25 th International Conference on
Information Technology, Computer and Telecommunication
Event Place: Tbilisi,Georgia
www.itctconf.ir
Publish in international journals (isi , scopus , ...)
25th International Conference on Information Technology,Computer and Telecommunication
PUBLISH IN JOURNALS — INTERNATIONAL CERTIFICATION

The effectiveness of artificial intelligence in establishing secure communication by creating personal boundary protection in ٥G Internet of Things networks(IOT)

Tara Toosi
Information and Communication Technology Expert(ICT)

Abstract

٥G networks are emerging as a major revolution in the field of communications and information technology, significantly affecting communication capabilities and data exchange. New protocols and innovations in these networks are designed to improve the speed, efficiency, and capabilities of mobile networks. ٥G communications are more creatively advanced in terms of speed, protocol usage, and network settings compared to ٤G communications. By providing higher speed, high capacity, and low latency, ٥G is expected to bring tremendous progress in large industries and macro economies in addition to cellular networks. Meanwhile, widespread cyber attacks on ٥G networks have created major risks for computing services.

Therefore, developing mechanisms to increase the security of ٥G networks and also to maintain the security structure of ٥G privacy seems absolutely necessary. This factor improves and makes the ٥G network as efficient as possible for carrying out the actions and operations of the Internet of Things networks. In this research, we try to introduce the mechanisms of privacy protection and trust management before any other discussion, because the mentioned items are used for Internet of Things network communications. Then, we will develop an artificial intelligence (AI)[1] auxiliary framework to pay attention to the issue of privacy protection for performing secure calculations and communications in ٥G-based Internet of Things networks. Of course, not much research has been done on the latter at present and it is somewhat new.

Keywords: Internet of Things, Artificial Intelligence, ٥G Network, Privacy

[1] . artificial intelligenc

Introduction

This paper reviews the Internet of Things (IoT)[۱] in the context of multimedia and broadband wireless networks and discusses the need to increase capacity and quality of service (QoS)[۲]. IoT computing and communication schemes may face operational barriers due to their dependence on diverse sensors and devices. To overcome these challenges, the integration of ۵G wireless networks is essential. These networks provide facilities for reliable wireless communications and the development of intelligent transportation systems. In addition, smart health systems help monitor human activities using mobile devices and sensors. [۵] Security and privacy challenges are also important issues in IoT applications. Researchers have investigated security in vehicular ad hoc networks (VANETs)[۴] and developed privacy and security mechanisms in these areas.

Achievements and Outline of the Paper

This paper examines trust and privacy management in ۵G-based IoT networks. First, the conditions and solutions related to communications and computing are defined, and application examples such as transportation networks and smart health systems are discussed. In particular, the need to distinguish between distributed and centralized privacy is examined. The paper also designs a unique framework for privacy and trust management and uses collaborative learning mechanisms. Finally, it points out cybersecurity challenges and future directions in secure communications and privacy. [۹] Different sections of the paper are dedicated to previous research and the development of new frameworks.

Privacy in ۵G-based IoT networks

Privacy has become one of the main challenges in the era of new technologies, especially in ۵G-based IoT networks. With the expansion of the use of artificial intelligence and big data technologies, the need to create more advanced and efficient security systems to protect user information is felt. Transportation networks and smart cities, as examples of these technologies, play an important role in improving the quality of life. In this regard, designing security frameworks that include attack detection and privacy protection seems essential. [۱۲]The use of anonymous mechanisms, especially in the field of driver and vehicle identification, can help reduce the risk of sensitive information disclosure. [۱۱] These mechanisms usually operate based on the creation of pseudonyms, which not only protect the identity of users but also allow for identity verification without disclosing personal information. In addition, the use of secure key management as a tool for encrypting information and determining the validity of communications can greatly increase the security of IoT networks. By applying advanced artificial intelligence algorithms, these processes can be performed more effectively and prevent cyber attacks. Finally, given the challenges in privacy and data security, it is essential to design comprehensive frameworks for trust and privacy management that simultaneously address the communication and computing needs of vehicles and protect information security against cyber threats. [۳]This approach can help create smart and secure systems in the near future.

