I.J. Wireless and Microwave Technologies, **2023, 2, 7-22**
Published Online on April 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.02.02

A Systematic Review of Privacy Preservation Models in Wireless Networks

Namrata J. Patel*
Computer Engineering, Ramrao Adik Institute of Technology, D Y Patil Deemed to be University, Nerul, Navi Mumbai,400706, MH, India.
Computer Engineering, SIES Graduate School of Technology, Nerul, NaviMumbai, MH, India
E-mail: namratajitenpatel@gmail.com
ORCID iD:https://orcid.org/0000-0001-8643-5723
*Corresponding Author

Ashish Jadhav
Information Technology, Ramrao Adik Institute of Technology, D Y Patil Deemed to be University, Nerul, Navi Mumbai, 400706, MH, India.
E-mail: ashish.jadhav@rait.ac.in
ORCID iD: https://orcid.org/0000-0002-3575-6794

Received: 15 September, 2022; Revised: 24 October, 2022; Accepted: 15 November, 2022; Published: 08 April, 2023

Abstract: Privacy preservation in wireless networks is a multidomain task, including encryption, hashing, secure routing, obfuscation, and third-party data sharing. To design a privacy preservation model for wireless networks, it is recommended that data privacy, location privacy, temporal privacy, node privacy, and route privacy be incorporated. However, incorporating these models into any wireless network is computationally complex. Moreover, it affects the quality of services (QoS) parameters like end-to-end delay, throughput, energy consumption, and packet delivery ratio. Therefore, network designers are expected to use the most optimum privacy models that should minimally affect these QoS metrics. To do this, designers opt for standard privacy models for securing wireless networks without considering their interconnectivity and interface-ability constraints. Due to this, network security increases, but overall, network QoS is reduced. To reduce the probability of such scenarios, this text analyses and reviews various state-of-the-art models for incorporating privacy preservation in wireless networks without compromising their QoS performance. These models are compared on privacy strength, end-to-end delay, energy consumption, and network throughput. The comparison will assist network designers and researchers to select the best models for their given deployments, thereby assisting in privacy improvement while maintaining high QoS performance.Moreover, this text also recommends various methods to work together to improve their performance. This text also recommends various proven machine learning architectures that can be contemplated & explored by networks to enhance their privacy performance. The paper intends to provide a brief survey of different types of Privacy models and their comparison, which can benefit the readers in choosing a privacy model for their use.

Index Terms: Privacy, network, QoS, machine learning, location, temporal data

1. Introduction

Preserving privacy in wireless networks requires node anonymity, efficient access control, effectual authentication, data confidentiality, source location privacy, and sink location privacy. To achieve these privacy constraints, network designers must model efficient data & route control techniques. These techniques are implemented after careful threat analysis, including eavesdropping traffic analysis, query reveals analysis, authentication testing, privacy tracking, and impersonation. While security usually deals with ensuring data communication between nodes, physical security, external attacks, and internal node functioning without disruption, privacy deals with the selective sharing of data between different network entities.

Researchers are marking wide usage of wireless networks, which has opened substantial opportunities for entertainment, emergency services, and location-based services. Many service providers gather multiple forms of data from users to enhance QoS. Perhaps many service providers are not credible in storing the privacy of users and may be sold to the third party which may result in a user privacy breach. Hence to fortify this problem, the first objective is to

statistically analyse different privacy models and summarise the best-performing model. Secondly, efforts must be taken to design a unified model for securing group communication and monitoring privacy and QoS.

thus, the primary motivation of this article is to segregate these models in terms of different performance measures. These measures should include security and QoS performance, which will assist researchers in selecting the best possible model for their application deployment. A survey of these techniques can be observed in this text's next section, followed by a comprehensive performance evaluation and comparison of the reviewed protocols. This will assist researchers and network designers to select the most optimum combination of privacy preservation protocols for their deployment. Finally, this text concludes with some interesting observations about the reviewed models and recommends methods to improve them.

2. Literature Review

Models for privacy preservation assist the network by encapsulating sensitive information such as node location, routing path, data values, etc. This information is communicated in a way which is not understandable to any adversary nodes, thereby incorporating a high level of trust during network communications. Such a privacy-aware network is proposed in [1], which uses a combination of cluster head selection using Low Energy Adaptive Clustering Hierarchy (LEACH), data slicing, and dummy packet generation for privacy enhancement. Due to this the model showcases high privacy performance, with moderate delay but has high computational complexity due to dummy packet generation. The proposed secure and efficient privacy-preserving data aggregation algorithm or SECPDA algorithm outperforms CPDA and integrity learning with clustering CPDA (ILCCPDA) in terms of privacy but has low throughput, moderate energy consumption, and high delay when compared with these models. To reduce this delay, the work in [2] proposes an energy-efficient privacy-preserving data aggregation protocol based on slicing or EPPA model. The model aims to reduce the number of slices formed during communication via Euclidean-based decomposition, drastically reducing computational overheads and end-to-end communication delay. It uses a multi-function privacy-preserving data aggregation protocol (MPPA) for data aggregation using multifunction optimisation. The model is highly secure against a limited set of attacks but can be traced using cryptanalysis via reverse engineering sliced data packets.Moreover, the system doesn't provide any security measures, which limits its route & node privacy capabilities for large-scale deployments. This issue can be resolved using an efficient key exchange and high-performance data encryption model as suggested in [3], wherein a privacy preservation and encryption model using ECC is proposed. The model provides large-scale authentication and anonymity due to the use of hashing and efficient key-exchange mechanisms. Performance evaluation of this model showcases that it is highly secure but has sizeable computational complexity, thereby reducing its energy efficiency and applicability for a more significant number of data types. The summarization from above suvey is about Delay, data integrity in the transmission process, Data Accuracy, and Computation complexity in terms of energy efficiency.

A dynamic privacy preservation model can be observed in [4], where researchers have quantised user preferences as fuzzy values. These fuzzy values assist the algorithm in adopting attributed-based privacy preservation models measured using Shannon information entropy. The system model for this proposed method can be observed in figure 1, where multiple attributes are scanned depending on the user's preferences. These multiple attributes are given to a normalisation & rule mechanism for classifying users into 1 of the 'M' classes.

