INTERNET OF THINGS (IOT)-CYBER PHYSICAL SYSTEMS (CPS) AN EXPLORATORY APPROACH ON THE SECURITY OF IOT-CPS FRAMEWORK USING BLOCKCHAIN TECHNOLOGIES

K.PRATHIBANANDHI
Assistant Professor,
Department of Electrical and Electronics Engineering in Saveetha School of Engineering

S. RAMESH
Assistant Professor,
Department of Computer Science & Engineering,
Krishnasamy College of Engineering & Technology, S.Kumarapuram, Cuddalore

Dr. C. YAASHUWANTH
Associate Professor,
Department of Information Technology,
Sri Venkateswara College of Engineering, Autonomous-Sriperumbudur, India.

Abstract- Internet of Things (IoT) is an emerging paradigm and have gained attention among various communities such as health care, industries, sports, automobile and media [1]. The rapid proliferation of ubiquitous sensors made the tasks proficient for performing the intended actions as it has the capability of connected anywhere, anytime and everywhere [2]. More recently, the ubiquitous nature of the IoT offers machine-machine interaction and human- machine interaction in many complex applications. In machine-machine interaction, industries exploit serial communication, and wireless communication strategies for exchanging and processing the machine data, which is a technological innovation in Industrial IoT [3]. As beneficial, many industries adopted industry 4.0 by utilizing the OPC.Net specifications [4] which integrates both smart industries and intelligent systems through PCs, mobile phones etc. Mostly these industries encompass RFID tags, cloud storage, IoT gateways for the effective data processing and predictions. Also, the IoT plays a great role in transforming the smart industries to Cyber physical systems (CPS) [5]. Generally, the CPS provide monitoring, computing and also it virtually replaces the machine and integrates the actions together using internet and cloud.

Keywords – Internet of Things, Cyber physical system, Block Chain

I. INTRODUCTION

Internet of Things (IoT) is an emerging paradigm and have gained attention among various communities such as health care, industries, sports, automobile and media [1]. The rapid proliferation of ubiquitous sensors made the tasks proficient for performing the intended actions as it has the capability of connected anywhere, anytime and everywhere [2]. More recently, the ubiquitous nature of the IoT offers machine-machine interaction and human-machine interaction in many complex applications. In machine-machine interaction, industries exploit serial communication, and wireless communication strategies for exchanging and processing the machine data, which is a technological innovation in Industrial IoT [3]. As beneficial, many industries adopted industry 4.0 by utilizing the OPC.Net specifications [4] which integrates both smart industries and intelligent systems through PCs, mobile phones etc. Mostly these industries encompass RFID tags, cloud storage, IoT gateways for the effective data processing and predictions. Also, the IoT plays a great role in transforming the smart industries to Cyber physical systems (CPS) [5]. Generally, the CPS provide monitoring, computing and also it virtually replaces the machine and integrates the actions together using internet and cloud.

Additionally, CPS enhances its range of features to minimize the energy and network utility. By focusing on energy consumption and safety, many CPS are designed in particular, transportation systems, power grids and smart buildings gained attraction in recent decades [6]. Significantly, IoT is applied in health care systems by employing doctor-on-chip which is a popular cyber physical system that adopts programable insulin pumps implanted to the heart devices [7]. However, due to the rapid increase of network utilization and mobile devices in recent days, IoT enabled cyber physical systems are still facing many security challenges in carrying out reasonable insights [8]. Also, the digital assets generated from CPS are alluring the computer criminals to pose vulnerabilities for stealing the information by injecting ransomware, software bombs and denying actions [9]. Hence to secure the industrial ecosystem, present industries demand “secured architecture” and “secured design” [10]. Also maintaining

integrity, confidentiality, availability and privacy are still challenging in many cyber physical systems [11]. To accomplish the above requirements, several security related algorithms and policies are modeled. But for enhanced protection and privacy, block chain technologies [12] are adopted in IoT-enabled cyber physical systems for its compatibility of validation and integrity. The main objective of this survey to investigate various security challenges and privacy issues associated with the block chain technologies for defending the IoT/CPS networks.
The following are the contributions for this paper:

- Section III explained the IoT-CPS infrastructure with its protocols
- Section IV depicts some IoT-CPS applications
- Section V investigates the recent security threats in IoT-CPS applications
- Section VI and V encompasses block chain concepts and features.