Trust Management in ۵G IoT Networks

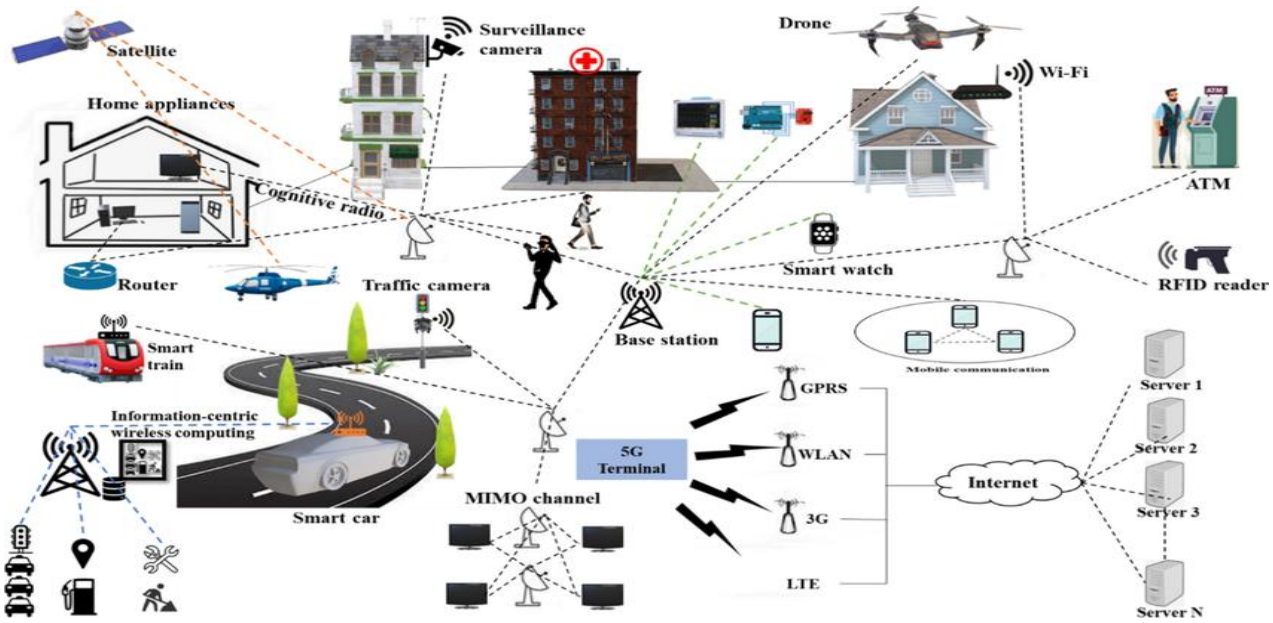
There are very important challenges in designing the trust model in ۵G IoT networks. Specifically in transportation networks, you can see its design in the figure below. Long-term operation cannot work effectively for vehicle communication due to high mobility. In addition, user mobility leads to dynamic location changes, and hence the topography update is done quickly[۷]. There are many types of attacks including: eavesdropping, privacy disclosure, adversarial machine learning, etc., so the trust model must simultaneously prevent various attacks and maintain data privacy. In the following, we will define person-centered trust models, data-centered trust models, hybrid trust models, and the application of blockchain in the trust model. [۲۱]

---

۱. Internet of thing

۲. quality of service

۴. vehicular ad hoc networks



Trust Modeling and Evaluation

Recently, many researchers have developed trust management methods based on third-party trust that work in a centralized and distributed manner. In centralized methods, trust management is used to create a global reputation system, while message evaluation and sharing provide strengths and fault tolerance. However, centralized methods show high costs for system maintenance and recovery after failure. To avoid this problem, a distributed attack detection framework is specified to protect IoT systems, in which the cluster head is selected based on user mobility and trust level. Also, a consensus mechanism is used for all cluster users to determine the trust of users and messages. [٢٥]