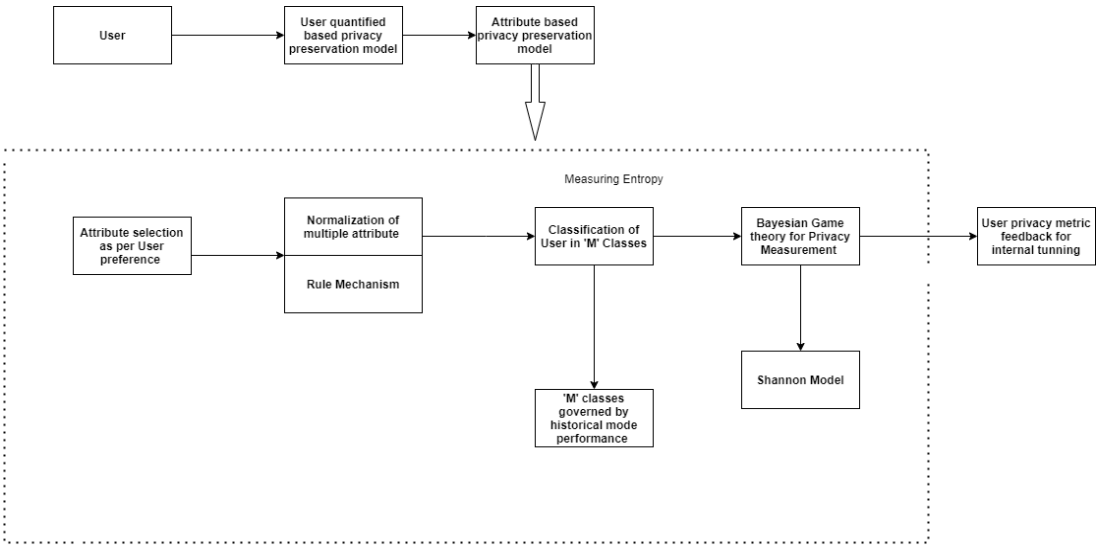

Fig. 1. Attribute based privacy preservation

Each of these 'M' classes are governed by historical node performance, and then using a Bayesian Game theory with mixed strategy equilibrium, the model is able to provide high levels of privacy. These privacy levels are measured by a Shannon model, and it again fed-back into the system for internal tuning. This tuning results into an improved privacy model via parameter tuning. The proposed model showcases high privacy performance, but requires large delay due to iterative privacy improvement. It has moderate packet delivery performance, and low energy efficiency due to continuous model tuning process. Such high privacy and moderate performance models can be applied for high security applications like medical image processing as observed from [5], where federated machine learning is deployed for low speed, and high privacy performance. In order to reduce this delay, the work in [6] proposes a privacy model that combines crowd-sourced data publishing with differential privacy. The model uses a combination of data perturbation, filtering, adaptive sampling, dynamic grouping and adaptive budget allocation in order to generate a sanitized and high privacy data stream. The model is observed to have high seclusion performance due to the use of differential privacy, dynamic grouping, recurrent neural networks (RNNs), and dynamic programming. But the delay, energy efficiency and throughput of network are drastically reduced due to RNN and other computationally complex sub models. Thus, limiting its performance for low power wireless networks. In order to overcome this drawback, the work in [7] proposes a high-speed model for data privacy using Boneh-Goh-Nissim homo-morphic encryption, and pseudo identity generation. The model is able to mitigate identity and data attacks, and showcases high QoS levels. But the model cannot be used for location, and temporal privacy preservation, which can be added by the use of Paillier cryptosystem as discussed in [8]. The proposed model is capable of removing internal network attacks and has good energy efficiency, but has low throughput due to slow operation of Paillier cryptosystem. To improve the speed of privacy preservation systems, the work in [9] can be referred, where researchers have used randomized responses for personalized privacy preservation. The personalized random response model assists in providing node-level privacy, but nodes need to share their personally identifiable information with this algorithm in order to preserve their privacy. Moreover, the model has cold-start issues, wherein initial data samples have generic privacy using conventional randomized response (CRRs), and then as data is gathered, the personalized randomized responses (PPRs) are used for privacy preservation. This issue can be removed via use of timestamp and instantaneous state-based responses for initial privacy preservation. Such a system can be observed from [10], wherein location privacy is provided to mobile nodes using semantic aware privacy model. The proposed model can be observed from figure 2, wherein inputs like trajectory database, points of interest (PoI), duration of stay, semantic categories, etc. are given to a deep semantic model for training. This model is able to fetch node's current location, and produce an anonymous fake location that can be used by router for route estimation and other network processes. The model can be extended for handling larger number of privacy preservation attributes via training the semantic tree with attribute-based datasets. Moreover, delay performance of this model is very low, which can be improved via use of light weight training models or hybrid computing models as discussed in [11]. Here, researchers have proposed a cooperative privacy preservation protocol, that uses space-aware edge computing for high privacy performance. The model is observed to support data-level privacy, but cannot be applied to low power remote devices due to use of edge computing. It has good throughput, and low delay, which makes it suitable for internet of things (IoT) like networks. The summarization from above is about Trust management, Recommendations on encrypted transfer learning approaches against individual privacy techniques like anonymisation, Testing the usability of differential privacy apart from Low Power wireless network , Achieving Data truthfulness on other services like Urban mapping,financial Data service ,Cold start issues due to randomised response, Location-based privacy can be trained using lightweight training models or hybrid models for improving delay.

The edge computing model can be replaced with a low power crowdsensing model as described in [12], where computational power is borrowed from mobile nodes, and privacy evaluations are performed. The model has low computational complexity, and thus is suitable for low power wireless networks. But due to use of crowdsensing, the model requires large computational delays, which slows down the network if limited number of processing nodes are available. In order to remove this drawback, metric temporal logic (MTL) [13] can be used, wherein simple Boolean expressions are evaluated in order to preserve privacy. The model is observed to be highly responsive, but has moderate privacy performance, and can only be applied to small & medium scale networks. Application of this model can be extended by incorporation of lightweight cryptographic modules as suggested in [14], wherein desynchronisation attacks are removed via kernel level privacy incorporation. This system model is found to be highly effective for static network scenarios, but does not support frequent updates in network structure and internal reconfiguration. Moreover, this model is applicable to only a small network of interconnected nodes and must be tested for a larger network. To summarise from above is about scalability which can also be tested for larger networks.

The process of aggregation can be explored in order to reduce input data size, and thereby improve internal working speed of privacy models. The work in [15] proposes such a scheme, wherein certificateless aggregate signature is used for high speed and high security data exchange between nodes. In order to perform this task, the model uses pseudo random key pairs, along with partial key generation, which makes it resilient against data forgery and spying attacks. But the model requires large computational delays for encryption, and aggregation, which reduces system throughput, and increases its energy consumption. The system can be further extended to support a greater number of attacks. A similar model that uses Chebyshev chaotic maps for randomizing node data can be observed in [16]. The model is able to remove any kind of data related privacy attacks, and must be tested for location & route privacy. Due to the simplicity of Chebyshev model, system complexity is reduced, thereby allowing for high throughput, and low delay communications. The only requirement of Chebyshev model is memory, thereby making it suitable for applications

where storage capacity is good. Due to this limitation, the model requires more energy, thereby limiting its use for low power applications. This limitation can be removed via the use of simpler models as proposed in [17], where round trip time (RTT) of packet is used for estimation of internal attacks. The model is light weight, and can be deployed for any wireless network that has loopback capabilities. But accuracy of attack prediction is limited by its capabilities to detect variations in RTT values. Thus, it is recommended that RTT must be combined with other network parameters for improving attack detection efficiency. To summarize from above is about Optimizing Energy requirements in chaotic maps for randomising node data. Improvising Round Trip Time packet from Network attacks

Protecting node identity is one of the most important tasks when considering network privacy. The work in [18] proposes a model that uses pseudonymous authentication for providing conditional privacy preservation. The model uses road side unit (RSU) for generation of pseudonymous IDs, along with specific time to live (TTL) information. This information is collected by an agent, and is enforced on the network in order to revoke access as soon as TTL condition is satisfied, thereby implementing conditional privacy. The model is able to remove node and network level attacks, and can be extended to counter data attacks via addition of slicing and other data privacy techniques. Performance of this model is good in terms of energy efficiency, but it requires large delays for authentication, which further reduces its throughput performance. This limitation can be removed via use of differential privacy schemes, similar to the one mentioned in [19], where Voronoi diagram is used to add dummies in the system. These dummies improve sensitivity of data by providing a cloak over the data using location shifting. The model must be extended for incorporation of other privacy preservation attributes. It is observed to have low energy requirement, but has high delay and low throughput due to addition of multiple dummies in the system. A similar model that uses combination of safe partitioning with random (dummy) data insertion can be observed from [20]. The proposed model is applied for temporal privacy preservation, wherein content similarity is evaluated and variance measures are added to it for anonymization. The model is tested on social networks, but must be evaluated on other networks for extensive analysis. Another specialized protocol that is applied for cognitive radios and uses bilateral privacy preservation with utility maximization can be observed from [21, 22]. The protocol is able to enforce location privacy, but can be extended for other attributed as well. It showcases low delay, and high throughput, but has low energy efficiency due to random deployment. To summarize from above is about motivating to use Pseudonymous ID along with specific time to live ,Cloaking the data by Location shifting .

