International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

Empirical Analysis of Privacy Preservation Models for Cyber Physical Deployments from a Pragmatic Perspective

Sarita M. Motghare[1], Dr. Pramod S. Nair[2]
[1]Ph.D. Scholar, Medi-Caps University,
Indore, MP, India
saritamotghare@gmail.com
[2]Professor, Computer Science & Engineering, Medi-Caps University,
Indore, MP, India
pramods.nair@medicaps.ac.in

Abstract: The difficulty of privacy protection in cyber-physical installations encompasses several sectors and calls for methods like encryption, hashing, secure routing, obfuscation, and data exchange, among others. To create a privacy preservation model for cyber physical deployments, it is advised that data privacy, location privacy, temporal privacy, node privacy, route privacy, and other types of privacy be taken into account. Consideration must also be given to other types of privacy, such as temporal privacy. The computationally challenging process of incorporating these models into any wireless network also affects quality of service (QoS) variables including end-to-end latency, throughput, energy use, and packet delivery ratio. The best privacy models must be used by network designers and should have the least negative influence on these quality-of-service characteristics. The designers used common privacy models for the goal of protecting cyber-physical infrastructure in order to achieve this. The limitations of these installations' interconnection and interface-ability are not taken into account in this. As a result, even while network security has increased, the network's overall quality of service has dropped. The many state-of-the-art methods for preserving privacy in cyber-physical deployments without compromising their performance in terms of quality of service are examined and analyzed in this research. Lowering the likelihood that such circumstances might arise is the aim of this investigation and review. These models are rated according to how much privacy they provide, how long it takes from start to finish to transfer data, how much energy they use, and how fast their networks are. In order to maximize privacy while maintaining a high degree of service performance, the comparison will assist network designers and researchers in selecting the optimal models for their particular deployments. Additionally, the author of this book offers a variety of tactics that, when used together, might improve each reader's performance. This study also provides a range of tried-and-true machine learning approaches that networks may take into account and examine in order to enhance their privacy performance.

Keywords: Privacy, network, QoS, machine learning, location, temporal, data

I. Introduction

In order to ensure privacy in cyber physical installations, it is important to have node anonymity, effective access control, high efficiency authentication, data confidentiality, source location privacy, and sink location privacy. The network designers must simulate efficient data and route management solutions in order to successfully adhere to these privacy requirements. These tactics are used after a comprehensive threat assessment. Eavesdropping traffic analysis, query reveal analysis, authentication testing, privacy monitoring, impersonation, and other actions could be a part of this evaluation. In contrast to security, which typically focuses on ensuring that data communication between nodes, physical security, external attacks, internal node functioning, and so forth are all carried out without any disruption, privacy is concerned with the selective sharing of data between different entities of a network. One of the criteria that may be used to categorize network privacy models is data privacy. In this paradigm, information is shared through multiple network entities in a manner that only the intended recipients may access it. Non-intended parties, including attackers and other nodes, are unable to understand the data even if they have

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

access to one or more data components. Data belonging to a single node is only accessible by that node or the shared parties, ensuring user privacy. Since the data is secured, no other node may access it or share it with any other nodes. Location privacy is the protection of a node's position such that it is impossible for other nodes to ascertain its specific location without the node's prior consent. In order to safeguard user privacy, data must be gathered in a way that restricts access to the final data values to the nodes that are intended to view them. Any other kind of privacy, such as holistic, trajectory, and so forth, may also be used depending on the network.

Most of these privacy-preserving algorithms use graph-based anonymization methods, including, for example, l-diversity and k-anonymity. In an attempt to make networks more private, researchers have created a wide range of privacy-protecting algorithms throughout the years. These techniques work regardless of whether an attacker has access to all or some of the data because they alter it in a manner that makes it worthless to them. Due to this characteristic, these models are less effective for networks that are moderately large to extremely huge. To achieve high levels of data access security in this setting, data confidentiality must be protected while keeping the data usable. In order to lessen the effects of this flaw, network infrastructure is using blockchain-based privacy mechanisms. These models aim to do data mixing, which involves combining and merging several blockchain transactions to mask the data's original identity. Both attribute-identity and attribute-privacy may be preserved using encryption, which may include the usage of either public or private keys. Before data is published or broadcast on the network, any information that may be used to identify a particular person is erased via the process of anonymization. Private contracts, in which transactional data is included and programmable contracts are established between communication nodes. private agreements. Differential privacy entails putting data into a noisy format that makes it difficult to decode for any nodes that are trying to attack it but simple for nodes that are believed to be genuine.

These features have led to an increase in the adoption of privacy models created on blockchains by both academics and network developers. You will discover a summary of these techniques in the next section of this book, which will be followed by a thorough examination of their effectiveness and a comparison with the reviewed protocols. This will make it easier for researchers and network builders to choose the best combination of protocols for privacy protection in each of their individual deployments. This essay concludes with some insightful observations on the models that have been looked at and some recommendations on how to improve those models.

II. Literature Review

Since these models incorporate sensitive information like node locations, routing routes, data values, and other things, the network may benefit from models that protect privacy. A high level of trust is included into the talks that take place throughout the network since this information is sent in a way that is not understandable to any hostile nodes. The authors of the research [1] propose a network that is sensitive to privacy issues and uses a combination of data slicing, cluster head selection using Low Energy Adaptive Clustering Hierarchy (LEACH), and the creation of fictitious packets to enhance users' degree of privacy. Because of this, the model has a low latency and strong privacy performance, but due to the creation of fictitious packets, it has a high computational cost. The suggested privacy-preserving data aggregation technique, commonly known as the SECPDA algorithm, performs better in terms of privacy than both the CPDA and the integrity learning with clustering CPDA (ILCCPDA) algorithms. The SECPDA method, in contrast, has a poor throughput, a moderate energy consumption, and a considerable latency. An energy-efficient, privacy-preserving data aggregation method based on slicing or the EPPA model is suggested by the study described in [2]. This protocol aims to minimize the wait time. The model aims to reduce the number of slices produced during communication by using a Euclidean-based decomposition. In turn, this results in a substantial decrease in computational overheads and a decrease in end-to-end communication delay. Additionally, it uses the MPPA multi-function privacy-preserving data aggregation protocol to gather data in a way that is tailored for a variety of uses. However, by doing reverse engineering on sliced data packets and utilizing cryptanalysis, it is feasible to track the model. The model is very secure against a few types of attacks. Furthermore, the system lacks security components, which limits its capacity to preserve route and node privacy for extensive deployments. As suggested in [3], which suggests a privacy preservation and encryption strategy that utilizes ECC, this issue may be solved by employing an effective key exchange and a high-performance data encryption model. [3] contains these solutions. The idea is able to provide large-scale authentication in addition to anonymity since it uses hashing and other efficient key exchange methods. This model's performance analysis shows that it has a very high degree of security, but it also has a very high level of computational complexity, which decreases both its energy efficiency and its capacity to adapt to more data kinds.

