International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 18, Number 1 (2022), pp. 1-11
© Research India Publications
http://www.ripublication.com

# Securing Data using Artificial Intelligence and Block Chain

**D. Pavan Srivasta[1], D. Suresh Babu[2], Srinivas Kanakala[3]**

*[1]Vasavi College of Engineering, Hyderabad, India,*

*[2]Kakatiya Government College, Warangal, India,*

*[3]VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India.*

## ABSTRACT

The input for several Artificial Intelligence algorithms is Data which is used for mining the valuable features. But, data on the internet are unbelievable and difficult to authorize. It is very difficult to verify the data for the users in this complex cyberspace. So, for this we proposed SecNet in this paper. SecNet , An architecture that helps in securing data storage, processing of data and sharing large scale Internet environments. The main aim of this architecture is to create a more secure cyberspace with real big data and to improve the Artificial Intelligence algorithms on various data sources. This architecture integrates and provides three main components1) The exchange of Blockchain-based data is done with guaranteed Ownership. This allows exchange of reliable data in large scale space and forms real big data.2) The securing of AI-based secure computing platform powered by Artificial Intelligence to create smarter security rules that helps to create a more stable cyberspace. 3)The trusted value-sharing Security Service purchase Mechanism, provides participants with a great opportunity to receive Economic Rewards for data or service provision, thus facilitating data sharing, resulting in better AI performance.

This also discusses common SecNet use cases and potential another deployment methods, and analyzes their effectiveness in terms of security in networks and their economic return.

**Keywords:** SecNet, Stable Cyberspace, Block chain, Artificial-Intelligence algorithm, reliable data.

## 1. INTRODUCTION

With the development of information technology, there is an increasing tendency to integrate cyberphysical social (CPS) systems not only into the digital Internet, but also into a highly standardized information society [1]. In such an informationoriented society, data is the property of the owner

and its use must be under the complete control of the owner, which is not a common case [2], [3]. Given that data is arguably the crude oil of the information society, almost every large company wants to collect as much data as possible for future competitiveness [4], [5]. Sensors built into the products of these large companies increase and implicitly record the amount of personal data such as location, web search behavior, user calls, and user preferences. This poses a great risk of losing the privacy of the data owner [6], [7]. Moreover, the use of this data is beyond the control of the owner, as there is currently no reliable way to record how and by whom the data is being used. Therefore, there are few ways to catch an infringer who abuses and tracks this data. Or punish [8]. This means that you cannot manage your data effectively, which makes it very difficult to manage the potential risks associated with the data collected [9]. For example, if data is collected by

a third party (such as a large company), the data is inaccessible and individuals cannot understand or control the risks associated with the data they are collecting. At the same time, there is no constant record for the use of the data, increasing the risk of data misuse [10]. If there is an efficient and reliable way to collect data scattered throughout CPS and merge it into real big data, AI can handle large amounts of data, resulting in significant artificial intelligence (AI) performance. Improve. At the same time, increasing the amount of data that contains vast amounts of information brings significant benefits (for example, better data security), empowering AI to outperform humans in more areas. [11]. According to a study in [12], even the simplest AI algorithms currently available (eg) The key is how to make the data exchange reliable and secure [13]. Fortunately, blockchain technology is a promising way to achieve this goal through a network-wide consensus mechanism that guarantees tamper-proof data exchange with economic incentives [14], [15]. Therefore, AI can be further enhanced through blockchain-protected data exchange [16][17] [18].. This allows AI to make more accurate decisions based on the vast amount of data collected from more locations on the Internet. meet. For example, collaboration between different edge computing paradigms can work together to improve the overall system performance of an edge network [19]. The reason blockchain enables a reliable mechanism is that it can provide a transparent, tamper-proof metadata infrastructure for seriously re-encoding all data usage [17]. That's why SecNet has introduced a blockchain-based data exchange mechanism with guaranteed properties. In addition, SecNet provides economic incentives between different units by embedding smart contracts in the data to trigger tamper-proof automatic value exchanges when sharing data or exchanging security services. To do. In this way, SecNet guarantees the security of your data and facilitates data exchange across CPS. In addition, the data is the fuel for AI [11] and can be very helpful.