An auction-based privacy preserving incentive scheme is proposed in [23], wherein software defined networks (SDNs) are used for auctioning privacy information. This information is collected from Mobile IoT nodes, and is used to enforce differential privacy in the network. The model is able to improve utilization of processing, but incurs longer delays when compared with random allocation, and price aware allocation schemes. This reduces its speed of operation, and thereby reduces communication throughput. In order to improve this throughput, the work in [24] proposes a distributed data privacy model, wherein privacy information is aggregated from different nodes, and used to preserve data & location privacy of underlying nodes. The network model has good speed, but does not support multiple privacy attributes, and requires more energy when compared with models that do not use aggregation. Similar models proposed in [25, 26] use collaborative computing, with differential privacy for enhancing indoor location & data privacy. These models do not have standard structures for representing privacy preserved data, which limits their applicability, because each protocol requires a separate adaptation engine for efficient deployment. In order to improve the applicability of privacy models, the work in [27] proposes use of blockchain with crowdsourcing for distributed computing. The model combines multiple criteria decisions making (MCDM) with simple additive weighting (SAW) for selection of consensus algorithms that can provide reduced energy consumption, maximization of service time, and improving profitability while network is in operation. The model is suitable for small to medium scale network, but its performance deteriorates as number of nodes in the network are increased. To summarize from above is about scheme for Auction based privacy preservation and to work for improving throughput,longer delay and privacy during Data Aggregation ,Preserving multiple Privacy attributes ,enhancing indoor location and data privacy and scalabilty.

Trust based routing can be used in order to identify unsafe nodes, and remove them from the network. Work in [28] proposes such a model for improving location privacy against nodes with low trust levels. The model proposes use of resilient privacy-preserving distributed localization algorithm for removing untrusted nodes from the network, thereby improving location privacy. This improves network security, but increases computational overheads, thereby reducing energy efficiency, and increasing delay of processing. This delay can be reduced via use of aggregative privacy preservation as observed previously, and also proposed in [29]. Here, an incentive mechanism is used in order to aggregate privacy data from crowdsourced nodes, thereby reducing delay of processing, and improving communication speed while adding highly efficient privacy model to the system. Similar crowdsourced models that use blockchain can be observed in [30-32], wherein deep learning with Variational Auto Encoder, smart contracts, and encrypted data processing are used. These models are able to mitigate data poisoning attacks, spoofing attacks, data integrity issues, etc. But these models face scalability challenges, and thus must be used with small & medium sized networks. Scalability of these models can be improved via use of sidechaining and blockchain sharding, that allows for smaller sized chains, thereby reducing the delay needed for mining and verification. To summarize from above is about delay in trust based routing,Incentive mechanism for aggregate Privacy data from Crowdsourced nodes,Issues related to Data attack and Data integrity and also introducing deep learning startegies .

Approaches like data slicing [33], attribute based file encryption [34], local randomization with alternating direction method of multipliers [35], centralized key management [36], diversity maximization techniques [37],

attribute-based entity transformation [38], and WiFi fingerprinting [39] can also be used. All these models have limited applicability, and can be used only for solving a particular set of privacy issues. Moreover, these models have low computational complexity, which reduces the delay of processing, but require higher energy, and have low accuracy when compared with blockchain, differential privacy, incentive-based [40], and consensus-based [41] models. Thus, it can be observed that machine learning, differential privacy, auction-based, chaotic & pseudorandom models outperform other models in terms of the overall performance of privacy preservation and network QoS. A statistical evaluation of these models, along with their comparison can be observed in the next section. This will assist system designers to select the best suited models for their particular application depending on model performance metrics. To summarise from above is about Attribute-based encryption , validating diversity in data management, Privacy preservation in WiFi fifingerprintingaccess model and Blockchain

3. Methodology of Research

Broadcast communication channels transact the group of user information data packets which may increase probability of spoofing and other network attacks and also privacy breach.Exisitng Models are available but compromise on communication QoS in order to enhance performance of Encryption.Hence Intended Framework is proposed for privacy preservation and Hybrid encryption .

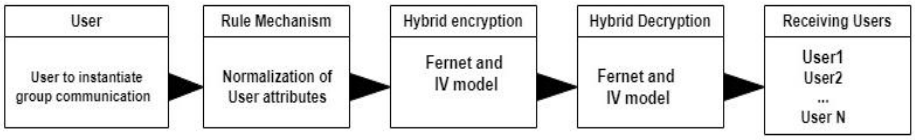

Fig. 2. Proposed Model for Privacy Preservation and Hybrid Encryption

From Fig.2. The User generates a communication request to the group of users where the request is to normalise the user's attributes which have to be preserved during communication with the help of a defined Rule mechanism. This request is fed to a Hybrid encryption model where it consists of two methods one is the Fernet Model and the second is IV model; during this process attributed -based key is generated which further assists in decrypting the communication in the Hybrid decryption Model. Further, the model is also preserved by differential Privacy.

4. Empirical Analysis

Each of the compared models is evaluated on different network architectures and under different simulation & deployment conditions. Thus, in order to analyze these models, their performance metrics were converted into fuzzy ranges of very low (VL), low (L), medium (M), high (H), and very high (VH). These ranges were observed from the comparative analysis mentioned in the referred texts, and by comparing these values with similar privacy models. Based on this evaluation, privacy level (P), end-to-end delay (D), computational complexity (CC), energy consumption (E), and area of application (A), were estimated for the reviewed models. These estimations are tabulated in Table 1, and are further analyzed on a per-parameter basis.

Table 1. Performance evaluation of different privacy preservation models

Method	**P**	**D**	**CC**	**E**	**A**
LEACH with Dummies [1]	M	H	H	M	General
EPPA [2]	L	M	M	L	General
ECC with key-exchange [3]	M	H	VH	M	IoT
Bayesian Game Theory [4]	H	H	H	H	IoT
Federated ML [5]	H	VH	VH	H	Medical Imaging
Crowd-sourced differential privacy [6]	M	M	H	H	General
Boneh-Goh-Nissim [7]	L	M	M	L	General
Paillier model [8]	M	H	M	L	IoT
Personal RR [9]	M	M	H	M	General
Conventional RR [9]	L	L	H	H	General
Semantic PoI [10]	H	M	H	H	MIoT
Co-operative model [11]	M	M	M	M	MIoT
Crowd-sensing with mobile nodes [12]	M	H	L	L	MIoT
MTL [13]	L	L	L	L	General
Light weight crypto [14]	M	M	H	M	MIoT
Certificate-less aggregate signature [15]	H	H	H	H	VANet
Chebyshev chaotic maps [16]	H	M	H	H	MIoT
RTT [17]	L	L	VL	L	IoT
Pseudo-anonymous auth [18]	H	H	VH	M	General
Voronoi with dummies [19]	M	VH	H	L	General

Safe partitioning [20]	M	H	H	M	General
Bilateral privacy preservation [21]	M	L	L	H	General
Auction based [23]	H	H	H	H	General
Distributed data privacy [24]	M	M	M	H	IoT
Collaborative computing [25]	M	H	H	M	General
Differential Privacy [26]	H	H	M	H	MIoT
Blockchain with MCDM & SAW [27]	VH	H	VH	H	MIoT
Trust based [28]	M	M	H	H	IoT
Aggregative privacy preservation [29]	M	L	M	M	General
Blockchain with DL [30]	VH	H	VH	VH	General
Smart contracts [31]	H	H	H	VH	General
Encrypted blockchain [32]	H	VH	VH	VH	General
Data slicing [33]	M	M	H	M	General
Attribute based file encryption [34]	L	H	H	H	General
Local randomization [35]	M	H	M	H	General
Centralized key management [36]	H	H	H	M	General
Diversity maximization [37]	H	M	H	H	General
Attribute-based entity modification [38]	M	M	H	H	General
WiFi fingerprinting [39]	L	M	M	H	MIoT
Incentive based [40]	H	H	H	M	VANet
Consensus based [41]	H	H	VH	M	General

From Table 1 it can be observed that privacy preservation models are evaluated for IoT, MIoT, and General-purpose wireless networks (including mobile Adhoc networks, vehicular Adhoc networks, etc.). Categorisation of IoT and MIoT is separately done because MIoT belongs to the class of low-power IoT networks. Each model is estimated for individual application areas, and their performance estimation is performed. For instance, the privacy performance of General-purpose wireless networks can be observed in Fig.3.

