on IoT**

***i) Game Theory based Privacy Preservation***

A game theory based framework for social connection and interaction is modelled in [20]. This framework analyze the complex interaction among service providers, adversary and user in the network. The privacy leakage of online users are investigated through game theory methodology which examines the participants behavior in the network. This also guarantees private data trading through third party game model.

***ii) Blockchain based Privacy Preservation***

Crowdsensing is also called as mobile crowdsensing, which allows mobile users to collect, share and compute data to the requestor for rewards. The location privacy of the mobile users are at risk in crowdsensing. A blockchain based privacy preserving mobile crowdsensing system is described in [21]. The anonymous nature of blockchain technology is used to protect the privacy of the users. It is utmost difficult for the attacker to collect the transaction records hence the system is secured from re-identification attacks.

Although blockchain has numerous merits because of its decentralized nature and cryptographic technologies it doesn’t support thin-client systems such as IoT devices which cannot full node in a blockchain. Thus it is challenging to protect the privacy of the users in an blockchain based IoT systems. To address this problem a privacy preserving thin-client authentication system to enable the thin-client system to act like a full node with private information retrieval(PIR) system is presented in [25]. PIR protects the identity of the nodes and preserves privacy of the system. The security of the system is further enhanced by (m-1) private authentication system where even if the (m-1) nodes colludes together the privacy is still guaranteed.

***iii) Fog Computing based Privacy Preservation***

A privacy preserving data search framework for fog-assisted IoT system is proposed in [27]. In this framework the data of IoT devices are collected fog nodes and stored in fog based cloud system. When the users wants to search for the data, they search through the fog nodes. This framework comprises of two encryption scheme based on searchable encryption scheme. They are Credible and Semi-trusted fog node assisted searchable encryption. The first scheme targets to reduce the computational cost and also to support the offline users of IoT devices. The second scheme provides a fine grained access search over the fog nodes while protecting the privacy of the users through different authentication keys. IoT devices generate large amount of data and it can be efficiently accommodated in a cloud platform. However, there are many conflicts are present in cloud environment such as privacy, data placement, resource efficiency, power consumption and access time.

To address these aforementioned conflicts an IoT based data placement and privacy preservation method is designed in [22]. A privacy aware data placement framework is designed. It restricts the privacy leakages through privacy constraints on the host. Securing the data of IoT applications on cloud is a predominant problem. To store the user data securely, Chinese Remainder Theorem (CRT) is utilized to develop a storage mechanism[26]. To access the encrypted data from the cloud a CRT-based group key management scheme is also presented. This scheme uses multiple steps of encryption and decryption to protect the privacy of the data. However this scheme is not efficient for the key sizes less than or equal to 512 bits.

***iv) Chaos based encryption in Privacy Preservation***

One of the important dimensions of IoT application are E-Healthcare. Health and medical data collected from the patients generally consists of sensitive information. It is essential to protect the privacy of patients. A chaos-based encryption cryptosystem to preserve the privacy of patients is proposed in [23]. The proposed method encrypts the medical images using fast probabilistic image encryption cryptosystem. It also secures the medical keyframes extracted from wireless capsule endoscopy. The proposed method perform symmetric block encryption using confusion and diffusion operations.

Privacy preserving IoT system has weaker identity whereas highly secure IoT system needs stronger identity. In order to provide a balance between security and privacy a privacy preserving authentication protocol for IoT systems is developed in [24]. This framework is designed for weaker identity IoT end devices. Secure communications between the IoT devices are equipped with secret sharing scheme. Short group signature scheme is utilized to develop authentication protocol. This protocol provides a balance between security and privacy of an IoT system.

**IV. CONCLUSION**

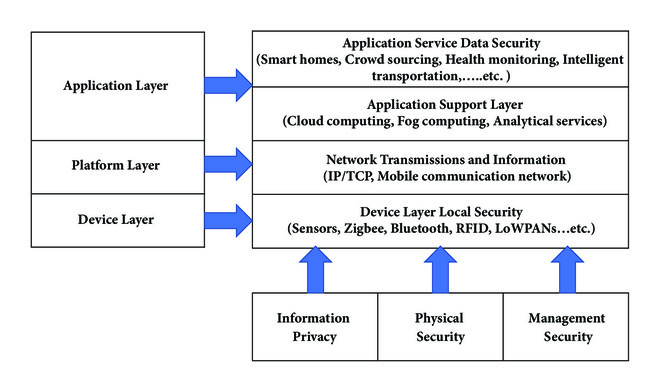
IoT devices collects lot of data which contains users personal information such as identity, location, and daily behavior. It is essential to preserve the privacy of users in IoT application.