## 2. RELATED WORK

Data security is a major concern of any network architecture and is the foundation for improving AI algorithms as it requires large amounts of data from as many locations on the Internet as possible. Work in [3] demonstrates an architecture called Amber that allows data isolation from web applications. This gives web users control over their personal data and provides powerful web-wide query capabilities for retrieving personal data. To extend the data and application decoupling mechanism from pure web services to all types of applications, a research group at the Massachusetts Institute of Technology's Media Lab is developing openPDS [5]. The author of [8] is developing the Origin Chain system to provide metadata transparency and operational security when tracking products in the supply chain. OriginChain allows all connected parties to receive the same trusted data and adapt to dynamic environments and regulations. The authors of [10] have proposed a blockchain-based MeDShare system for effectively managing and protecting medical records and exchanging medical data between cloud repositories, with data transmission, auditing, and control. Guaranteed. Work in [17] provides a detailed overview of the background of blockchain and intrusion detection systems (IDS), explains how to apply blockchain technology to IDS, and rationalizes possible hidden dangers in this direction. Make a guess. In addition, work [15] designs a blockchain-based incentive mechanism for cloud sensing applications. This guarantees privacy and data security. It is also a promising way to improve. Work in [11] provided a detailed overview of the use of AI for big data and the use of big data for AI, as well as some development directions, such as improving data security with AI. Work in [16] emphasizes that the performance of AI improves when a large amount of data is provided to realize a better basic model, and is larger and more valuable to use AI better. We are looking for more effort to build a dataset. 1 Enable data security. In addition, work [21] outlines AI techniques for cybersecurity and provides a comprehensive overview. It is worth mentioning that the SecNet is different from the HyperNet [1]. In addition, SecNet aims to realize a safer cyberspace by sharing not only user data but also security rules created by AI, while HyperNet aims only to share user data safely. is. Last but not least, PDC is just one of SecNet's data storage solutions (see Section V), but HyperNet's only solution.

## 3. SECNET'S ARCHITECTURE

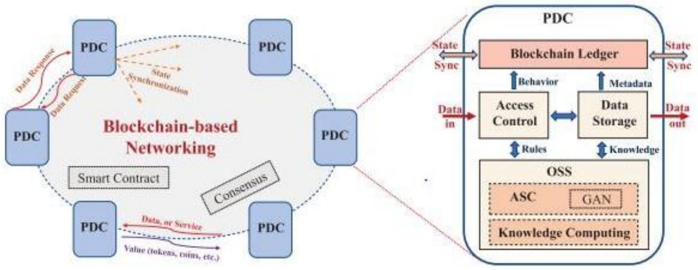

FIGURE 1. The SecNet architecture.

**Figure 1:** Architecture of secenet

SecNet is built as a more secure cyberspace architecture by integrating the following three key components: 1) Blockchain-based data exchange with guaranteed ownership. 2) Big data-based AI- based secure computer platform for creating intelligent and dynamic security rules. 3) Reliable replacement mechanism for purchasing security services. status with other nodes. In terms of data technology, SecNet nodes are equipped with a data storage module and an access control module for data security.

### 3.1 Data Sharing Guaranteed By Blockchain

For data protection, SecNet takes over the private data center (PDC) from HyperNet [1] and is a blockchain-based protection mechanism for data exchange between untrusted entities. To integrate. The PDC provides physical security for the data and uses an advanced architectural and engineering approach to the operation of AI-based OSS. An important function of PDC is unified data access control. Uniform data access control has two aspects. Before sharing data over the Internet, this data must be registered with the DRB to notify the availability of transfers. The DRB is responsible for not only naming the data, but also validating the data and recording the behavior of the data interactions.

### 3.2 AI-based secure computing

Data is very important to the owner and can generate different types of data by transforming the raw data according to different needs and scenarios. For example, you can extract user health information stored in a PDC and reorganize it into structured medical data. This is very useful for hospitals, research institutes, and medical application developers. After extensive generation and classification by the GAN module, the PDC's OSS has become much more intelligent and powerful, and fake access requests to data have little opportunity to compete with this PDC's secure and intelligent OS Paraphrased Text Different entities can share their computations with each other in a blockchain- protected way to achieve higher performance and lower energy consumption.

### 3.2 AI-based secure computing

Aside from the security concerns of every single PDC, the Internet has its own set of threats. For example, various cyberattacks and computer viruses are moving over the Internet and are constantly evolving, resulting in inadequate protection from the perspective of individual PDCs.. The smart contract returns an access token for this data. Access tokens allow consumers to fetch the desired data from the storage system at the appropriate address. SGX ensures that the intelligent contract processing process is unobstructed by the user and guarantees the value exchange process. Execution of SGX- based smart contracts allows the blockchain ledger to manage the value exchange process (eg).