Trust modeling is also categorized into three types: person-centered trust model, data-centered trust model, and hybrid trust model. The first model focuses on evaluating user trust. The main methods are based on building a trust system or making decisions based on the opinions of neighboring users or small base stations. Therefore, the system can quickly identify attackers who create malicious data. The system can also accurately identify selfish users who rarely share useful information. [٦] One of the effective methods is to assign credentials to individuals and securely manage these credentials for further auditing. However, it is very difficult to collect enough information to evaluate the user credentials all the time due to the high user mobility. [١٣]

The second model focuses on the credibility of received data, which is jointly evaluated by neighboring users or base stations or RSUs. The credibility values of data can be directly determined using many factors such as data similarity and conflict, or calculated using the received signal strength. Also, the credibility evaluation is performed using a voting system and a social trust model based on the email and network mechanism. Zhang and his colleagues developed an experimental design that integrated a semantic trust routing pattern that was capable of filtering malicious content from invalid parts. The last model focuses on determining the trust value of users and data. The trust value is measured based on the data received from different sources, while the trust value of the node is evaluated based on the completion of activities and the validity of recommendations. [١٦] Also, the reputation of each user is one of the most important factors to evaluate the value of his trust. This trust is obtained through previous

direct interactions and indirect views. We also need to integrate privacy preservation into the trust model and also design the supplementary model in a distributed and efficient way. Another important issue that has not yet been addressed is how to ensure the security of the trust system. [۱۹]

Blockchain-assisted Authentication

We now discuss the new blockchain technology to design an efficient distributed trust management framework in the IoT due to its features of decentralization, consistency, and anti-tampering. Specifically, blockchain-assisted authentication can cover the credibility assessment for data and nodes received, as well as the activity in a decentralized manner. In order to meet these conditions, we can develop a decentralized cryptographic storage system to manage malicious user behaviors by using blockchain methods. Blockchain technology can also adapt the voting mechanisms to generate and store the public keys of well-behaved users, which is confirmed by most blockchain networks. The advantages of blockchain as a promising solution for trust management in the IoT are due to the achievements of aspects such as decentralization, anti-tampering, consistency, and proportionality. [۱۸] However, these current models do not fully address the computational delay and data dispersion due to the large data from a large number of nodes. To address the problem, Takharbaza and his colleagues developed an efficient and anonymous blockchain payment system based on real money tokens and integrated it into an anonymous authentication model. [۲۶] The proposed model for electric vehicles demonstrates low communication and storage costs, as well as preventing unauthorized use of coins in the energy trading system. [۲۷] It also requires the use of compact sensor technology to address issues related to computation delays and data fragmentation. Another important issue that needs to be addressed is the integration of privacy protection into the trust model and the computation process, as well as designing the complete model in a distributed and efficient manner.

A Case Study of Distinct Privacy in Secure Computing and Communications

So far, the current research has specifically defined privacy and trust management. However, these two activities are related and should be defined jointly and using a unique framework. [۲۰] Also, essential computing in ۵G IoT networks is not the main topic of this research. We also discuss how machine learning methods can effectively preserve privacy and manage trust for computing in today's IoT networks. To achieve this, we first examine privacy in a distinct way in secure data-centric computing for a specific healthcare system. Specifically, we evaluate a mechanism based on generative adversarial networks (GANs)[۵] used to identify human activities in the smart healthcare sector while preserving the confidentiality of individuals' data. Based on the successful development of this application example, we can provide guidelines for ۵G IoT network applications, such as transportation networks and defining challenges related to user mobility. [۷]

Computing Scenarios in ۵G IoT Networks

The computing scenarios in ۵G IoT networks focus on trust management and privacy. The need for trust management and privacy protection schemes in IoT computing is felt, especially in transportation networks and smart health systems. Advanced equipment in cars provides information about entertainment and traffic safety. Computing scenarios include vehicle motion control, video streaming, and reward computing. Vehicles can use computing resources to perform activities and earn rewards. Smart health systems also require higher security and better access control methods. This research examines trust management and privacy in human computing. Secure communications in this context are presented in three main pillars using artificial intelligence, blockchain, and privacy techniques. The first pillar deals with a variety of artificial intelligence technologies, while the second pillar refers to the use of blockchain for trust management, and finally the third pillar considers the privacy of users at the local terminal and prevents the release of sensitive information. [۸]