Researchers have quantized user preferences as fuzzy values in [4], which allows the reader to see a dynamic privacy protection technique. The algorithm receives the help it needs from these fuzzy values to adopt attributed-based privacy preservation

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

models that are measured using Shannon information entropy. The system model that will be utilized to execute this recommended solution, which entails scanning several attributes in accordance with the user's specified preferences, is shown in Figure 1. The algorithm then applies normalization and rules based on these numerous attributes to categorize the user as falling into one of "M" types of categories.

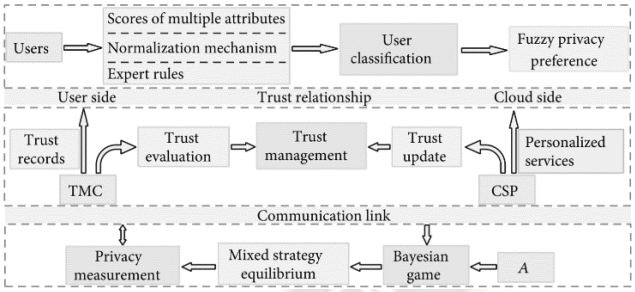

Figure 1. Attribute based privacy preservation [4]

Each of these "M" types of classes are decided by the nodes' past performance, and the model's capacity to provide high levels of privacy is made feasible by the combination of mixed strategy equilibrium and Bayesian game theory. The Shannon model is used to assess these privacy levels, and the findings are then sent back into the system for internal adjustment. This modification results in a better privacy model via parameter tinkering. The model that was provided exhibits a high degree of privacy performance, however it requires a large delay due to privacy's gradual advancements. Its performance in delivering packets is merely mediocre, and its energy efficiency is subpar as a consequence of the ongoing model tuning process. Such high privacy and moderate performance models may be utilized for high security applications like medical image processing, as illustrated in [5], where federated machine learning is used for low speed and high privacy performance. The study provided in [6] provides a privacy paradigm that uses differential privacy together with crowd-sourced data dissemination to reduce this delay. The model uses a number of approaches, including as data perturbation and filtering, adaptive sampling, dynamic grouping, and adaptive budget allocation, to generate a data stream that is both clean and highly private. As found, the model's high seclusion performance is a result of the use of differential privacy, dynamic grouping, recurrent neural networks (RNNs), and dynamic programming. However, RNN and other computationally intensive submodels have significantly improved the network's throughput, energy efficiency, and latency. This drastically limits its performance for low power cyber physical setups. According to the study discussed in [7], a high-speed paradigm for data privacy that uses both Boneh-Goh-Nissim homo-morphic encryption and fake identities is suggested. To overcome this disadvantage, this is done. The approach exhibits high quality of service criteria and is capable of preventing assaults on both identity and data. The Paillier cryptosystem may be used to protect anonymity in terms of place or time, as stated in [8], but these two things cannot be done using the model. The architecture that has been shown has good energy efficiency and is efficient at preventing internal network attacks, but it has a low throughput since the Paillier cryptosystem operates slowly. For tailored privacy preservation, researchers have used randomized responses in the work that is detailed in [9], which may be referred to in order to speed up privacy preservation systems. The tailored random response model helps to offer privacy at the node level, but nodes must furnish this algorithm with personally identifying information in order to keep their privacy. The methodology also has issues with its cold start, which implies that although conventional randomized replies (CRRs) are used to maintain general privacy for early data samples, personalized randomized answers (PPRs) are used to maintain individual privacy as more data is gathered. For the first privacy protection, this issue may be resolved by using timestamps and instantaneous state-based solutions. By reading [10], which explains how mobile nodes might use a semantically aware privacy model to keep their location hidden, one can obtain an understanding of such a system. The recommended method, which involves training a deep semantic model utilizing inputs like a trajectory database, points of interest (PoI), duration of stay, semantic categories, and more, is shown in Figure 2. This model can determine a node's present position as well as create an entirely anonymous fake location that the router may use for route estimations and other network-related tasks. The model may be extended so that it can handle a larger number of privacy preservation characteristics by training the semantic tree using datasets that are based on attributes. This model's delay performance is also quite subpar, although it may be improved by employing lightweight training models or hybrid computing models, as detailed in [11]. The researchers that worked on this project have put forward a cooperative privacy preservation strategy that takes use of space-aware edge computing. Although it has been shown that the approach can enable data-level privacy, it cannot be used with low-power remote devices since edge computing is needed. It is ideal for networks that function similarly to the internet of things since it has a high throughput and a low latency (IoT).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

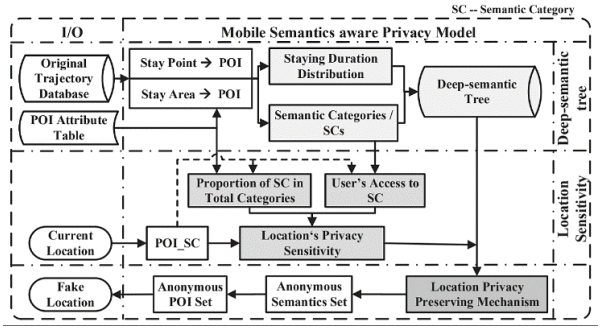

Figure 2. Semantic processing for location-based privacy preservation [10]

The edge computing approach might be replaced with a low power crowdsensing paradigm like the one in [12]. In this paradigm, privacy evaluations are conducted while processing capacity is borrowed from mobile nodes. The paradigm is ideally suited for low-power cyber-physical deployments due to its reasonable degree of computing complexity. However, since the model relies on crowdsourcing, it requires considerable amounts of computational delay, which might slow down the network if there are just a few available processing nodes. One option to lessen the effects of this restriction is to use metric temporal logic (MTL) [13], which includes assessing simple Boolean formulae in order to safeguard an individual's privacy. Although the model has a high responsiveness, it only performs modestly well in terms of privacy and can only be used to small to medium-sized networks. By including lightweight cryptographic modules, as suggested in [14], where desynchronization threats are prevented by incorporating kernel-level privacy, the usage of this strategy may be broadened. Although it has been shown that this system paradigm is highly helpful in scenarios requiring static networks, it does not permit routine changes in the topology of networks or internal reconfiguration. Additionally, this model must be evaluated for a larger network since it can only be utilized for a small network with a few connected nodes.

