Privacy-Preserving Internet of Things: Techniques and Applications

Andrew J, Karthikeyan J

Abstract*: Privacy has become an imperative term in the recent technology developments. Lots of data are being collected through every digital activity of users. The expeditious development of IoT applications have raised the concern about the privacy of the IoT systems. The data collected via IoT sensors can reveal the daily behavior of the users, location, and other sensitive information. Hence, it is necessary to preserve the privacy of data collected by IoT devices. A large number of techniques and approaches have been implemented and used in different IoT based applications such as cloud computing based IoT, fog computing based IoT, blockchain based IoT and trajectory applications. In this paper, we present a detailed investigation of the existing approaches to preserve the privacy of data in IoT applications. The techniques like k-anonymity, secure multiparty computation, attribute based encryption and homomorphic encryption are analyzed. Finally, a comparative analysis of privacy preserving techniques with its applications are presented.

Keywords* : Privacy-preserving, IoT, Fog Computing, Cloud Computing, K-anonymity, Homomorphic Encryption, secure multi-party computation, attribute based encryption.

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.

II. 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

Revised Manuscript Received on August 25, 2019.

***** Correspondence Author

Andrew J*, Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, India. Email: onesimu@gmail.com

Karthikeyan J, School of Information Technology Engineering, VIT University, Vellore, India. Email: karthikeyan.jk@vit.ac.in