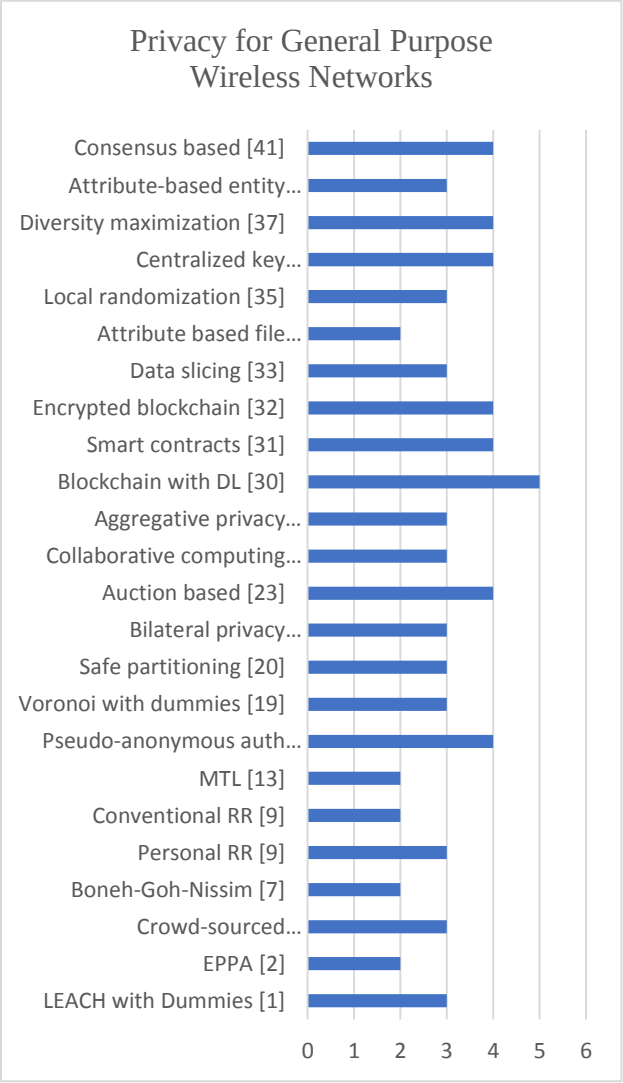

Fig. 3. Privacy comparison for General Purpose Wireless Networks

From this comparison, it can be observed that Blockchain with DL [30], Consensus-based [41], and Pseudo-anonymous auth [18] outperform other models for General purpose wireless networks. Similarly, the delay performance can be observed in Fig.4. as follows,

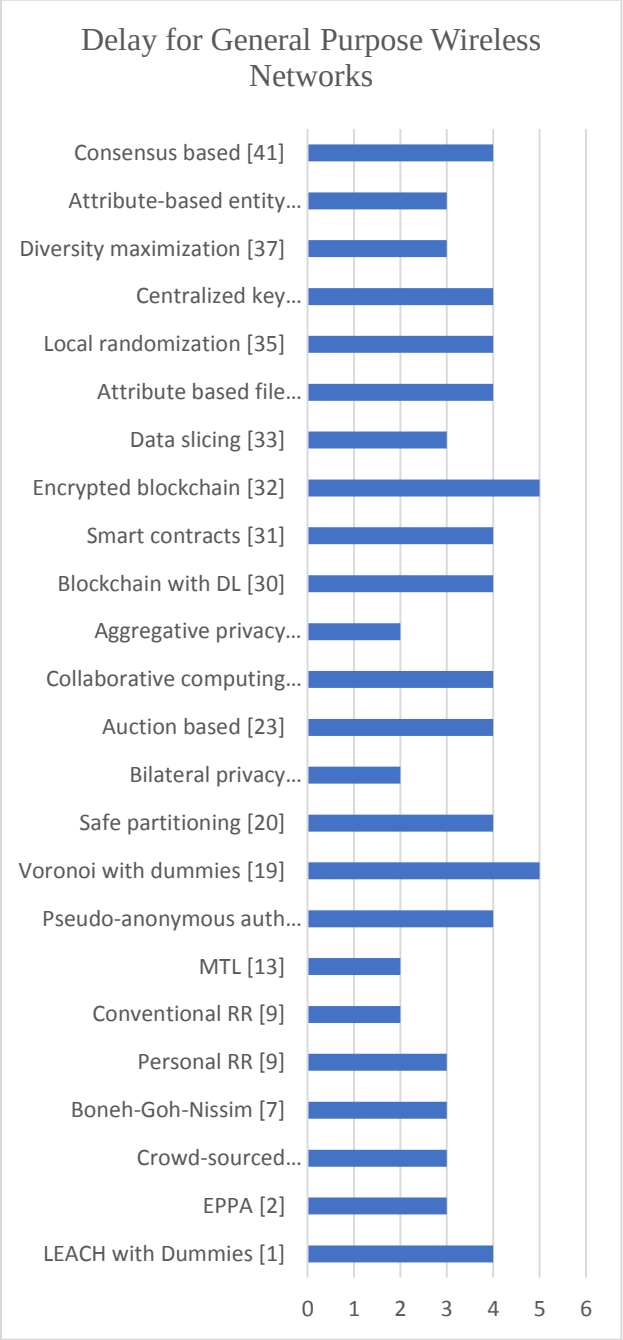

Fig. 4. Delay comparison for General Purpose Wireless Networks

From this comparison, it can be observed that Conventional RR [9], MTL [13], and Diversity maximisation [37] outperform other models for General purpose wireless networks. Similarly, the computational complexity performance can be observed in Fig.5. as follows,