It is feasible to look into the aggregation process to reduce the quantity of input data, which will eventually boost the privacy models' internal running speed. In order to attain high levels of both speed and security, the study published in [15] offers a system similar to this one, in which certificateless aggregate signature is used for data exchange across nodes. The model creates pseudo-random key pairs and also makes use of partial key generation in order to fulfill this task. These characteristics work together to make the model immune to attacks from data forgery and espionage. The model's encryption and aggregation functions, however, need a large degree of processing time. As a consequence, the system's throughput decreases and its energy use increases. To make the system more resilient to more hits, it may be further expanded. This model and one similar to it may be found in [16]. The node data in this model is randomly generated using Chebyshev chaotic maps. The model must be assessed for both location and route privacy and can protect against any kind of data-related privacy assault. The simplicity of the Chebyshev model may significantly reduce the system's complexity. As a result, communication may be accomplished with a high throughput and little delay. The Chebyshev model just requires memory; hence it is appropriate for applications with enough storage since it only has one need. This restriction causes the model to have a greater energy need, making it unsuitable for applications with low power requirements. By using simpler models, such as those recommended in [17], which utilize the round-trip time (RTT) of packets for the evaluation of internal attacks, this limitation may be addressed. This type is very portable and may be used to establish any wireless network with loopback features. The system's incapability to detect variations un RTT values, however, restricts the accuracy of attack prediction. In order to increase the efficiency of attack detection, it is suggested that round-trip time (RTT) be combined with other network metrics.

Making ensuring that node identities are kept hidden is one of the most important things to accomplish when considering network privacy. In the study described in [18], a pseudonymous authentication-based paradigm for guaranteeing conditional privacy protection is proposed. The approach uses road side units (RSU) and takes into consideration specific time to live (TTL) information to produce pseudonymous IDs. This data is gathered by an agent, which is then enforced on the network to revoke access as soon as the TTL condition is met. Conditional privacy is implemented in this manner. With the addition of slicing and other data privacy techniques, the model may be enhanced to avoid attacks on data as well as attacks at the node and network level. These two talents are really outstanding. Although this architecture has good energy efficiency, its throughput performance is further hindered by the large delays required for identification. One way to get around this restriction and remove it completely from the system is to use differential privacy systems, like the one described in [19], which uses the Voronoi diagram to integrate dummies into the system. These dummies may conceal the data through location shifting, making the data more sensitive as a result. To add more features that safeguard users' privacy, the model must be extended. The system has been shown to have a low energy need, but it also has a significant delay and a subpar throughput due to the presence of several dummies. A model that uses a combination of safe partitioning and random (dummy) data insertion that is somewhat comparable to this one is shown in [20]. The recommended paradigm is used in order to protect temporal privacy. The content similarity is evaluated throughout this

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

procedure, and variance measurements are added to it to make it anonymous. The model has been verified on social networks, but in order to conduct a more thorough investigation, it must also be verified on other networks. There is still another tailored protocol utilized for cognitive radios, according to [21, 22]. This protocol maximizes the utility of both parties while protecting their privacy. The protocol may be developed to secure the privacy of additional characteristics in addition to users' location privacy. Although it has a low latency and fast throughput, its random deployment reduces its energy efficiency.

The authors of the study [23] propose a privacy preservation incentive system based on an auction, where software defined networks (SDNs) are utilized to auction off user data. This information is collected from Mobile IoT nodes and then applied to the network to offer differential privacy. Although the method may make better use of the CPU, it causes longer delays than random and price-aware allocation techniques. This causes it to operate more slowly, which reduces the quantity of information that can be transferred. According to the study in [24], a paradigm for distributed data privacy may be used to boost throughput. In accordance with this paradigm, location and data privacy of underlying nodes are protected by aggregating privacy information from several nodes. The network model's performance is acceptable when compared to models that do not use aggregation, but it lacks several privacy features and consumes more energy. Similar to the models shown in [25, 26], these models make use of collaborative computing and differential privacy to increase the amount of privacy provided to indoor location and data. These models' use is limited due to the lack of standardized frameworks for conveying data that has had its privacy safeguarded. This is because each protocol requires a different adaptation engine in order to be effectively implemented. According to the study discussed in [27], one way to improve the use of privacy models is to combine blockchain technology with crowdsourcing for distributed computing. The model combines multiple criteria decision making (MCDM) with simple additive weighting (SAW) to choose consensus methods that might result in reduced energy consumption, greater service time, and higher profitability when the network is in operation. The concept works well for small to medium networks, but as the number of nodes in the network grows, performance degrades.

Using trust-based routing, it is feasible to identify and eliminate potentially harmful nodes from the network. Such a methodology is suggested in work in [28] for enhancing location privacy against nodes with low trust ratings. For the purpose of eliminating untrusted nodes from the network and enhancing location privacy, the model suggests using a robust privacy-preserving distributed localization technique. Although this improves network security, it also increases computational costs, which in turn causes processing times to become longer and energy efficiency to decline. One strategy that can reduce the length of this delay is the use of aggregative privacy preservation, which was mentioned before and also supported in [29]. In this instance, privacy data from crowdsourcing nodes are aggregated via an incentive mechanism. This introduces a very effective privacy paradigm to the system and lowers processing delay while increasing communication speed. In [30, 31, 32], which provides crowdsourcing models that are similar to those mentioned above and makes use of blockchain technology, deep learning with variational auto encoding, smart contracts, and encrypted data processing are all employed. These models can stop data spoofing attacks, data poisoning attacks, worries about data integrity, and other dangers of a similar kind. These models can only be used with small and medium-sized networks because to scaling issues, which limit their applicability. The use of sidechaining and blockchain sharding, both of which allow for the development of chains of a smaller size and, as a consequence, decrease the amount of time needed for mining and verification, may boost the scalability of these models.

Data slicing [33], attribute-based file encryption [34], local randomization with alternating direction method of multipliers [35], centralized key management [36], techniques for maximizing diversity [37], attribute-based entity transformation [38], and WiFi fingerprinting [39] are additional techniques that can be used. All the models discussed in [33] [34] [35] [36] [37] [38] [39] [40] [41] [42] [43] [44], have a narrow range of applications and can only be used to address a specific set of privacy issues. These models also consume more energy than other models, and their accuracy is less than that of the blockchain, differential privacy, incentive-based, and consensus-based models [40, 41]. However, they have a low computational complexity, which reduces processing delays. Work in [42, 43, 44] propose the use of Differential Privacy, Robust Continual Learning, and Clustering Based Anonymization for different use cases. It is evident that machine learning, differential privacy, auction-based, chaotic, and pseudorandom models outperform other models in terms of overall performance for maintaining privacy and delivering high-quality service over a network. A statistical analysis of these models will be presented in the paragraph that follows, and then those models will be compared to one another. Based on model performance indicators, this will be useful for system designers in helping them choose the models that are best suited for their particular application sets.