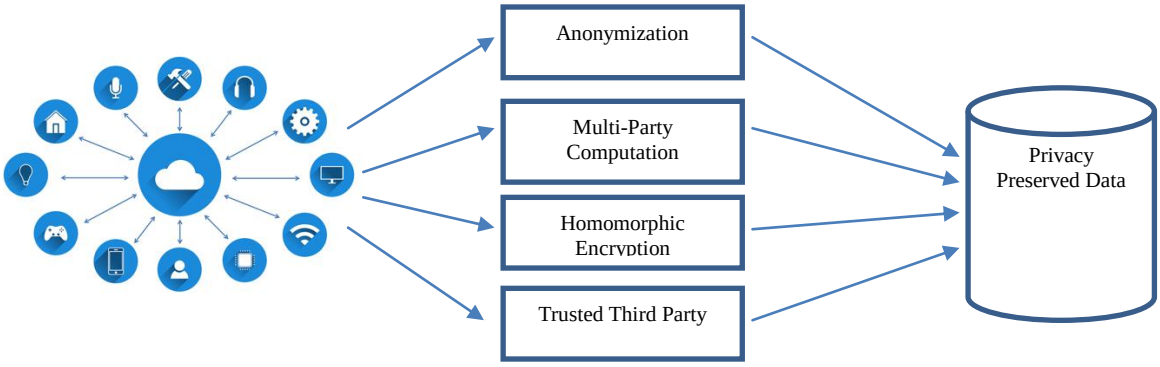

Fig.1. Privacy-Preserving IoT Model

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

Table- I Comparative analysis of privacy-preserving techniques on IoT

References	Technique	Application	Performance Evaluation	Year	Privacy-Preserving Strategy
[5]	Diffie-Hellman Key Exchange and Hash Function	LAN IoT	Time cost of aggregation	2019	Aggregation
[13]	attribute based encryption (ABE) and homomorphic encryption (HE)	Fog-enabled IoT application	Computation complexity & communication overhead	2019	Encryption
[14]	Fully Homomorphic Encryption (FHE) and Multiparty computation	Smart Grid	Paillier & EtoE Aggregation (Pai-EtoE), Packet Delivery Ratio (PDR) & Average Data Collection Completion Time (CT)	2018	Encryption
[12]	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	Fog-enabled IoT application	Computational cost	2018	Encryption
[22]	Genetic Sorting Algorithm	Cloud Computing	Average access time	2018	Data placement method
[6]	K-anonymity	Fog-enabled IoT application	Computational overhead & Communication Overhead	2019	Anonymization
[23]	Chaotic maps cryptosystem	Healthcare	NPCR & UACI	2019	Encryption
[19]	Ciphertext-Policy Attribute-Based Encryption (CP-ABE)	Fog-enabled IoT application	Computation complexity & Decryption time	2019	Encryption
[7]	Attribute based Encryption	Healthcare	Computational overhead & Communication Overhead	2018	Anonymization & Encryption
[20]	Game theory	Online social network	Nash bargain	2019	Randomization
[15]	Secure Route and VPN	Smart City	Completeness and Consistency	2019	Encryption
[24]	Shamir's Secret Sharing & Short Group Signature	Medical & Daily Living Environment	Security attacks	2017	Encryption
[8]	Shamir's Secret Sharing	Target driven applications	Unlinkability attack	2013	Anonymization
[16]	Paillier Cryptosystem	OpenIoT platform	Query processing time	2017	Encryption
[21]	Private blockchain	Mobile Application	Task Assignment success rate	2018	Anonymization
[25]	Public key infrastructure	Blockchain	Computational overhead & Communication Overhead	2019	Encryption
[26]	Chinese Remainder Theorem (CRT)	Secured storage	Compared with other encryption techniques	2019	Encryption
[27]	Searchable encryption	Fog-enabled IoT application	Keyword confidentiality and query privacy	2019	Encryption
[17]	Paillier cryptosystem	Fog-enabled IoT application	Computational overhead & Communication Overhead	2018	Encryption
[10]	K-anonymity	Location based system	Entropy and time complexity	2017	Anonymization
[11]	Multiparty Computation	OppNets	Network overhead ratio	2019	Anonymization
[18]	Spatial K-Anonymity	Mobile IoT	Average processing overhead and query processing	2019	Anonymization

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.

Further, a comparison Table-I is presented with IoT application details, techniques used to preserve the privacy and strategies.

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.