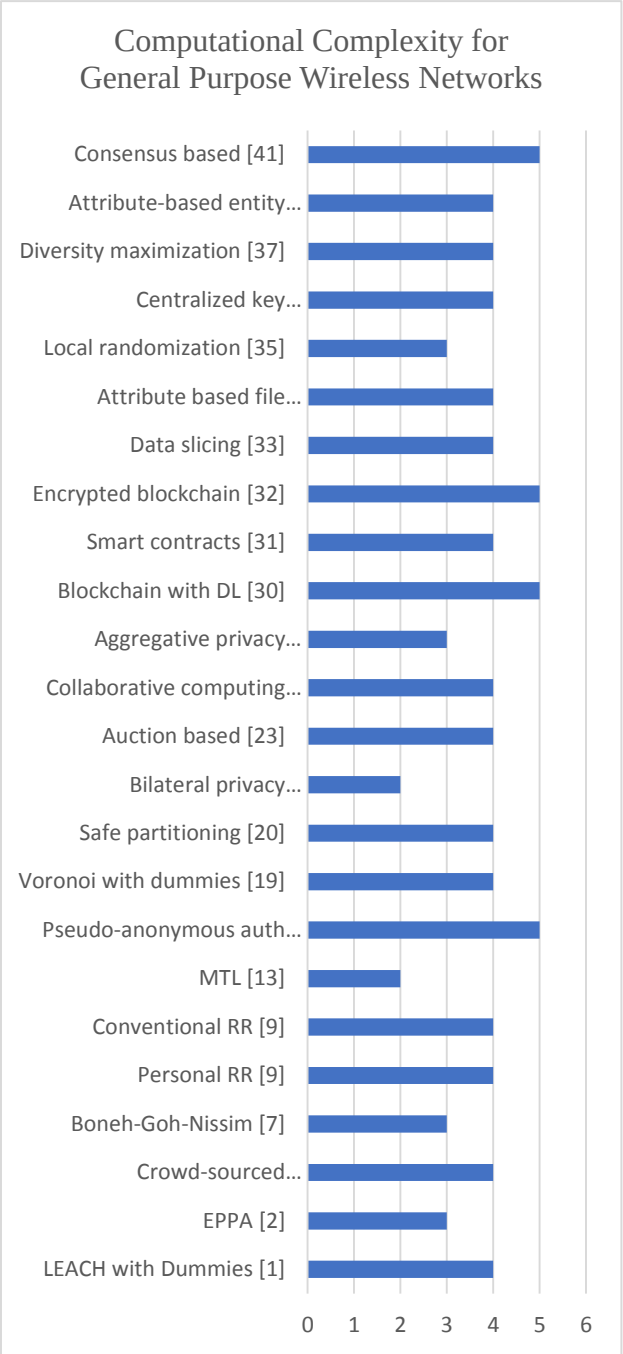

Fig. 5. Computational complexity comparison for General Purpose Wireless Networks

This comparison shows that MTL [13] and Local randomisation [35] outperform other models for General purpose wireless networks. Similarly, the energy requirement can be observed in Fig.6. from where it can be observed that MTL [13], EPPA [2], Boneh-Goh-Nissim [7], and Consensus-based [41] outperform other models for General purpose wireless networks.

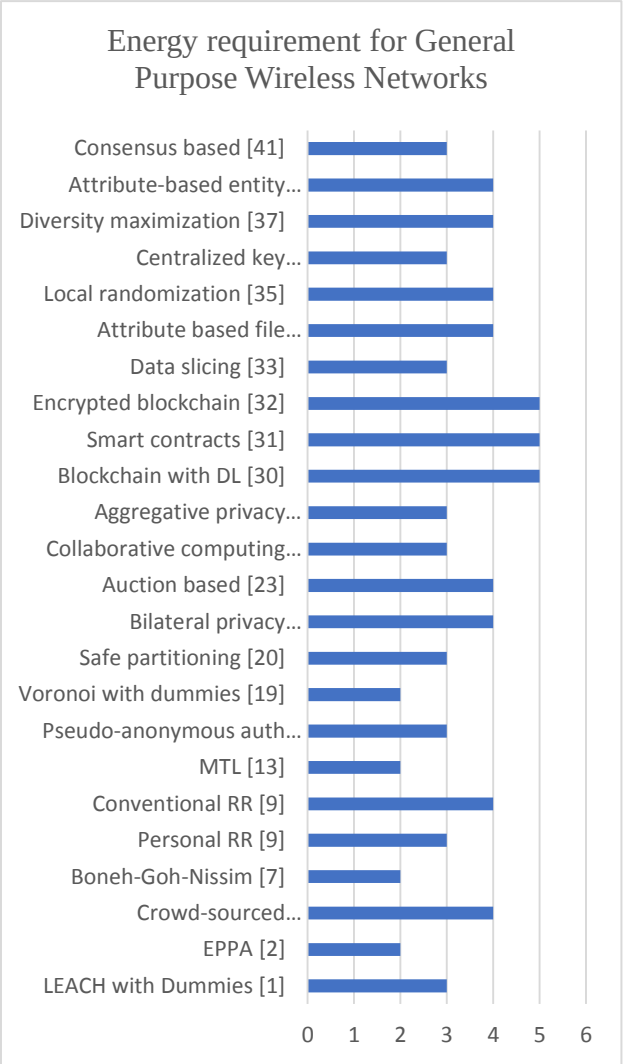

Fig. 6. Energy requirement comparison for General Purpose Wireless Networks

Continuing this comparison for MIoT, the privacy performance can be observed from Fig.7. as follows,

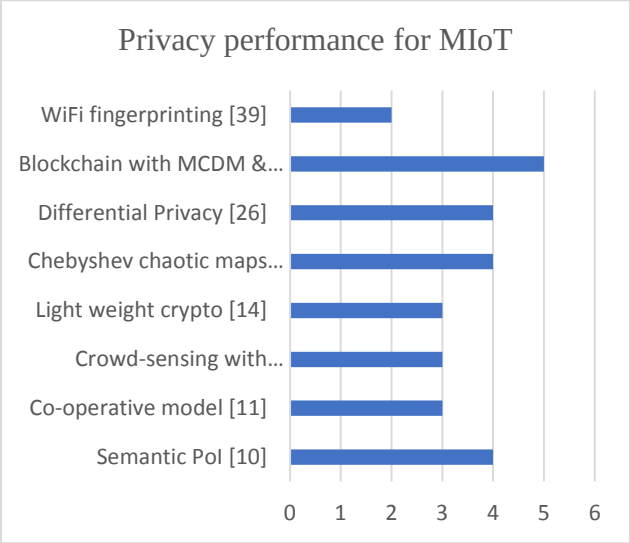

Fig. 7. Privacy comparison for MIoT Networks

From Fig.7. it can be observed that Blockchain with MCDM & SAW [27] outperform other models. Similarly, the delay performance can be observed in Fig.8. as follows,

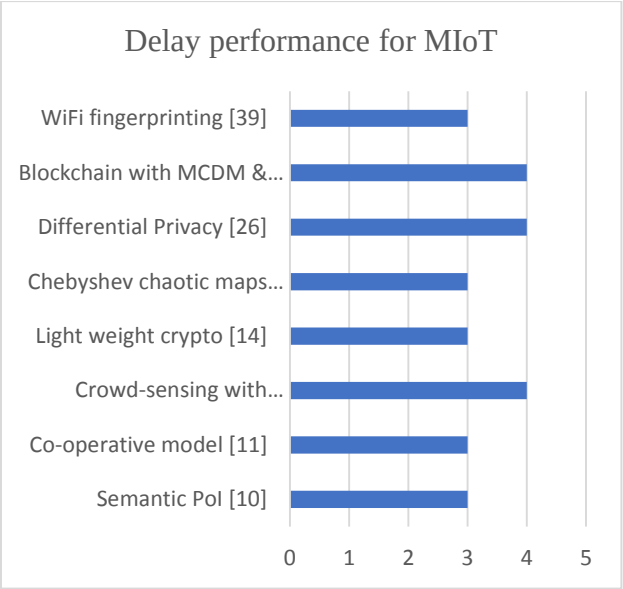

Fig. 8. Delay comparison for MIoT Networks

From Fig.8. it can be observed that Blockchain with Semantic PoI [10] outperforms other models. Similarly, the computational complexity performance can be observed from Fig.9. as follows,

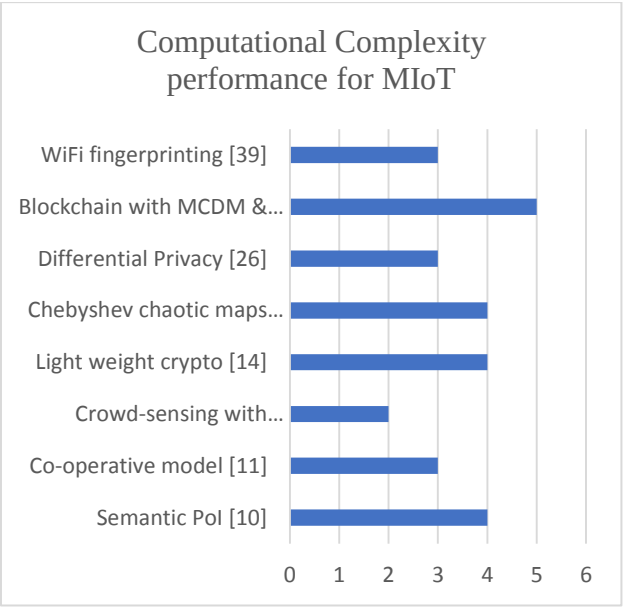

Fig. 9. Computational complexity comparison for MIoT Networks

From Fig.9. it can be observed that Crowd-sensing with mobile nodes [12] outperform other models. Similarly, the energy requirement can be observed from Fig.10. as follows,