III. Statistical analysis

A unique set of network designs, as well as a range of simulation and deployment settings, are used to examine each

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

of the models that are being compared. The performance metrics related to these models were thus fuzzy-ranged and classified into the following categories: very low range (VLR), low range (LR), medium range (MR), high range (HR), and very high range (VHR) in order to undertake a study of them (VH). These ranges were established by comparing these values to those of similar privacy models as well as the comparative analysis that was covered in the publications that were cited. The analysis's findings made it possible to estimate the models' privacy level (P), end-to-end delay (D), computational complexity (CC), and energy consumption (E). Based on this methodology, it is easy to observe that general-purpose cyber physical deployments, industrial Internet of Things (MIoT), and Internet of Things (IoT) models are all being evaluated (include mobile adhoc networks, vehicular adhoc networks, etc.). Because MIoT fall within the category of low power IoT networks, there is a clear distinction between the classification of IoT and MIoT. Each of these models' performances is computed, and each model's performance is estimated independently for each of their several application domains. For instance, picture 3 above illustrates the degree of privacy protection provided by general-purpose cyber physical infrastructure.

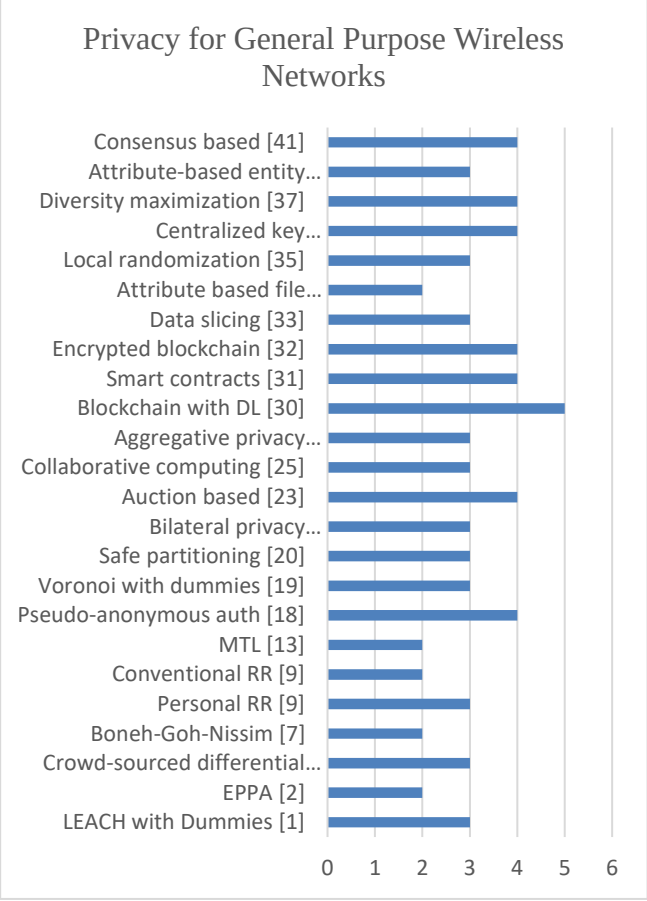

Figure 3. Privacy comparison for General Purpose Cyber physical deployments

This research shows that for general purpose cyber physical installations, Blockchain with DL [30], Consensus based [41], and Pseudo-anonymous auth [18] outperform other models. [30], [41], and [18] Similar to this, figure 4's performance of the delay may be evaluated as follows,

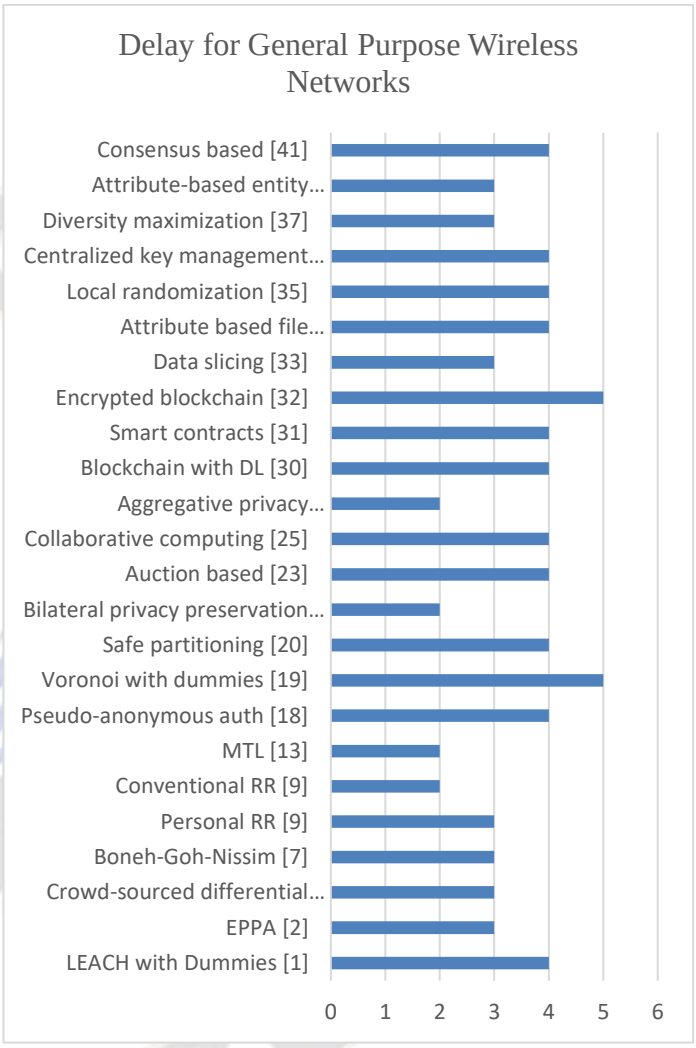

Figure 4. Delay comparison for General Purpose Cyber physical deployments

This comparison demonstrates that the model's Conventional RR [9], MTL [13], and Diversity maximization [37] perform superiorly to those of other models when used to general-purpose cyber-physical installations. In a manner comparable to this, figure 5 illustrates the performance of the computational complexity as follows:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