REFERENCES

1. T. K. L. Hui, R. S. Sherratt, and D. D. Sánchez, “Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies,” *Futur. Gener. Comput. Syst.*, vol. 76, pp. 358–369, Nov. 2017.
2. J. Jia *et al.*, “Intelligent and privacy-preserving medication adherence system,” *Smart Heal.*, Jul. 2018.
3. [3] A. Botta, W. de Donato, V. Persico, and A. Pescape, “On the Integration of Cloud Computing and Internet of Things,” in *2014 International Conference on Future Internet of Things and Cloud*, 2014, pp. 23–30.
4. S. Huh, S. Cho, and S. Kim, “Managing IoT devices using blockchain platform,” in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 464–467.
5. T. Li, C. Gao, L. Jiang, W. Pedrycz, and J. Shen, “Publicly verifiable privacy-preserving aggregation and its application in IoT,” *J. Netw. Comput. Appl.*, Oct. 2018.
6. Y.-N. Liu, Y.-P. Wang, X.-F. Wang, Z. Xia, and J.-F. Xu, “Privacy-preserving raw data collection without a trusted authority for IoT,” *Comput. Networks*, vol. 148, pp. 340–348, Jan. 2019.
7. Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, “Privacy-preserving fusion of IoT and big data for e-health,” *Futur. Gener. Comput. Syst.*, vol. 86, pp. 1437–1455, Sep. 2018.
8. A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, “Anonymous authentication for privacy-preserving IoT target-driven applications,” *Comput. Secur.*, vol. 37, pp. 111–123, Sep. 2013.
9. X. J. Lin, L. Sun, and H. Qu, “Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications,” *Comput. Secur.*, 2015.
10. G. Sun *et al.*, “Efficient location privacy algorithm for Internet of Things (IoT) services and applications,” *J. Netw. Comput. Appl.*, 2017.
11. S. Rashidibajgan and R. Doss, “Privacy-preserving history-based routing in Opportunistic Networks,” *Comput. Secur.*, vol. 84, pp. 244–255, Jul. 2019.
12. S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, “Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 547–557, Jan. 2018.
13. A. Viejo and D. Sánchez, “Secure and privacy-preserving orchestration and delivery of fog-enabled IoT services,” *Ad Hoc Networks*, vol. 82, pp. 113–125, Jan. 2019.
14. Z. Guan *et al.*, “APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT,” *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.
15. M. Gheisariy, G. Wang, W. Z. Khanz, and C. Fernández-Campusano, “A Context-aware Privacy-preserving Method for IoT-based Smart City Using Software Defined Networking,” *Comput. Secur.*, May 2019.
16. P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, “Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation,” *Futur. Gener. Comput. Syst.*, 2017.
17. C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, “LPTD: Achieving lightweight and privacy-preserving truth discovery in CIoT,” *Futur. Gener. Comput. Syst.*, 2019.
18. L. Zhang *et al.*, “A Trajectory Privacy Preserving Scheme in the CANNQ Service for IoT,” *Sensors*, vol. 19, no. 9, p. 2190, May 2019.
19. K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, “Efficient and privacy preserving access control scheme for fog-enabled IoT,” *Futur. Gener. Comput. Syst.*, vol. 99, pp. 134–142, Oct. 2019.
20. K. Li, L. Tian, W. Li, G. Luo, and Z. Cai, “Incorporating social interaction into three-party game towards privacy protection in IoT,” *Comput. Networks*, vol. 150, pp. 90–101, Feb. 2019.
21. M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, “A blockchain-based location privacy-preserving crowdsensing system,” *Futur. Gener. Comput. Syst.*, 2019.
22. X. Xu *et al.*, “An IoT-Oriented data placement method with privacy preservation in cloud environment,” *J. Netw. Comput. Appl.*, vol. 124, pp. 148–157, Dec. 2018.
23. R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, “A privacy-preserving cryptosystem for IoT E-healthcare,” *Inf. Sci. (Ny).*, Jan. 2019.
24. Z. Wang, “A privacy-preserving and accountable authentication protocol for IoT end-devices with weaker identity,” *Futur. Gener. Comput. Syst.*, 2018.
25. W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, “PTAS: Privacy-preserving Thin-client Authentication Scheme in blockchain-based PKI,” *Futur. Gener. Comput. Syst.*, 2019.
26. B. Prabhu kavin and S. Ganapathy, “A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications,” *Comput. Networks*, 2019.

27. R. Zhou, X. Zhang, X. Wang, G. Yang, H. Wang, and Y. Wu, "Privacy-preserving data search with fine-grained dynamic search right management in fog-assisted Internet of Things," *Inf. Sci. (Ny).*, 2019.

AUTHORS PROFILE

Andrew J at present serving as a faculty member in the Department of Computer Science and Engineering at Karunya Institute of Technology and Sciences, Coimbatore India. He is currently pursuing his Ph.D. degree from VIT University, Vellore, India. He has received his Bachelor of Engineering (B.E.) degree and Master of Engineering (M.E.) degree from Anna University, India in the year 2011 and 2013. He has published research articles in Springer and other Scopus indexed journals. He has authored/co-authored multiple journal articles, book chapters, and conference contributions. His research interests include IoT security, privacy preserving techniques, big data security, machine learning, deep learning, and blockchain technologies.

Karthikeyan J received his Ph.D. degree from Vellore Institute of Technology (VIT University), India in 2013. He has obtained his Bachelor of Science (B.Sc.) and Master of Computer Applications (M.C.A.) in the year 2005 and 2010 from VIT University, India. At present, he is serving as an assistant professor in the Department of Software and Systems Engineering, School of Information Technology and Engineering, VIT University, India. He is currently guiding 5 research scholars. He has authored and co-authored several research articles, book chapters, and conference contributions. His research area includes machine learning, big data security, privacy-preserving data publication, deep learning, etc.