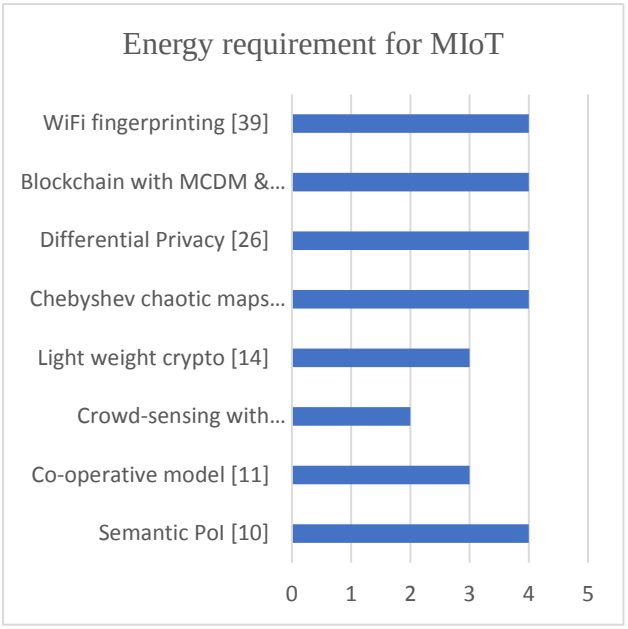

Fig.10.Energy requirement for MIoT Networks

From Fig.10. it can be observed that Crowd-sensing with mobile nodes [12] outperform other models. Similarly, the privacy performance for IoT networks can be observed from Fig.11. as follows,

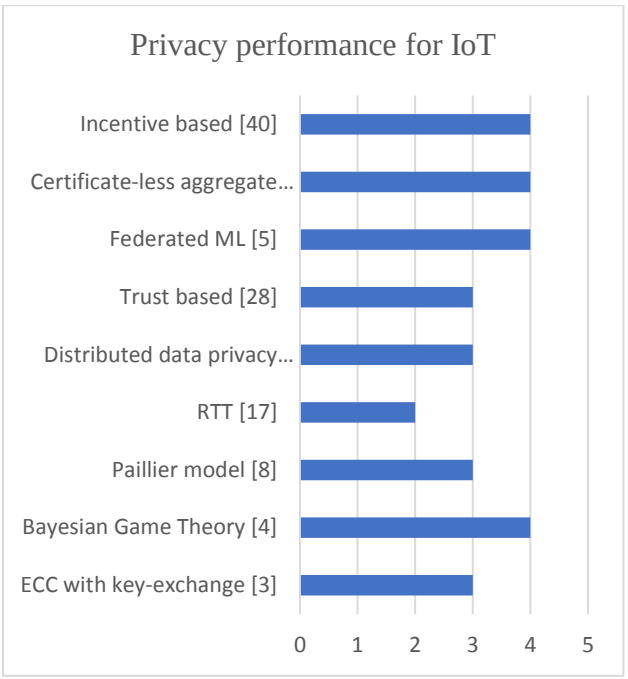

Fig.11. Privacy comparison for IoT Networks

From Fig.11 it can be observed that Bayesian Game Theory [4] outperform other models. Similarly, the delay performance for IoT networks can be observed in Fig.12. as follows,

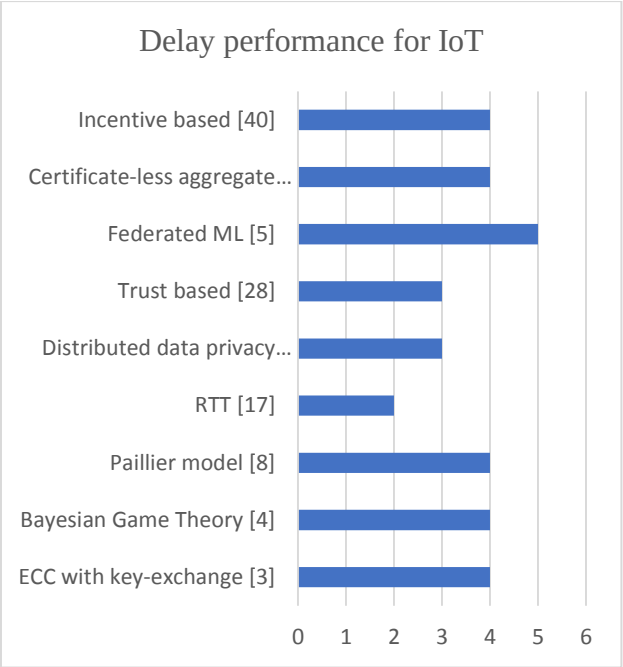

Fig. 12. Delay comparison for IoT Networks

From Fig.12. it can be observed that RTT [17], and Distributed data privacy [24] outperform other models. Similarly, the computational complexity performance for IoT networks can be observed from Fig.13. as follows,

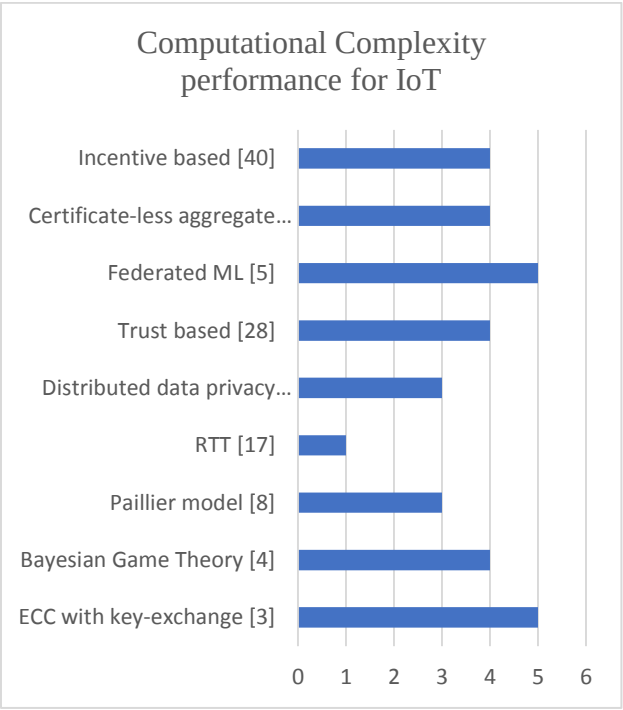

Fig. 13. Computational complexity comparison for IoT Networks

From Fig.13. it can be observed that RTT [17] outperform other models. Similarly, the Energy requirements for IoT networks can be observed from Fig.14. as follows,

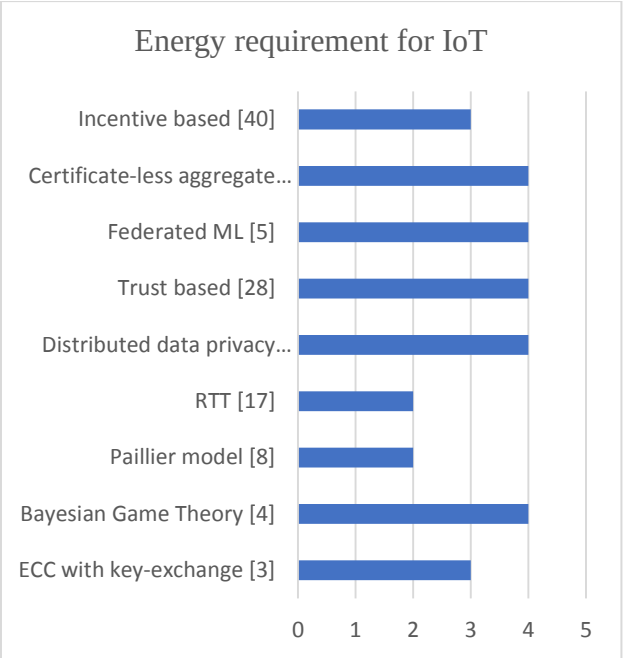

Fig. 14. Energy requirement for IoT Networks

From Fig.14. it can be observed that RTT [17] outperform other models. Thus, researchers and system designers can select any application, and select a privacy model based on their requirements using this analysis.