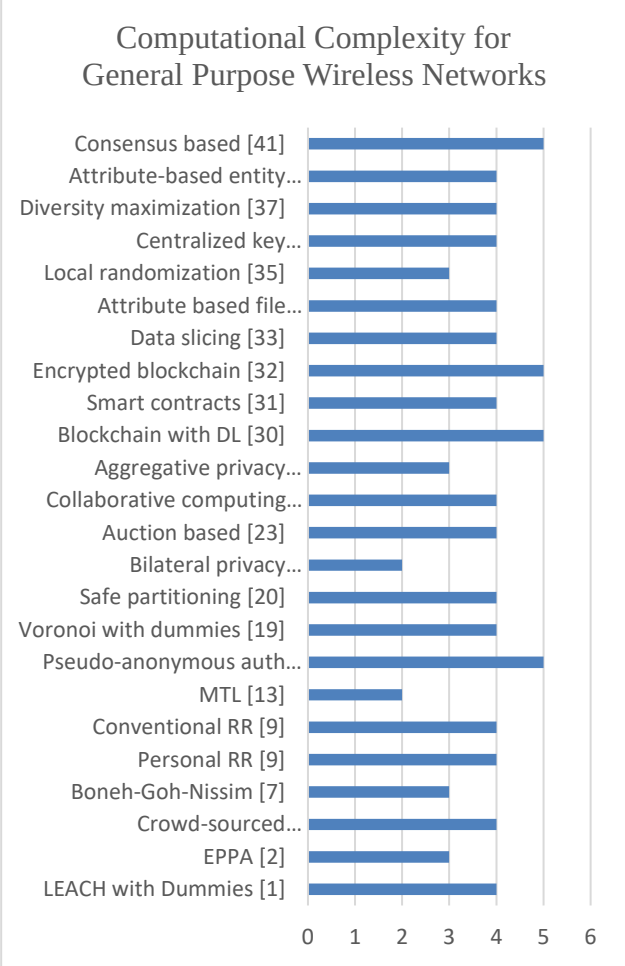

Figure 5. Computational complexity comparison for General Purpose Cyber physical deployments

This research shows that for general purpose cyber physical installations, MTL [13] and local randomization [35] outperform other models. [Reference required] The energy need can also be shown by looking at figure 6, which shows that for general-purpose cyber-physical installations, MTL [13], EPPA [2], Boneh-Goh-Nissim [7], and consensus-based [41] perform better than other models.

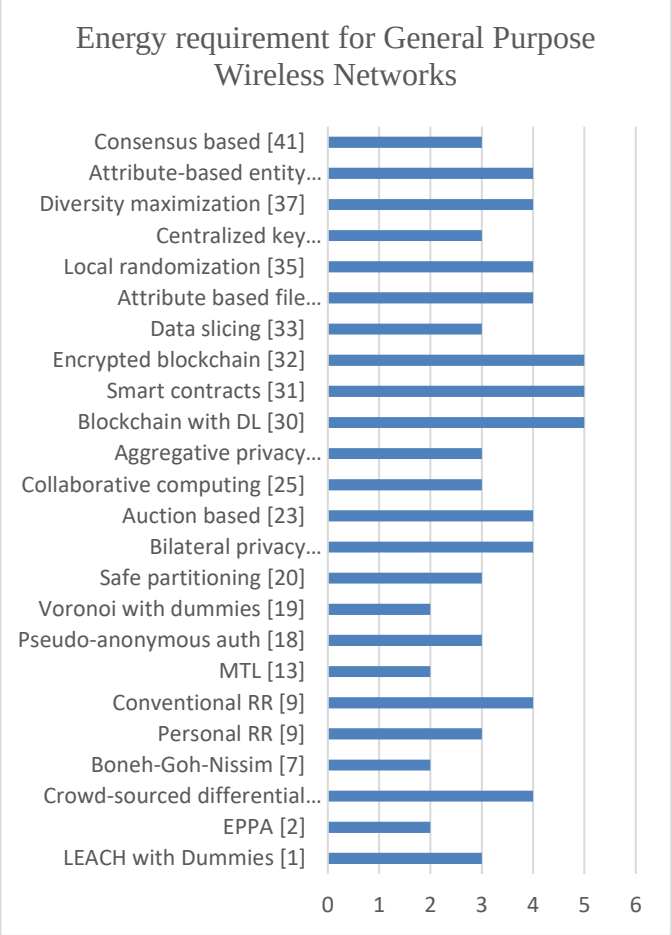

Figure 6. Energy requirement comparison for General Purpose Cyber physical deployments

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

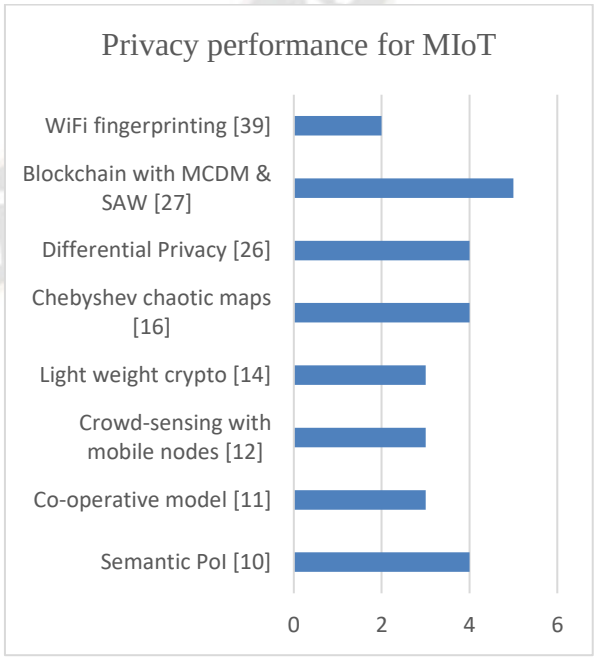

Figure 7. Privacy comparison for MIoT Networks

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

Figure 7 makes it obvious that Blockchain with MCDM & SAW [27] outperforms other models. [27] Similar to this, figure 8's performance of the delay may be seen as follows.

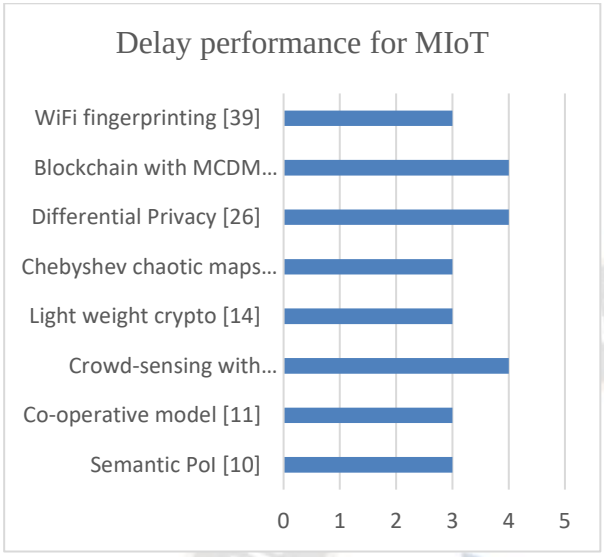

Figure 8. Delay comparison for MIoT Networks

It is clear from looking at figure 8 that Blockchain with Semantic PoI [10] performs better than other models. In a similar vein, the performance of the computational complexity may be shown as follows in figure 9, which can be seen here.