This paper presents a list of privacy preserving techniques in IoT. At first, an overview of security mandate IoT applications are presented. Then various privacy preserving techniques in IoT are surveyed. Such as k-anonymity technique, secure multi-party computation, attribute based encryption and homomorphic encryption techniques.

Finally, a comparative analysis of various IoT based applications and privacy preserving techniques are presented. The table also compares different strategies followed to protect the privacy and performance evaluation methods of different IoT applications.

**Privacy Preserving IoT Environments**

Applying existing Internet standards to smart devices can simplify the integration of the envisioned scenarios in the IoT contexts. However, the security mechanisms in conventional Internet protocols need to be modified or extended to preserve user privacy in IoT applications. In this section, we discuss privacy preserving at different layers of the IoT stack. We build our discussions based on a three-layer IoT stack as shown in Figure [3](https://www.hindawi.com/journals/wcmc/2018/1032761/fig3/).

[](https://www.hindawi.com/journals/wcmc/2018/1032761/fig3/)

**Figure 3** IoT three-layered architecture.

**Privacy Preservation in IoT Device Layer**

The IoT device layer (also known as perception layer) contains all physical resources that collect/control data (sensors and actuators). However, these resources are highly heterogeneous and resource-constrained. Such constraints pose unique challenges on applying privacy preserving techniques. Thus, IoT devices are subject to several attacks discussed in [99] including node capture, fake node, malicious data, denial of service attack (DoS), timing attack, routing threats, replay attack, side channel attack (SCA), and mass node authentication problem. Therefore, several security measures must be considered when designing this layer as follows:(i)Access control and authentication: to prevent user privacy leaks from open and unauthorized access. Juels et al. [100] present a good solution to implement Selective RFID Jamming as an access control scheme on low-cost tags(ii)Data encryption: to secure data exchange and guarantee safe delivery. Wang [101] presents a nonlinear key algorithm based on displaced calculation to provide data encryption. This key algorithm requires low computational power to provide high security and good data transmission rate(iii)Secure channel using IPSec: the IPSec protocol [102] offers both authentication and encryption. Raza et al. [103] present a 6LoWPAN/IPsec extension to provide security for IoT devices. The authors demonstrate that IPSec outperforms the standard IEEE 802.15.4 link layer security in IoT environments(iv)Cryptography technology: to offer privacy protection, confidentiality, authenticity and data integrity. Secure communication protocols include digital signatures and hash values are used to ensure data integrity

**6.2. Privacy Preservation in Platform/Infrastructure Layer**

The platform layer represents the classical network layer in the OSI model [104]. This layer integrates intelligent data preprocessing to reduce resource requirements at the application layer. The network layer poses some general security problems related to data integrity and confidentiality such as unauthorized access to networks, eavesdropping, confidentiality and integrity damage, DDoS attacks, and man-in-the-middle attacks. Although existing network protocols implement highly secured measures, they are not robust enough for M2M communications in resource-constrained environments. As such, existing security mechanisms are weak/inapplicable on IoT devices and may lead to creating barriers rather than connections between different machines. Therefore, the heterogeneity of these networks makes security, interoperability, and coordination of networks becoming worse, leading to security vulnerabilities. New IoT-oriented security mechanisms must be designed from the ground up to fit IoT environments, taking into consideration the following security measures:(i)Set up an end-to-end authentication and key agreement mechanism, PKI (Public-Key Infrastructure), WPKI for wireless, Security routing, IDS, etc.(ii)Utilize network virtualization to reduce the network management complexity and the likelihood of improper operations.(iii)Adopt IPv6 as a standard network layer protocol to support inherited security mechanisms [105].

**6.3. Privacy Preservation in Application Layer**

The application layer encompasses 2 parts: the support layer where the edge computing and analytical services run and the application service layer that provides necessary support from the IoT infrastructure. IoT applications are also highly versatile and heterogonous with varying needs, which makes it a challenge to offer a standard support. Different applications target different domains with unique data collection requirements, which may require different security measures. Therefore, the application layer security considerations/requirements differ from the previous two layers in the following sense:(1)Nontechnical:(a)Privacy awareness: makes users aware of private data collection, potential risks, and how to safely use IoT services and avoid private information leakage.(b)Security management: strengthens resources, physical security information, password management, etc.(2)Technical:(a)Cryptography: fingerprint technology, digital watermarking, anonymous authentication, and homomorphic and threshold cryptography.(b)Key agreements: incorporate symmetric and asymmetric cryptosystems and certification transfer technology.