### Algorithm - smart contract on data

```
def add_block(self, block, proof):
previous_hash = self.last_block.hash
if previous_hash != block.previous_hash:
return False
if not self.is_valid_
proof(block, proof):
 return False
block.hash = proof
print("main "+str(block.hash))
self.chain.append(block)
return True
def is_valid_proof(self, block, block_hash):
print("compare "+str(block_hash == lock.compute_hash())+" "+block.compute_hash()+" "+str(block_hash.startswith('0' * Blockchain.difficulty)))
return (block_hash.startswith('0' * Blockchain.difficulty) and block_hash == block.compute_hash())
def proof_of_work(self, block):
block.nonce = 0
computed_hash = block.compute_hash()
while not computed_hash.startswith('0' * Blockchain.difficulty):
block.nonce += 1
 computed_hash = block.compute_hash()
 return computed_hash
def add_new_transaction(self, transaction):
self.unconfirmed_transactions.append(transaction)
def AccessData(request):
if request.method == 'GET':
return render(request, 'AccessData.html', {})
def index(request):
if request.method == 'GET':
return render(request, 'index.html', {})
def CreateProfile(request):
if request.method == 'GET':
return render(request, 'CreateProfile.html', {})
```

## 4. USE SCENARIO

SecNet enables a huge number of applications with AI and blockchain-specific embedding. One of the typical cases of deploying and using SecNet is medical data sharing between trusted parties, supporting a smart and secure ecosystem for medical data management. This is the key of the global health care system.

### 4.1 Necessaries of Implementing Secnet for Medical Care

Implementation of SECNET required for medical supplies Traditional methods of managing medical data are inefficient in building a global health system. On the one hand, today, medical data is stored in diverse health environments and is controlled by different entities that may have different commercial needs . To solve the above problems, SecNet is 1) blockchain-based data release guarantee, 2) smart contract that regulates interactions between trusted entities, 3) AI-based for behavioral analysis. Use to effectively identify the source of secure computing and data. -Provides audit and control, and behavior tracking in a fraudulent open prevention method. The detailed workflow for achieving reliable sharing of medical data embedded in these characters provided by SecNet is as follows.