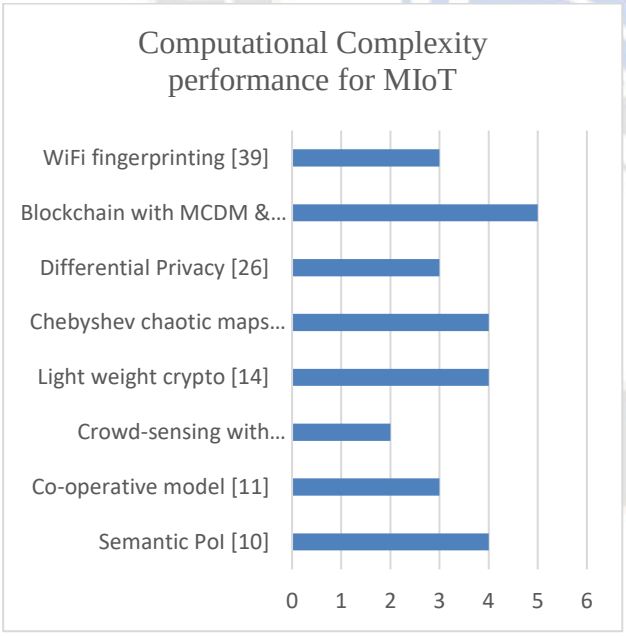

Figure 9. Computational complexity comparison for MIoT Networks

Figure 9 shows that crowd-sensing with movable nodes [12] works much better than other models. More information on the energy needs is provided in Figure 10, which may be summed up as follows,

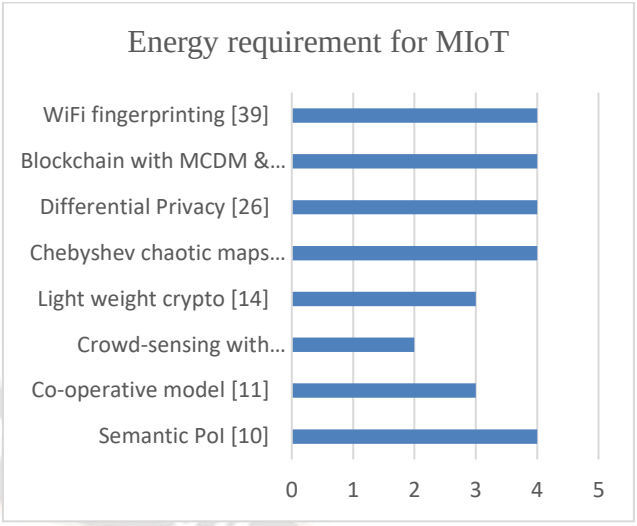

Figure 10. Energy requirement for MIoT Networks

As shown in Figure 10, crowd-sensing models that include moveable nodes [12] perform much better than competing models. In a manner comparable to this, figure 11 presents the following performance statistics about the privacy of IoT networks,

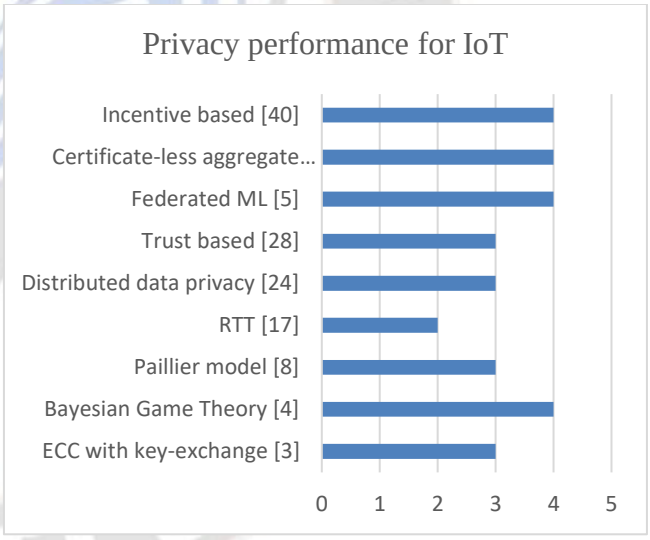

Figure 11. Privacy comparison for IoT Networks

As can be shown in Figure 11, the Bayesian Game Theory [4] performs much better than the competition. On a similar note, the delay performance of Internet of Things networks is shown as follows in figure 12,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

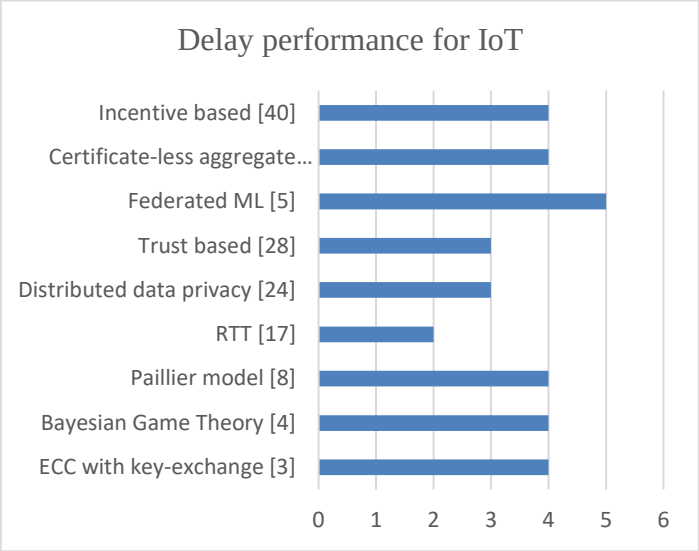

Figure 12. Delay comparison for IoT Networks

As shown in Figure 12, the Distributed data privacy [24] and RTT [17] models perform much better than the competition. In a manner similar to this, figure 13 demonstrates the computational complexity performance of IoT networks in the following manner,