[۵] . generative adversarial network

Brief description of the application cases of human activity recognition computations

In the first step, we define a centralized mechanism for recognizing human activities that uses the Variable Autoencoder (VAE)[۱] model and the semi-supervised classification model. In fact, our design is implemented in a module for different types of applications in the smart health system, namely: ۱) daily activity reporting ۲) activity reporting to the center for monitoring and ۳) live recording of daily activities. For simplicity, we consider six daily activities in our model, which are: walking, jogging, climbing stairs, sitting, standing and descending stairs. Our classification module is created according to different cascade classification such as active classifiers and drop-off classifiers. [۲٤] We can recognize human activities when we use sensors such as accelerometers to record time series inputs.

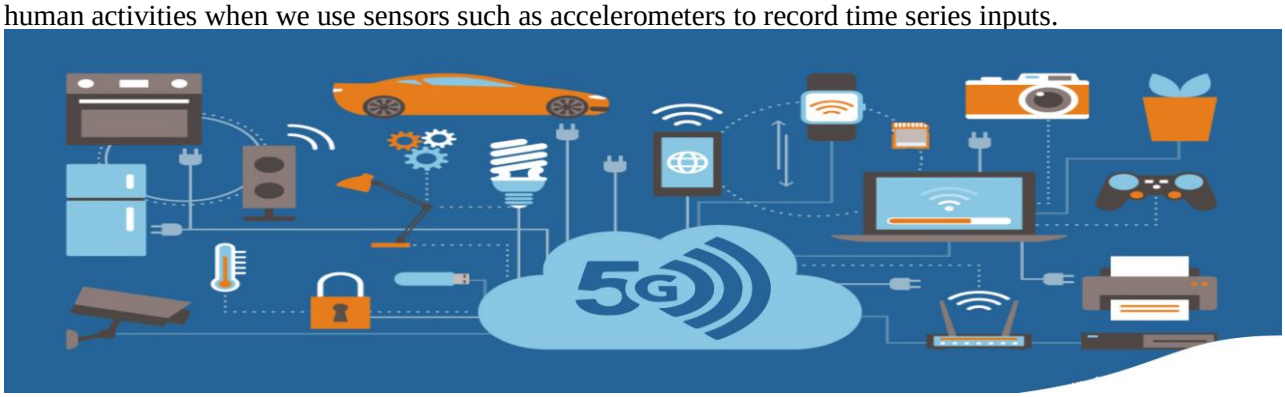


Figure ۲. Privacy-preserving secure computing and communications in ۵G IoT networks

We use the Variable Autoencoder (VAE) model for learning, which is a combination of variable inference and deep learning. Apart from the conventional autoencoder method, our proposed system can sample from any point in the latent dimension and still produce diverse performance due to the diverse contributions of the VAE model. First of all, the VAE model can generalize by reconstructing the estimated inputs by imposing some constraints on the latent space. This trend shows that the VAE model can obtain the salient features of the data that support the reconstruction of the data. Also, the reconstruction activity depends on the estimation of the probability distributions over the individual inputs in the latent space. [۱۰] The Kolick-Leibler criterion in the language function of the VAE model prevents this behavior by training the model to find a solution to the reconstruction errors and the posterior probability distribution close to the prior probability distribution.