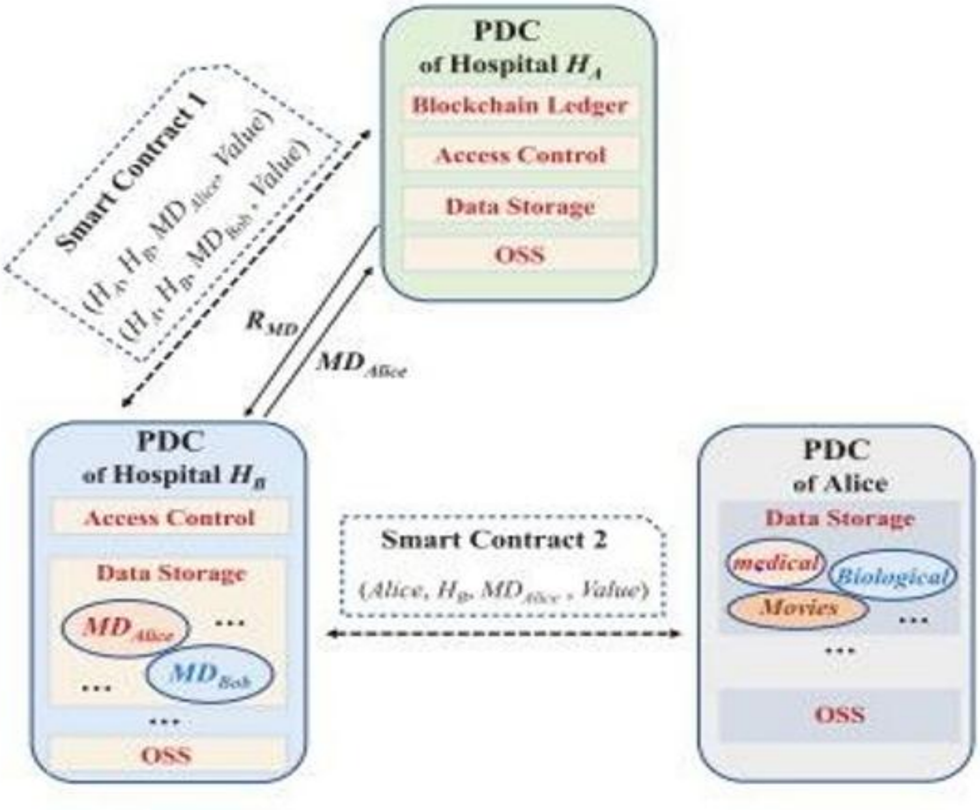

**Figure 2:** Medical data sharing

### 4.1 Alternative Way for Secnet

SecNet data storage is provided by the PDC and data security is the responsibility of the PDC owner. In this way, the data is controlled by its owner and the interaction with the data can be monitored locally on the PDC. However, if SecNet users store their data in a secure cloud provided by a reputable and large company that can guarantee the security of their data, instead of storing it in their own PDC, the InterPlanetary file. This data is distributed throughout SecNet and is the data owner's PDC. A possible solution is to build some secure compute nodes on the SecNet where data can flow, but you can only answer, not answer High-dimensional data can be leaked to support AI-based computing and knowledge extraction for specific users without compromising data security and privacy.

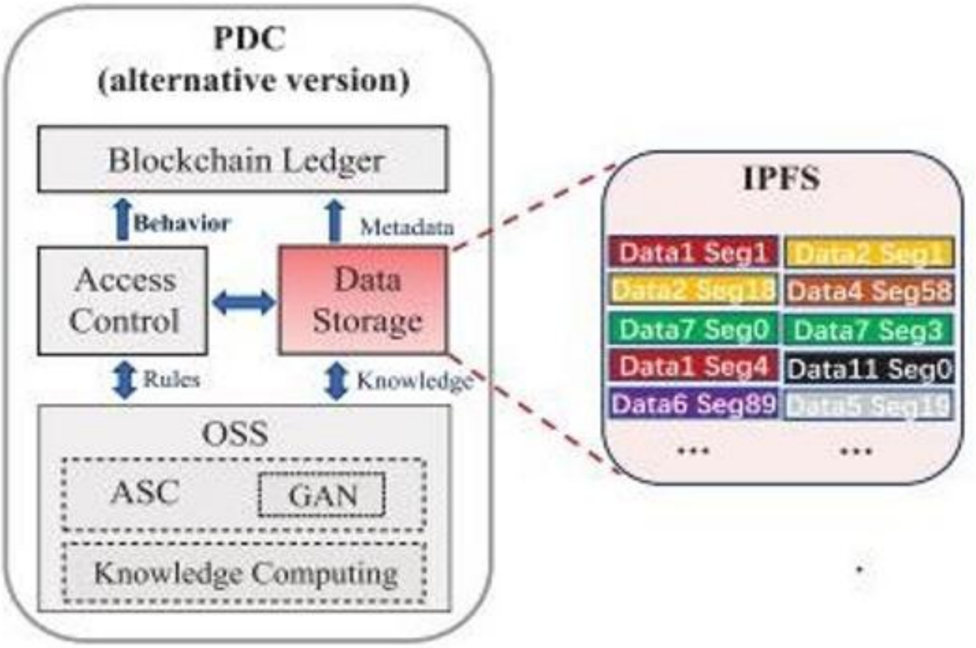

**Figure 3:** Alternative storage model of secnet

## 5. PERFORMANCE ANALYSIS

DDoS attacks are one of the most serious network attacks on both Internet infrastructure and its 4,444 application. Attackers can use these types of attacks to run out of bandwidth resources for popular and critical web applications, making these services unavailable to users, or blocking internet connections in most parts of the country This means that SecNet can significantly reduce the impact of the infamous DDoS attacks. The results show that the SecNet vulnerabilities decrease significantly as the number of common security rules increases. This is because as the number of common security rules increases, all participants become more knowledgeable about the security of the network, making it harder for an attacker to successfully and recognize a DDoS attack. increasing security rules.