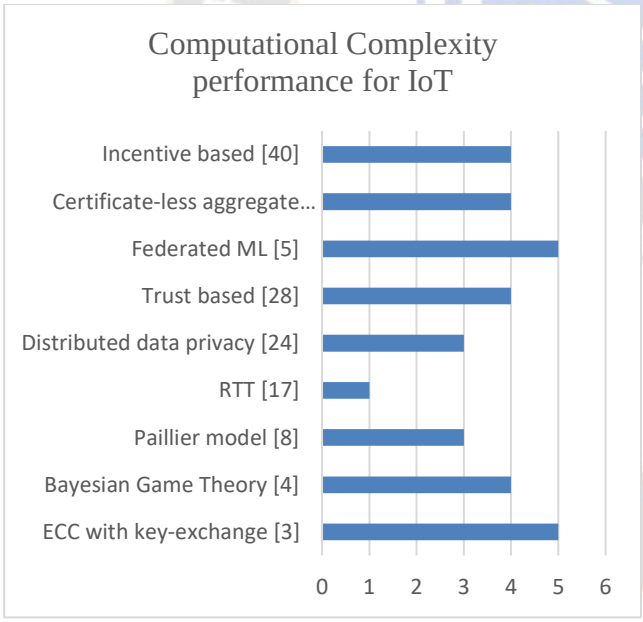

Figure 13. Computational complexity comparison for IoT Networks

Figure 13 demonstrates that the RTT [17] model performs much better than competing models. In a manner comparable to this, figure 14 presents the performance of IoT networks in terms of their computational complexity as follows,

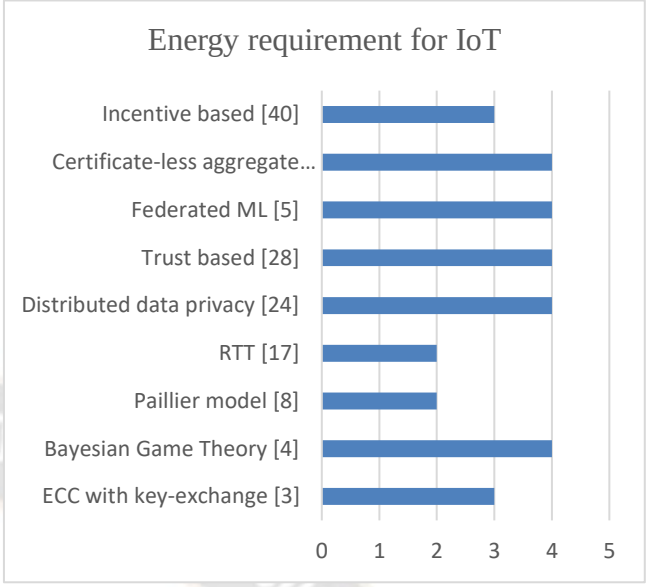

Figure 14. Energy requirement for IoT Networks

Figure 14 demonstrates that the RTT [17] model performs much better than competing models. Therefore, by using this strategy, researchers and system designers have the ability to choose any application and decide on a privacy model that best suits their requirements.

IV. Conclusion & Future scope

The empirical study makes it abundantly evident that there is a disparity between the privacy protection models for general-purpose cyber physical deployments, Internet of Things networks, and Industrial Internet of Things networks. This comparison is performed with regard to the degree of privacy offered, the amount of time required for processing, the amount of computational complexity, and the amount of energy effectively used. In terms of general purpose cyber physical deployments, it is clear from this comparison that Blockchain with DL [30], Consensus based [41], Diversity maximization [37], Centralized key management [36], Encrypted blockchain [32], Smart contracts [31], Auction based [23], and Pseudo-anonymous auth [18] perform better than other models in terms of maintaining privacy levels, whereas Conventional RR [9], MTL [13], and Bilateral privacy preservation models. When it comes to the delay performance of MIoT networks, Blockchain with Semantic PoI [10], Chebyshev chaotic maps [16], Co-operative model [11], Light weight crypto [14], and WiFi fingerprinting [39] outperform other models. On the other hand, Blockchain with MCDM & SAW [27], Semantic PoI [10], and Differential Privacy [26] outperform other models when it comes to the privacy performance of MIoT networks. The models Crowd-sensing with mobile nodes [12], Co-operative model [11], WiFi fingerprinting [39], Differential Privacy [26], and lastly Crowd-sensing with mobile nodes [12], Co-operative model [11], and Light weight crypto [14] are

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

superior to other models in terms of the computational complexity they require.

Similar to how Bayesian Game Theory [4], Federated ML [5], Certificate-less aggregate signature [15], and Incentive based [40] outperform other models for IoT networks in terms of privacy performance, RTT [17], Distributed data privacy [24], and Trust based [28], and RTT [17], Distributed data privacy [24], and Paillier model [8, and finally RTT [17], Paillier model [8, and Distributed data privacy [24] outer Deep learning blockchain solutions that include sidechains and reinforcement learning will need to be adopted in order for future privacy protection measures to be as successful as possible.

References

[1] Dou, Hui κ.ά. 'A Secure and Efficient Privacy-Preserving Data Aggregation Algorithm'. Journal of ambient intelligence and humanized computing 13.3 (2022): 1495–1503. Web.

[2] Liu, Xiaowu κ.ά. 'Energy-Efficient Privacy-Preserving Data Aggregation Protocols Based on Slicing'. EURASIP journal on wireless communications and networking 2020.1 (2020): n. pag. Web.

[3] Xie, Qi κ.ά. 'A Secure and Privacy-Preserving Authentication Protocol for Wireless Sensor Networks in Smart City'. EURASIP journal on wireless communications and networking 2021.1 (2021): n. pag. Web.

[4] Bi, Renwan κ.ά. 'A Privacy-Preserving Personalized Service Framework through Bayesian Game in Social IoT'. Wireless communications and mobile computing 2020 (2020): 1–13. Web.

[5] Kaissis, Georgios A. κ.ά. 'Secure, Privacy-Preserving and Federated Machine Learning in Medical Imaging'. Nature Machine Intelligence 2.6 (2020): 305–311. Web.

[6] Wang, Qian κ.ά. 'Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy'. IEEE transactions on dependable and secure computing (2016): 1–1. Web.

[7] Niu, Chaoyue κ.ά. 'Achieving data truthfulness and privacy preservation in data markets'. IEEE transactions on knowledge and data engineering 31.1 (2019): 105–119. Web.

[8] Babu, S. Sathees, και K. Balasubadra. 'Revamping Data Access Privacy Preservation Method against inside Attacks in Wireless Sensor Networks'. Cluster computing 22.S1 (2019): 65–75. Web.

[9] Song, Haina κ.ά. 'Multiple sensitive values-oriented personalized privacy preservation based on randomized response'. IEEE transactions on information forensics and security 15 (2020): 2209–2224. Web.

[10] Qiu, Guoying κ.ά. 'Mobile semantic-aware trajectory for personalized location privacy preservation'. IEEE internet of things journal 8.21 (2021): 16165–16180. Web.

[11] Liu, Hong κ.ά. 'Cooperative privacy preservation for wearable devices in hybrid computing-based smart health'. IEEE internet of things journal 6.2 (2019): 1352–1362. Web.

[12] Ni, Jianbing κ.ά. 'Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing'. IEEE transactions on mobile computing 19.6 (2020): 1317–1331. Web.