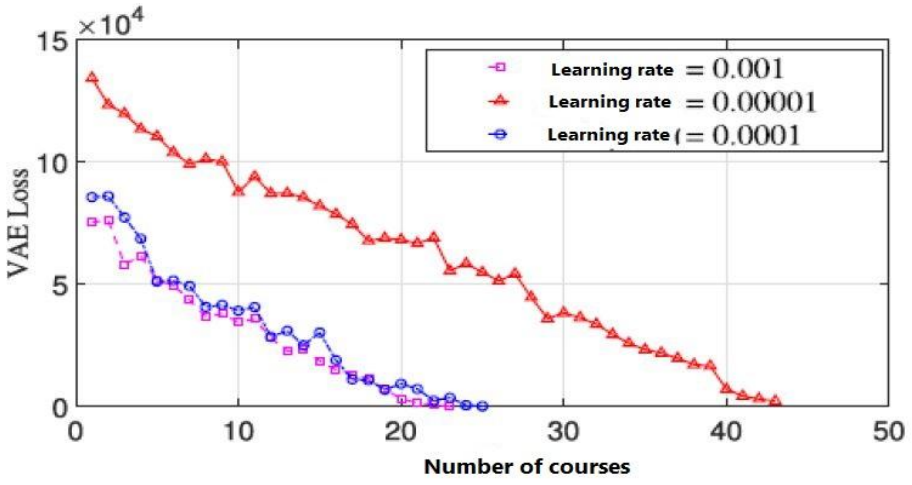


Figure ۳ VAE loss of training data

[۱]. variational auto-encoder

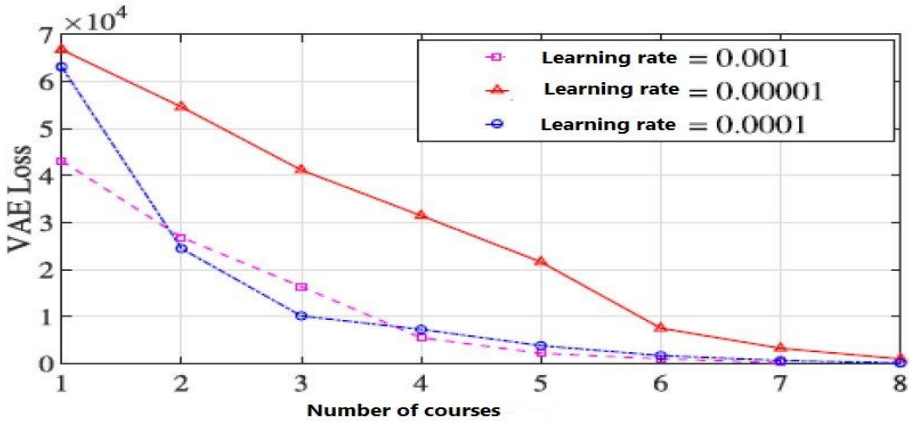


Figure ٤ VAE loss of test data

We create semi-supervised classification to train the model, with time series data in the form of labeled and unlabeled data. For unlabeled data Xu, two networks are trained. The first network is called the cryptographic network $q\emptyset(z|XU$, whose output is Z; the second is called the classification network $q\emptyset(y|XU$, whose output is y. In our model, both the cryptographic and classification networks use convolutional neural networks (CNN). Based on the cryptographic output Z and the label Y, the decoder performs variable inference on them via $P\theta(XU|z.y$ and tries to estimate the input as much as possible. For labeled data XL, we only train the cryptographic network $q\emptyset(z|XL$. In this way, the output of the labels is used as the inputs of the decoder. Again, we perform variable inference on the output of the decoder and the label by We perform the following operations on the reconstructed data: $P\theta(YL.XL|z$ and obtain the reconstructed data. The details of the semi-supervised method for analyzing the loss function are described in the reference. After proper training, we store the configured parameters of the classifier $q\emptyset(y|X)$ and use them to test the real time series input. Specifically, we implement the classifier module that receives the raw time series input from the overlay section and classifies various unobservable variables of some specific actions.