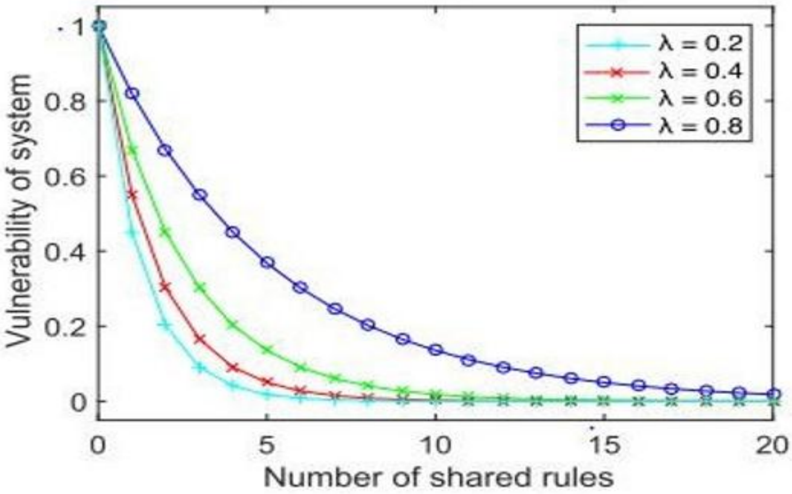

**Figure 4:** Vulnerability of secnet suffering from DDOS

SecNet's security level continues to improve when each participant uses their own security rules on the blockchain along with other participants. This is because every participant in the system has over security knowledge to defend against attacks. Each member's revenue is a key factor influencing member initiativesDuring evaluation, three price levels were examined for general safety rules (αp = 1.05, 1.5, 2). The price level represents the ratio of a fixed price of to its fair market value. in the picture. 6 shows that if the price of the rule capable of collusion is set unreasonably high (), the income of the rule publisher may decrease..