[13] Xu, Zhe, και A. Agung Julius. 'Robust temporal logic inference for provably correct fault detection and privacy preservation of switched systems'. IEEE systems journal 13.3 (2019): 3010–3021. Web.

[14] Shuai, Mengxia κ.ά. 'Lightweight and Privacy-preserving Authentication Scheme with the Resilience of Desynchronisation Attacks for WBANs'. IET information security 14.4 (2020): 380–390. Web.

[15] Kamil, Ismaila A., και Sunday O. Ogundoyin. 'On the Security of Privacy-preserving Authentication Scheme with Full Aggregation in Vehicular Ad Hoc Network'. Security and privacy 3.3 (2020): n. pag. Web.

[16] Deebak, B. D., Fadi Al-Turjman, και Anand Nayyar. 'Chaotic-Map Based Authenticated Security Framework with Privacy Preservation for Remote Point-of-Care'. Multimedia tools and applications 80.11 (2020): 1–26. Web.

[17] Roy, Amit Kumar, και Ajoy Kumar Khan. 'Privacy Preservation with RTT-based Detection for Wireless Mesh Networks'. IET information security 14.4 (2020): 391–400. Web.

[18] Chavhan, Suresh κ.ά. 'Agent pseudonymous authentication-based conditional privacy preservation: An emergent intelligence technique'. IEEE systems journal 14.4 (2020): 5233–5244. Web.

[19] Zhang, Lei, Meina Chen, κ.ά. 'A ε-Sensitive Indistinguishable Scheme for Privacy Preserving'. Cyber physical deployments 26.7 (2020): 5013–5033. Web.

[20] Safia, Bourahla, και Challal Yacine. 'Privacy preservation in social networks sequential publishing'. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2018. Web.

[21] Zhang, Zhikun, Heng Zhang, κ.ά. 'Bilateral privacy-preserving utility maximization protocol in database-driven cognitive radio networks'. IEEE transactions on dependable and secure computing 17.2 (2020): 236–247. Web.

[22] Errapotu, Sai Mounika κ.ά. 'Bid privacy preservation in matching-based multiradio multichannel spectrum trading'. IEEE transactions on vehicular technology 67.9 (2018): 8336–8347. Web.

[23] Xu, Qichao κ.ά. 'APIS: Privacy-preserving incentive for sensing task allocation in cloud and edge-cooperation mobile internet of things with SDN'. IEEE internet of things journal 7.7 (2020): 5892–5905. Web.

[24] Du, Jun κ.ά. 'Distributed data privacy preservation in IoT applications'. IEEE wireless communications 25.6 (2018): 68–76. Web.

[25] Wang, Xin κ.ά. 'Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism'. IEEE transactions on signal processing: a publication of the IEEE Signal Processing Society 67.1 (2019): 221–233. Web.

[26] Hussain, Siam U., και Farinaz Koushanfar. 'Privacy preserving localization for smart automotive systems'.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3s
DOI: https://doi.org/10.17762/ijritcc.v11i3s.6151
***Article Received**: 30 November 2022 **Revised**: 26 December 2022 **Accepted**: 04 January 2023*

Proceedings of the 53rd Annual Design Automation Conference. New York, NY, USA: ACM, 2016. Web.

[27] Xu, Xiaolong κ.ά. 'A blockchain-powered crowdsourcing method with privacy preservation in mobile environment'. IEEE transactions on computational social systems 6.6 (2019): 1407–1419. Web.

[28] Shi, Xiufang κ.ά. 'Resilient privacy-preserving distributed localization against dishonest nodes in internet of things'. IEEE internet of things journal 7.9 (2020): 9214–9223. Web.

[29] Zhang, Zhikun, Shibo He, κ.ά. 'REAP: An efficient incentive mechanism for reconciling aggregation accuracy and individual privacy in crowdsensing'. IEEE transactions on information forensics and security 13.12 (2018): 2995–3007. Web.

[30] Keshk, Marwa κ.ά. 'A privacy-preserving-framework-based blockchain and deep learning for protecting smart power networks'. IEEE transactions on industrial informatics 16.8 (2020): 5110–5118. Web.

[31] Zhu, Saide κ.ά. 'Hybrid blockchain design for privacy preserving crowdsourcing platform'. 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019. Web.

[32] Linoy, Shlomi κ.ά. 'Scalable Privacy-Preserving Query Processing over Ethereum Blockchain'. 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019. Web.

[33] Yao, Lin κ.ά. 'Sensitive Attribute Privacy Preservation of Trajectory Data Publishing Based on L-Diversity'. Distributed and parallel databases 39.3 (2021): 785–811. Web.

[34] Shabbir, Maryam κ.ά. 'Enhancing security of health information using modular encryption standard in mobile cloud computing'. IEEE access: practical innovations, open solutions 9 (2021): 8820–8834. Web.

[35] Lu, Xiuqing, Zhenkuan Pan, και Hequn Xian. 'An Efficient and Secure Data Sharing Scheme for Mobile Devices in Cloud Computing'. Journal of Cloud Computing Advances Systems and Applications 9.1 (2020): n. pag. Web.

[36] Khan, Razaullah κ.ά. 'Privacy Preserving for Multiple Sensitive Attributes against Fingerprint Correlation Attack Satisfying c-Diversity'. Wireless communications and mobile computing 2020 (2020): 1–18. Web.

[37] Song, Yujiao κ.ά. 'Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud'. Security and communication networks 2019 (2019): 1–9. Web.

[38] Zhang, Guanglin, Anqi Zhang, κ.ά. 'Lightweight privacy-preserving scheme in WI-fi fingerprint-based indoor localization'. IEEE systems journal 14.3 (2020): 4638–4647. Web.

[39] Sun, Gang κ.ά. 'Toward incentivizing fog-based privacy-preserving mobile crowdsensing in the internet of vehicles'. IEEE internet of things journal 7.5 (2020): 4128–4142. Web.

[40] Zhao, Chengcheng κ.ά. 'Privacy-preserving consensus-based energy management in smart grids'. IEEE transactions on signal processing: a publication of the IEEE Signal Processing Society 66.23 (2018): 6162–6176. Web.

[41] Zhu, Tianqing κ.ά. 'More than privacy: Applying differential privacy in key areas of artificial intelligence'. IEEE transactions on knowledge and data engineering (2021): 1–1. Web.

[42] Majeed, Abdul, Safiullah Khan, και Seong Oun Hwang. 'Toward privacy preservation using clustering based anonymization: Recent advances and future research outlook'. IEEE access: practical innovations, open solutions 10 (2022): 53066–53097. Web.

[43] Hassanpour, Ahmad κ.ά. 'Differential privacy preservation in robust continual learning'. IEEE access: practical innovations, open solutions 10 (2022): 24273–24287. Web.