Now, we will prove our successful experiments in previous research to show the efficiency and effectiveness of semi-supervised models. Here, we train our model for labeled and unlabeled data and also examine the performance of our model in terms of VAE model loss on test data. In Figure ٣, it can be easily seen that the VAE model loss decreases when the number of epochs is approximately ٥٠. During training, we test our model on test data with training model parameters ∅ and θ after every ٥ epochs. The VAE model loss for a training rate of ٠,٠٠٠٠١ shows a gradual and slow decay. But it quickly reaches a significantly low value of ٢١٥,٣١٤. This is because ١) the VAE model extracts the most salient features of the human activity data, which provides a useful benchmark for compact retrieval, and ٢) the proposed CNN algorithm also extracts most of the discrete features, which results in low-dimensional hidden codes. There are similar observations regarding the two learning rates as well as the test results in Figure ٤.

Distributed Privacy Separation as a Proposal for Trustworthy Computing

Given the success of centralized privacy separation, we need to develop centralized or decentralized privacy separation using collaborative learning mechanisms, including the use of collaborative learning. Interestingly, non-centralized privacy separation provides good suggestions that can later be used for trust management. This means that we can design a unique framework for privacy and trust management. Here, we develop a collaborative deep learning algorithm to balance the trade-off between accuracy and privacy as well as proportionality. [١٧] In the collaborative mechanism, there is also injustice in that honest miners cannot have a high stake according to the predicted label and hence gain little benefit due to their low computational capacity. This means that they are not malicious actors but may have low participation in the execution of the algorithms. In order to solve this problem, we provide this place for

honest miners to gain more credibility and share more data, namely synthetic examples and gradients, with others. Of course, this shared data is recorded and later used by the subscribers. They can then use these credits to download more gradients from others, which improves the computation. Note that this selective parameter sharing is used because the random gradient descent algorithms are parallelized and run asynchronously. Again, controlling the amount of parameter sharing allows participants or miners to avoid local minimization but reduces information exchange. Trust management is also incorporated into the system to identify potential malicious actors. For example, miners may disrupt the algorithm by updating gradients incorrectly, leading to unexpected convergence or divergence of solutions. To prevent this situation, we can use blockchain technology to cluster and isolate these attackers. Therefore, decentralized privacy disaggregation can provide suggestions for trust management. In short, the main goals of disaggregation are to regulate computational data. Therefore, such a process makes computations more efficient and prevents malicious actors from reconstructing the original data, thus ensuring accurate performance. Also, the user of blockchain technology can be a license for communication and computation. Also, blockchain-based license for communication is defined in Section ۲،۳.

Table ۱

Human activity image (AC, activity, id = ID, weight = W, height = H, age = G, gender).

(x, y, z, Acce x, Acce y, Acce z)	ac	id	w	h	ag	g
(0.176202, −0.17276, 0.056415, 0.06936, 0.072678, −0.10292)	0	0	102	188	46	1
(0.274786, 0.446585, −0.13277, 0.072889, 0.079921, −0.07532)	0	0	102	188	46	1
(−0.99277, 0.826626, 0.088124, −0.10313, −0.11922, −0.54275)	1	0	102	188	46	1
(2.486806, 0.79397, 0.979456, −0.29051, 0.270367, −0.03214)	2	0	102	188	46	1
(2.282, 1.854114, 0.866477, 0.035073, 0.501231, −0.50166)	2	3	90	176	31	1
(2.411877, −0.25831, 1.262217, −0.82369, 0.726726, 0.337789)	2	2	48	161	28	0
(−1.61294, 0.226406, −0.49678, −0.08073, −0.44755, 0.046214)	1	8	93	190	32	1
(2.77218, −1.62248, 2.153218, −0.57944, 1.071683, 0.567687)	2	19	88	180	25	1
(−2.78058, −0.58426, −1.3941, 0.121653, −0.24384, −0.24066)	1	10	70	178	24	1

Table ۲

Removing "identity", hiding "gender"

(A; B)	(0.1; 0.6)	(0.1; 0.7)	(0.1; 0.8)
Activity forecast	0.955361	0.926369	0.73723

Table ۳

Removing "ID" and "Gender"; Hiding "Age"