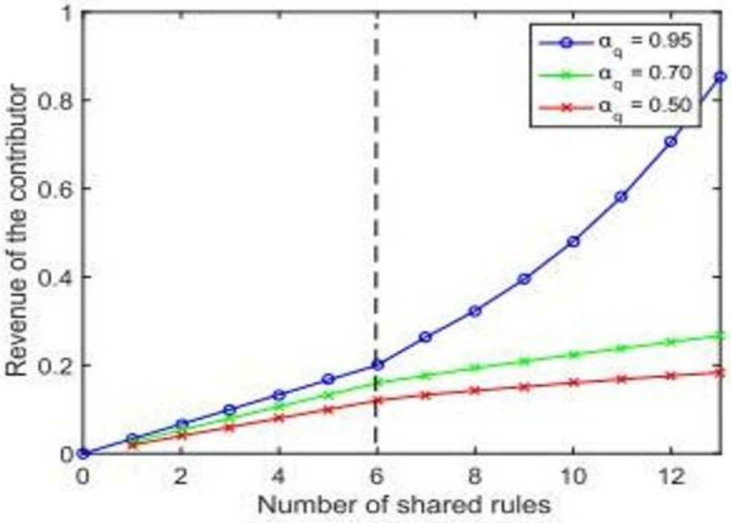

**Figure 5:** Revenue when sharing security rules with varying quality

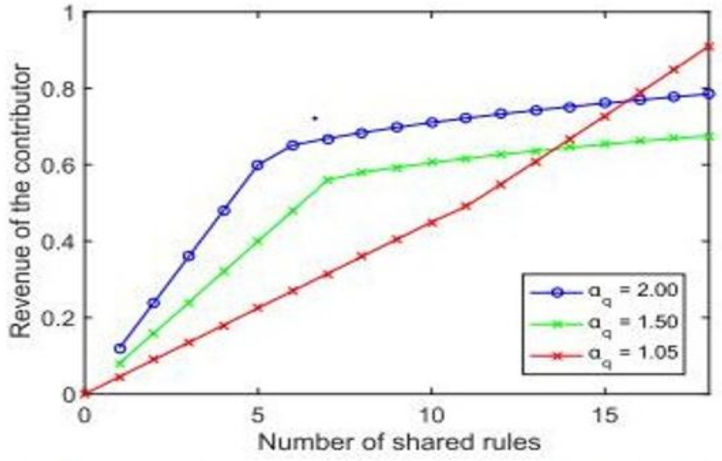

**Figure 6:** Revenue when sharing security rules with rule price

## 5. CONCLUSION

We propose SecNet, a new network paradigm focused on secure data, to utilize AI and blockchain to solve data abuse and enable AI to reliably manage data in an insecure environment through the blockchain. Store, share, and compute instead of exchanging data. SecNet is a blockchain technology and AI-based secure computing platform to ensure data ownership, a blockchain-based incentive mechanism to provide the paradigm and incentives for data convergence, and provide stronger AI for, ultimately better networking Provides security. It also discusses, a common use case for SecNet in healthcare systems, and provides an alternative way to use the SecNet storage capabilities. It also evaluates the improvement of network vulnerabilities in response to DDoS attacks, and analyzes the creative aspects that encourage users to share security rules for a more secure network. Future work on will look at using the blockchain to grant access to data requests and design secure and detailed smart contracts for data exchange and AI-powered computing services on SecNet. It also simulates SecNet and analyzes its performance through extensive experimentation on advanced platforms .

## REFERENCES

[1] H. Yin, D. Guo, K. Wang, Z. Jiang, Y. Lyu and J. Xing, "Hyperconnected network: A decentralized trusted computing and networking paradigm", *IEEE Netw.*, vol. 32, pp. 112-117, Jan./Feb. 2018.

[2] K. Fan, W. Jiang, H. Li and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT", *IEEE Trans Ind. Informat.*, vol. 14, no. 4, pp. 1656-1665, Apr. 2018.

[3] T. Chajed, J. Gjengset, J. Van Den Hooff, M. F. Kaashoek, J. Mickens, R. Morris, et al., "Amber: Decoupling user data from Web applications", *Proc. 15th Workshop Hot Topics Oper. Syst. (HotOS XV)*, pp. 1-6, 2015.

[4] M. Lecuyer, R. Spahn, R. Geambasu, T.-K. Huang and S. Sen, "Enhancing selectivity in big data", IEEE Security Privacy, vol. 16, no. 1, pp. 34-42, Jan./Feb. 2018.

[5] A. de Montjoye, E. Shmueli, S. S. Wang and A. S. Pentland, "openPDS: Protecting the privacy of metadata through SafeAnswers", PLoS ONE, vol. 9, no. 7, 2014.

[6] C. Perera, R. Ranjan and L. Wang, "End-to-end privacy for open big data markets", IEEE Cloud Comput., vol. 2, no. 4, pp. 44-53, Apr. 2015.

[7] X. Zheng, Z. Cai and Y. Li, "Data linkage in smart Internet of Things systems: A consideration from a privacy perspective", IEEE Commun. Mag., vol. 56, no. 9, pp. 55-61, Sep. 2018.

[8] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability", IEEE Softw., vol. 34, no. 6, pp. 21-27, Nov./Dec. 2017.

[9] Y. Li, Z. Cai, J. Yu, Q. Han and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices", IEEE Netw. Mag., vol. 32, no. 4, pp. 8-14, Jul./Aug. 2018.

[10] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017.

[11] D. E. O'Leary, "Artificial intelligence and big data", IEEE Intell. Syst., vol. 28, no. 2, pp. 96-99, Mar. 2013.

[12] A. Halevy, P. Norvig and F. Pereira, "The unreasonable effectiveness of data", IEEE Intell. Syst., vol. 24, no. 2, pp. 8-12, Mar. 2009.

[13] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems", IEEE Trans. Netw. Sci. Eng..

[14] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy", IEEE Commun. Mag., vol. 55, no. 12, pp. 119-125, Dec. 2017.

[15] J. Wang, M. Li, Y. He, H. Li, K. Xiao and C. Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications", IEEE Access, vol. 6, pp. 17545-17556, 2018.

[16] C. Sun, A. Shrivastava, S. Singh and A. Gupta, "Revisiting unreasonable effectiveness of data in deep learning era", Proc. IEEE Int. Conf. Comput. Vis. (ICCV), pp. 843-852, Oct. 2017.

[17] Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "When intrusion detection meets blockchain technology: A review", IEEE Access, vol. 6, pp. 10179-10188, 2018.

[18] J.-H. Lee, "BIDaaS: Blockchain based ID as a service", IEEE Access, vol. 6, pp. 2274-2278, 2017.

[19] K. Wang, H. Yin, W. Quan and G. Min, "Enabling collaborative edge computing for software defined vehicular networks", IEEE Netw., vol. 32, no. 5, pp. 112-117, Sep./Oct. 2018.

[20] A. B. Kurtulmus and K. Daniel, "Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain" in arXiv:1802.10185, 2018, [online] Available: https://arxiv.org/abs/1802.10185.