5. Conclusion and Future Scope

Privacy and security are two inter-twined pillars of any wireless network that often cross-paths regarding internal network functioning.Privacy is a claim of individual , groups or institution to determine for themselves when, how and to what extent information about them is to be communicated in Network. Privacy is also a choice of an individual or group to seclude information about them and thereby reveal them selectively. Since Privacy is a multidomain task, sincere advancements like efficiency in hashing, secure routing, third-party data sharing, effectual authentication, data confidentiality, and source location privacy are been presented. The author has made sincere efforts to project Privacy models starting from Anonymization to Blockchain and various other inculcation of machine learning models.The empirical analysis shows that privacy preservation models for General-purpose wireless networks, IoT networks and MIoT networks are compared. This comparison is done regarding privacy level, processing delay, computational complexity, and energy efficiency. From this comparison it can be observed that, Blockchain with DL, Consensus-based, Diversity maximization Centralized key management, Encrypted blockchain, Smart contracts, Auction based, and Pseudo-anonymous auth, outperform other models for General purpose wireless networks in terms of privacy levels, while Conventional RR, MTL, Bilateral privacy preservation, Aggregative privacy preservation, EPPA, Boneh-Goh-Nissim, Crowd-sourced differential privacy, Personal RR, Data slicing, Attribute-based entity modification, and Diversity maximization outperform other models in terms of delay performance, similarly, MTL, Bilateral privacy preservation, Aggregative privacy preservation, EPPA, Boneh-Goh-Nissim, and Local randomization outperform other models in terms of computational complexity, and finally, MTL, EPPA, Boneh-Goh-Nissim, Voronoi with dummies, Aggregative privacy preservation, Personal RR, Data slicing, LEACH with Dummies, Safe partitioning, Collaborative computing, Centralized key management, Pseudo-anonymous auth, and Consensus-based outperform other models in terms of energy efficiency.

While for MIoT networks, Blockchain with MCDM & SAW, Semantic PoI, Chebyshev chaotic maps, and Differential Privacy outperform other models in terms of privacy performance. In contrast, Blockchain with Semantic PoI, Chebyshev chaotic maps, Cooperative model, Lightweight crypto, and WiFi fingerprinting outperform other models in terms of delay performance, Crowd-sensing with mobile nodes, Co-operative model, WiFi fingerprinting, Differential Privacy outperform other models in terms of computational complexity. Finally, Crowd-sensing with mobile nodes, a Co-operative model, and Lightweight crypto outperform other models regarding energy requirements.

Similarly, for IoT networks, Bayesian Game Theory, Federated ML, Certificate-less aggregate signature, and Incentive based outperform other models in terms of privacy performance, while RTT, Distributed data privacy, and Trust based outperform other models in terms of delay performance, and RTT, Distributed data privacy, and Paillier model outperform other models in terms of computational complexity, finally, RTT, Paillier model, Incentive-based, and ECC with key-exchange outperform other models in terms of energy requirements. This paper is a review paper,

and the outcome of the paper is for analysing the best-fitted privacy model. Paper also targets researchers who wish to work in securing communications, Privacy, Security and for lifelong learning.

Future Scope

In future, it is recommended that deep learning blockchain solutions with sidechains and reinforcement learning must be used for improving the efficiency of privacy preservation techniques. Researchers can also use a combination of RTT with Pallier, and other cryptosystems to improve the performance of attack resilience and increase awareness towards a large number of security attacks. Furthermore, researchers can augment the parameters of the most efficient approaches for a given domain and try to apply them to other domains to validate their security performance. Researchers must also perform inter-domain privacy checks to reduce dependency on a single model and improve the effectiveness & QoS of hybrid security & privacy models.

References

[1] Dou, H., Chen, Y., Yang, Y. et al. A secure and efficient privacy-preserving data aggregation algorithm. J Ambient Intell Human Comput (2021). https://doi.org/10.1007/s12652-020-02801-6

[2] Xie, Q., Li, K., Tan, X. et al. A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city. J Wireless Com Network 2021, 119 (2021). https://doi.org/10.1186/s13638-021-02000-7

[3] Renwan Bi, Qianxin Chen, Lei Chen, Jinbo Xiong, Dapeng Wu, "A Privacy-Preserving Personalized Service Framework through Bayesian Game in Social IoT", Wireless Communications and Mobile Computing, vol. 2020, Article ID 8891889, 13 pages, 2020. https://doi.org/10.1155/2020/8891889

[4] Kaissis, G., Makowski, M., Rückert, D., & Braren, R. (2020). Secure, privacy-preserving and federated machine learning in medical imaging. Nature Machine Intelligence, 2, 305-311.

[5] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin and K. Ren, "Real-Time and Spatio-Temporal Crowd-Sourced Social Network Data Publishing with Differential Privacy," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 591-606, 1 July-Aug. 2018, doi: 10.1109/TDSC.2016.2599873.

[6] C. Niu, Z. Zheng, F. Wu, X. Gao and G. Chen, "Achieving Data Truthfulness and Privacy Preservation in Data Markets," in IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 1, pp. 105-119, 1 Jan. 2019, doi: 10.1109/TKDE.2018.2822727.

[7] Babu, S.S., Balasubadra, K. Revamping data access privacy preservation method against inside attacks in wireless sensor networks. Cluster Comput 22, 65–75 (2019). https://doi.org/10.1007/s10586-018-1706-1

[8] H. Song, T. Luo, X. Wang and J. Li, "Multiple Sensitive Values-Oriented Personalized Privacy Preservation Based on Randomized Response," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2209-2224, 2020, doi: 10.1109/TIFS.2019.2959911.

[9] G. Qiu, D. Guo, Y. Shen, G. Tang and S. Chen, "Mobile Semantic-aware Trajectory for Personalized Location Privacy Preservation," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3016466.

[10] H. Liu, X. Yao, T. Yang and H. Ning, "Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-Based Smart Health," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1352-1362, April 2019, doi: 10.1109/JIOT.2018.2843561.

[11] J. Ni, K. Zhang, Q. Xia, X. Lin and X. S. Shen, "Enabling Strong Privacy Preservation and Accurate Task Allocation for Mobile Crowdsensing," in IEEE Transactions on Mobile Computing, vol. 19, no. 6, pp. 1317-1331, 1 June 2020, doi: 10.1109/TMC.2019.2908638.

[12] Z. Xu and A. A. Julius, "Robust Temporal Logic Inference for Provably Correct Fault Detection and Privacy Preservation of Switched Systems," in IEEE Systems Journal, vol. 13, no. 3, pp. 3010-3021, Sept. 2019, doi: 10.1109/JSYST.2019.2906160.