II. RELATED SURVEYS

Several literature retrospect has been put forth to perform a complete survey of IoT/CPS domain. In [13], various privacy and security challenges in Internet of Things are discussed and requirements for resource constrained environment is focused. Later Vikas Hassija et.al [14] presented a detailed view on security challenges and threats associated with the existing technologies and combat techniques in preserving the IoT frameworks. Followed by Hassija et.al, survey focused on security and layer wise issues are presented in [15]. In this study various algorithms based on machine learning, AI and blockchain are suggested to protect the IoT framework against security threats. Extending from [15], IoT security system architecture and issues related to security is discussed in [16]. In this work the underlying framework for enabling the security for home appliances is proposed and several challenges in designing the system is focused. Q.Jing et.al [17] surveyed about various security challenges and privacy issues corresponding to three layers of IoT. Later [18] focused in edge side security threats and corresponding counter measures are suggested.
Various authentication protocols with layer wise applications are discussed in [19]. Followed by [19] layer-wise security threats and countermeasures are investigated along with security threat models in [20]. Likewise, various trust management systems are surveyed with security and threat models in [21]. Moreover, systems on Internet of things with Cyber physical systems are reviewed in [22]. In this work, edge computing is utilized for preserving the security. Also, in [23] several existing works based on ensuring security in IoT-CPS for business insights with CPS vulnerabilities are addressed. In [24], hardware-based security in CPS along with security vulnerabilities are deeply studied. Focusing on Industry 4.0, security threats along with QoS requirements in CPS are reviewed [25]. Blockchain technology is a recent fascinating technology for providing security in IoT-CPS networks. Several surveys have been undergone for providing valuable knowledge in applying blockchain for IoT-CPS frameworks. Bitcoin is a popular cryptocurrency technology operates on blockchain. Several security and privacy issues related to blockchain in executing the bitcoin is discussed in [26]. In [27] holistic review of wide range of applications that are running on IoT-CPS is done. Also, some real-world applications that can benefit from blockchain enabled IoT-CPS is discussed. Additionally, studies on convergence of IoT with Blockchain and issues in cope up with 5G is done in [28]. In addition, with security, studies related to improve the efficiency parameters like lightness, QoS, and robustness is discussed in [29]. As beneficial, studies based on the current state of block chain enabled IoT-CPS is made [30]

III. INTERNET OF THINGS (IOT)-CPS INFRASTRUCTURE AND PROTOCOLS

Cyber-physical Systems (CPS) has acquired a growing amount of attention in academia, industry, and government due to its noteworthy potential on society, environment, and economy. It forms the basis of next-generation computer systems, which integrates computing elements with physical components and processes. Also, CPS encompasses the connected components and software to sense the objects in real world [31] and sends the signals accordingly. In industrial applications, it integrates the devices, motors and the internet to the cloud. Several CPS systems utilizes IoT devices for its enhanced functions such as motor control [32] and defect identification, which is considered as a multidisciplinary engineering design.

3.1 IoT-CPS Infrastructure:-

The high-level architecture of CPS is given in Figure 1. It integrates several computational elements and physical components proposed in [33]. The architecture as depicted in figure 1 clearly shows that different issues and design challenges that will be encountered in mechanical systems [34-35]. Also, the generic layered architecture (figure 2) for IoT-CPS is proposed in [36] which combines the two architectural frameworks proposed in [37-38]. In the generic framework, three layers are outlined in which the first layer performs IoT devices connected to the real-world entities followed by second layer comprises of communication protocols to connect with the network and the third layer meant for cloud services and management of virtual entities

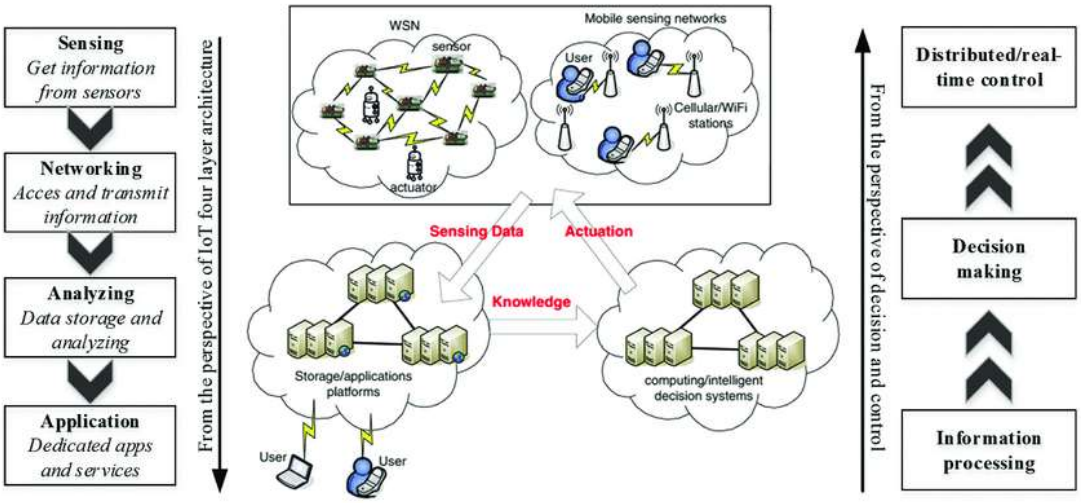
Sensing
Get information from sensors
Networking
Acces and transmit information
Analyzing
Data storage and analyzing
Application
Dedicated apps and services
From the perspective of IoT four layer architecture
WSN
sensor
actuator
Mobile sensing networks
User
Cellular/WiFi stations
Sensing Data
Actuation
Knowledge
Storage/applications platforms
computing/intelligent decision systems
User
User
From the perspective of decision and control
Distributed/real-time control
Decision making
Information processing

Figure 1: High Level architecture of IoT-CPS

.