(A; B)	(0.3; 0.2)	(0.5; 0.3)	(0.7; 0.2)	(0.1; 0.6)
Activity forecast	0.632628	0.615601	0.502853	0.807874

Conclusion

In this paper, we firstly examined the trust and privacy management in ٥G IoT networks. According to the extensive reviews conducted in this area, most of the research focuses on the communication part, while computing has been neglected. However, many modern IoT devices are equipped with new methods, and thus computing is a basic requirement in the current situation. For example, many new brand cars in transportation networks have been developed in such a way that new advanced technologies have been integrated into them with the goals of creating security and entertainment; and considering these emerging changes, computing is used in areas such as video streaming, route estimation, etc. In order to fill this gap, we developed an AI-based trust and privacy management framework for general computing and specific application cases. Specifically, the proposed mechanisms can achieve operational excellence and cost-effectiveness, such that we will be able to conduct comparative assessments of accuracy and privacy as well as proportionality. Finally, we highlight potential future directions in the field of trust management and privacy based on these advances.

Sources and references:

[١] Schwab, K. (٢٠١٧). The fourth industrial revolution. New York, NY: Currency Books.
[٢] Tapscott, D., & Tapscott, A. (٢٠١٧). How blockchain will change organizations. MIT Sloan Management Review, ٥٨(٢), ١٠.
[٣] Glaser, F. (٢٠١٧). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.
[٤] Risius, M., & Spohrer, K. (٢٠١٧). A blockchain research framework. Business & Information Systems Engineering, ٥٩(٦), ٣٨٥-٤٠٩.
[٥] Carson, B., Romanelli, G., Walsh, P., & Zhumaev, A. (٢٠١٨). Blockchain beyond the hype: What is the strategic business value. McKinsey & Company, ١.
[٦] Pedersen, A. B., Risius, M., & Beck, R. (٢٠١٩). A ten-step decision path to Determine When to use blockchain technologies. MIS Quarterly Executive, ١٨(٢), ٣.
[٧] Hochstein, M., De, N., & Baydakova, A. (٢٠١٩). Beyond KYC: Regulators Set to Adopt Tough New Rules for Crypto Exchanges.
[٨] Zyskind, G., & Nathan, O. (٢٠١٥, May). Decentralizing privacy: Using blockchain to protect personal data. In ٢٠١٥ IEEE Security and Privacy Workshops (pp. ١٨٠-١٨٤). IEEE.
[٩] N. Sawyer and D. B. Smith, "Flexible resource allocation in device- to-device communications using stackelberg game theory," IEEE
[١٠] Trans. on Communications, vol. ٦٧, no. ١, pp. ٦٥٣-٦٦٧, Jan. ٢٠١٨. [٢١] Y. Li and A. S. Morse, "The power allocation game on a network: a paradox," IEEE/CAA J. of Automatica Sinica, vol. ٥, no. ٤, pp. ٧٧١- ٧٧٦, Jul. ٢٠١٨.
[١١] T. Fang, D. Wu, J. Chen, and D. Liu, "Cooperative task offloading and content delivery for heterogeneous demands: a matching game- theoretic approach," IEEE Trans. on Cognitive Communications and Networking, vol. ٨, no. ٢, pp. ١٠٩٢-١١٠٣, Jun. ٢٠٢٢.
[١٢] T. Fang, D. Wu, J. Chen, C. Yue, and M. Wang, "Joint distributedcache and power control in haptic communications: a potential game approach," IEEE Internet of Things J., vol. ٨, no. ١٨, pp. ١٤٤١٨- ١٤٤٣٠, ١٥ Sept. ٢٠٢١.