[13] Shuai, M., Xiong, L., Wang, C. and Yu, N. (2020), Lightweight and privacy-preserving authentication scheme with the resilience of desynchronisation attacks for WBANs. IET Inf. Secur., 14: 380-390. https://doi.org/10.1049/iet-ifs.2019.0491

[14] Kamil, IA, Ogundoyin, SO. On the security of privacy-preserving authentication scheme with full aggregation in vehicular ad hoc network. Security and Privacy. 2020; 3:e104. https://doi.org/10.1002/spy2.104

[15] Deebak, B.D., Al-Turjman, F. & Nayyar, A. Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. Multimed Tools Appl 80, 17103–17128 (2021). https://doi.org/10.1007/s11042-020-10134-x

[16] Roy, A.K. and Khan, A.K. (2020), Privacy preservation with RTT-based detection for wireless mesh networks. IET Inf. Secur., 14: 391-400. https://doi.org/10.1049/iet-ifs.2019.0492

[17] S. Chavhan, D. Gupta, C. B. N, A. Khanna and J. J. P. C. Rodrigues, "Agent Pseudonymous Authentication-Based Conditional Privacy Preservation: An Emergent Intelligence Technique," in IEEE Systems Journal, vol. 14, no. 4, pp. 5233-5244, Dec. 2020, doi: 10.1109/JSYST.2020.2994631.

[18] Zhang, L., Chen, M., Liu, D. et al. A ε-sensitive indistinguishable scheme for privacy preserving. Wireless Netw 26, 5013–5033 (2020). https://doi.org/10.1007/s11276-020-02378-0

[19] B. Safia and C. Yacine, "Privacy Preservation in Social Networks Sequential Publishing," 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), 2018, pp. 732-739, doi: 10.1109/AINA.2018.00110.

[20] Z. Zhang, H. Zhang, S. He and P. Cheng, "Bilateral Privacy-Preserving Utility Maximization Protocol in Database-Driven Cognitive Radio Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 2, pp. 236-247, 1 March-April 2020, doi: 10.1109/TDSC.2017.2781248.

[21] S. M. Errapotu et al., "Bid Privacy Preservation in Matching-Based Multiradio Multichannel Spectrum Trading," in IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8336-8347, Sept. 2018, doi: 10.1109/TVT.2018.2845798.

[22] Q. Xu, Z. Su, M. Dai and S. Yu, "APIS: Privacy-Preserving Incentive for Sensing Task Allocation in Cloud and Edge-Cooperation Mobile Internet of Things With SDN," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 5892-5905, July 2020, doi: 10.1109/JIOT.2019.2954380.
[23] Du, Jun & Jiang, Chunxiao & Gelenbe, Erol & Xu, Lei & Li, Jianhua & Ren, Yong. (2018). Distributed Data Privacy Preservation in IoT Applications. IEEE Wireless Communications. 25. 68-76. 10.1109/MWC.2017.1800094.
[24] X. Wang, J. He, P. Cheng and J. Chen, "Privacy Preserving Collaborative Computing: Heterogeneous Privacy Guarantee and Efficient Incentive Mechanism," in IEEE Transactions on Signal Processing, vol. 67, no. 1, pp. 221-233, 1 Jan.1, 2019, doi: 10.1109/TSP.2018.2880722.
[25] Hussain, Siam Umar & Koushanfar, Farinaz. (2016). Privacy preserving localization for smart automotive systems. 1-6. 10.1145/2897937.2898071.
[26] X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi and W. Dou, "A Blockchain-Powered Crowdsourcing Method With Privacy Preservation in Mobile Environment," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1407-1419, Dec. 2019, doi: 10.1109/TCSS.2019.2909137.
[27] X. Shi, F. Tong, W. -A. Zhang and L. Yu, "Resilient Privacy-Preserving Distributed Localization Against Dishonest Nodes in Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 9214-9223, Sept. 2020, doi: 10.1109/JIOT.2020.3004709.
[28] Z. Zhang, S. He, J. Chen and J. Zhang, "REAP: An Efficient Incentive Mechanism for Reconciling Aggregation Accuracy and Individual Privacy in Crowdsensing," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 12, pp. 2995-3007, Dec. 2018, doi: 10.1109/TIFS.2018.2834232.
[29] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan and K. R. Choo, "A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5110-5118, Aug. 2020, doi: 10.1109/TII.2019.2957140.
[30] S. Zhu, H. Hu, Y. Li and W. Li, "Hybrid Blockchain Design for Privacy Preserving Crowdsourcing Platform," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 26-33, doi: 10.1109/Blockchain.2019.00013.
[31] S. Linoy, H. Mahdikhani, S. Ray, R. Lu, N. Stakhanova and A. Ghorbani, "Scalable Privacy-Preserving Query Processing over Ethereum Blockchain," 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 398-404, doi: 10.1109/Blockchain.2019.00061.
[32] Yao, Lin & Chen, Zhenyu & Hu, Haibo & Wu, Guowei & Wu, Bin. (2020). Sensitive attribute privacy preservation of trajectory data publishing based on l-diversity. Distributed and Parallel Databases. 1-27. 10.1007/s10619-020-07318-7.
[33] Shabbir, Maryam & Shabbir, Ayesha & Iwendi, Celestine & Javed, Abdul Rehman & Rizwan, Muhammad & Herencsar, Norbert & Lin, Chun-Wei. (2021). Enhancing Security of Health Information Using Modular Encryption Standard in Mobile Cloud Computing. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3049564.
[34] Wang, Xin & Ishii, Hideaki & Linkang, Du & Cheng, Peng & Chen, Jiming. (2019). Privacy-preserving Distributed Machine Learning via Local Randomization and ADMM Perturbation.
[35] Lu, Xiuqing & Pan, Zhenkuan & Xian, Hequn. (2020). An efficient and secure data sharing scheme for mobile devices in cloud computing. Journal of Cloud Computing. 9. 10.1186/s13677-020-00207-5.
[36] Razaullah Khan, Xiaofeng Tao, Adeel Anjum, Haider Sajjad, Saif ur Rehman Malik, Abid Khan, Fatemeh Amiri, "Privacy Preserving for Multiple Sensitive Attributes against Fingerprint Correlation Attack Satisfying c-Diversity", Wireless Communications and Mobile Computing, vol. 2020, Article ID 8416823, 18 pages, 2020. https://doi.org/10.1155/2020/8416823
[37] Yujiao Song, Hao Wang, Xiaochao Wei, Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud", Security and Communication Networks, vol. 2019, Article ID 3249726, 9 pages, 2019. https://doi.org/10.1155/2019/3249726
[38] G. Zhang, A. Zhang, P. Zhao and J. Sun, "Lightweight Privacy-Preserving Scheme in Wi-Fi Fingerprint-Based Indoor Localization," in IEEE Systems Journal, vol. 14, no. 3, pp. 4638-4647, Sept. 2020, doi: 10.1109/JSYST.2020.2977970.
[39] G. Sun, S. Sun, H. Yu and M. Guizani, "Toward Incentivizing Fog-Based Privacy-Preserving Mobile Crowdsensing in the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4128-4142, May 2020, doi: 10.1109/JIOT.2019.2951410.
[40] C. Zhao, J. Chen, J. He and P. Cheng, "Privacy-Preserving Consensus-Based Energy Management in Smart Grids," in IEEE Transactions on Signal Processing, vol. 66, no. 23, pp. 6162-6176, 1 Dec.1, 2018, doi: 10.1109/TSP.2018.2872817.

Authors' Profiles

Ms.Namrata Jiten Patel PhD Research Scholar in Computer Engineering at DY Patil Deemed to University and Assistant professor in SIES Graduate School of Technology undertaken various subjects like Discrete Mathematics, Computer Network , Information Security, and Operating System.

Dr.Ashish Jadhav is a Head of the IT Department, Professor and Dean of Industrial Consultancy and Research at RAIT.Ph.D.(Electrical Engineering)IIT Kanpur, M.Tech (BITS Pillani),BE(RAIT).With 7 years of Industrial Background as a Principal Architect in the company IGATE .

How to cite this paper: Namrata J. Patel, Ashish Jadhav, "A Systematic Review of Privacy Preservation Models in Wireless Networks", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.2, pp. 7-22, 2023. DOI:10.5815/ijwmt.2023.02.02