[١٣] J. Zhang and J. Wang, "Deep adversarial reinforcement learning based incentive mechanism for content delivery in D٢D-enabled mobile networks," Neurocomputing, vol. ٥٤٤, Article ID:١٢٦٢٥٨, Aug. ٢٠٢٣.
[١٤] B. Wang, Y. Sun, S. Li, and Q. Cao, "Hierarchical matching with peer effect for low-latency and high-reliable caching in social IoT," IEEE Internet of Things J., vol. ٦, no. ١, pp. ١١٩٣-١٢٠٩, Feb. ٢٠١٨. [٢٦] D.
[١٥] Wu, L. Zhou, Y. Cai, H. C. Chao, and Y. Qian, "Physical-social- aware D٢D content sharing networks: a provider-demander matching game, " IEEE Trans. on Vehicular Technology, vol. ٦٧, no. ٨, pp. ٧٥٣٨-٧٥٤٩, Aug. ٢٠١٨.
[١٦] S. A. Kazmi, et al., "Mode selection and resource allocation in device-to-device communications: a matching game approach," IEEE Trans. on Mobile Computing, vol. ١٦, no. ١١, pp. ٣١٢٦-٣١٤١,
[١٧] K. Pandey and R. Arya, "Lyapunov optimization machine learning resource allocation approach for uplink underlaid D٢D communication in ٥G networks," IET Communications, vol. ١٦, no. ٥, pp. ٤٧٦-٤٨٤, Mar. ٢٠٢٢.
[١٨] M. H. Zafar, I. Khan, and M. O. Alassafi, "An efficient resource scheme for D٢Dcommunication," Digital Communications and Networks, vol. ٨, no. ٦, pp. ١١٢٢-١١٢٩,optimizationDec. ٢٠٢٢.
[١٩] I. Ioannou, V. Vassiliou, C. Christophorou, and A. Pitsillides, "Distributed artificial intelligence solution for D٢D communication in ٥G networks," IEEE Systems J., vol. ١٤, no. ٣, pp. ٤٢٣٢-٤٢٤١, Sept. ٢٠٢٠.
[٢٠] W. Jiang, et al., "Joint computation offloading and resource allocation for D٢D-assisted mobile edge computing." IEEE Trans. on Services Computing, vol. ١٦, no. ٣, pp. ١٩٤٩-١٩٦٣, May/Jun. ٢٠٢٢.
[٢١] L. L. H. Xing, J. Xu, and A. Nallanathan, "Joint task assignment and resource allocation for D٢D-enabled mobile-edge computing," IEEE Trans. on Communications, vol. ٦٧, no. ٦, pp. ٤١٩٣-٤٢٠٧, Jun. ٢٠١٩. [
[٢٢] W. Song, Y. Zhao, and W. Zhuang, "Stable device pairing for collaborative data dissemination with device-to-device communications," IEEE Internet of Things J., vol. ٥, no. ٢, pp. ١٢٥١- ١٢٦٤, Apr. ٢٠١٨.
[٢٣] Zhang, N., Cheng, N., Gamage, A., & Yang, J. "G Security: Challenges and Opportunities." IEEE Communications Surveys & Tutorials, vol. ١, no. ٥, T., pp. ١-١.
[٢٤] Abadi, M., & Andersen, D. G. "Secure Computation Using Machine Learning." Proceedings of the ACM on Data Privacy and Security, vol. ١٠, no. ٢, ٢٠١٦, pp. ٦٧-٤٥.
[٢٥] .Kumar, R., & Tripathi, R. "Blockchain Technology: A Revolution in Privacy and Security." Journal of Network and Computer Applications, vol. Y, Y., article no. ١+TAOY.
[٢٦] Stojmenovic, I., & Wen, S. "The Fog Computing Paradigm in IoT Security." IEEE Transactions on Smart Grids,

vol. ٥, no. ٣, ٢٠١٤, pp. ١١٩٠ - ١١٩٦

[٢٧] Tang, J., Liu, X., Liu, Y., & Shao, L. "AI and Trust Management in IoT Ecosystems." Future Generation Computer Systems, vol. ٩١, ٢٠١٩, pp. ١١٣-١٨٠Mohamed, N., & Al-Jaroodi, J. "Applications of Machine

[٢٨] Fan, C., Huang, H., & Wang, Z. "Blockchain for Privacy Preservation in IoT: A Survey." Computer Networks, vol. ١,٢٠٠, article no. ١٠١٢٩٣.