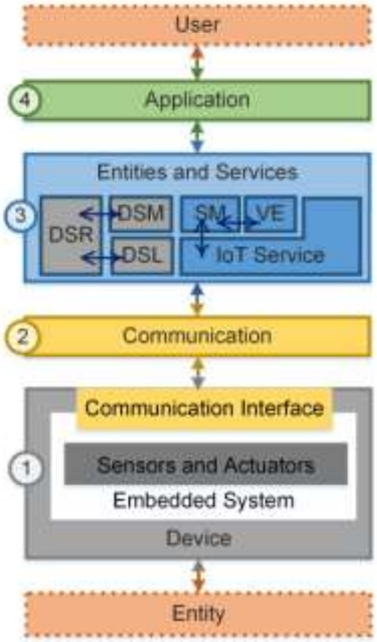

Figure 2: Generic Layered architecture

3.2 IoT-CPS Protocols:-

With the rapid proliferation of sensors and physical devices, the communication systems enable automation and intelligent services to accomplish tasks. Most of present day IoT-CPS systems generally operated in homogenous mode by means of traditional communication protocols. Protocols such as MQTT [39] meant for bandwidth efficiency, CoAP [40] for providing mobility management, AMQP [41] for message transfer in business applications, DCCP [42] for congestion-control are widely adopted in IoT networks. CPS are mostly dealt with heterogenous networks as most of IoT frameworks are unaware of location and installation parameters. Hence the protocols that supports CPS compatibility and QoS support is fairly needed. SPEED [43] ,MMSPEED [44] ,QoS aware protocol[45] are some of protocols widely used in IoT-CPS. SPEED protocol is fairly adopted in IoT-CPS which guarantees end-end delivery and real time adaptability. Generally, the nodes keep track of the information of the neighboring nodes. It decides the path by calculating the speed of the delivery of the information. Usually the routing information of each node contains only the neighborhood information and hence separate memory backup for each node is no longer needed as in DSV[46] and AODV[47].If the acquired speed is greater than the desired speed then the recorded speed is considered as the end-end time and hence QoS is achieved in CPS. MMSPEED is another routing protocol used in industrial CPS systems for providing the factors such as time efficiency and reliable transfer. It uses local neighbor node information and keep track of multiple paths for shortest path finding. Additionally, the routing decisions can be taken based on the end-end time delay for achieving QoS.QoS- aware protocol is designed for reducing the energy consumption and dealing with real time traffic. It efficiently divides the nodes into two queues in which one queue is used for real-time nodes that operate on time-critical manner and next queue is intended for non-time critical nodes MZRP[48] protocol is formally used for secure and energy efficient communication in IoT-CPS as most of the IoT -CPS, the embedded sensors and microcontrollers are battery or solar powered [49]. Also, to cope with the advancements in 5G[50], multi-hop zone routing protocol is designed for energy efficient transfer in industrial systems. It takes the benefit of MAC(Message Authentication Code) and CSMA(Carrier Sense Multiple Access) for secure multi-hop communication.

IV. IOT-CPS APPLICATIONS

The present-day industries are closely been move to be data-driven approach in recent decades, IoT-CPS are becoming popular in many domains:

4.1 Smart Hospital:-

Current CPS technologies in accordance with IoT are progressing the smart healthcare ecosystem. It encompasses the sensors and fog computing for data aggregation in clinical environments [51]. Additionally, [52] authentication and authorization for secure transfer of secret assets is also performed. In healthcare systems, the integrity, availability and privacy of medical records is of utmost importance for effective healthcare CPS. In most of cases, the EHR (Electronic Health record) which is a vital source for processing of data to yield better results for further diagnosis.

4.2 Smart Grid:-

In most of the electrical energy distribution systems, the automation is enabled by deploying effective CPS for real-time monitoring among customers. The smart grid is then accompanied with cyber security solution for securing the data and the network [53]. By adopting IoT in electrical systems, the efficient and economic distribution is guaranteed [54] and several open issues can be addressed. Additionally, smart metering management is an additional feature by integrating wind-energy with the IoT-CPS for electricity generation and transmission [56].

4.3 Smart Home:-

In IoT-CPS based smart homes, due to the development of smart things, the intelligent home system can be built using IoT and Fog computing where the remote monitoring in addition of processing can be done effectively [57]. At the same time the authentication of the devices is also done by incorporating security policies. Moreover, in [58] and [59] several authentication schemes are designed for smart home systems and various security issues are addressed in [60].

4.4 Smart Transportation

For a safe and smart travel, various IoT-CPS innovations are being built using vehicular sensor networks and network connectivity. It acquires signals from nearby vehicles and warns the driver to prevent accidents. Moreover, it sends the information of journey path, nearby petrol stations and traffic areas by utilizing GPS tracking and sensors. Also, some security issues accompanied with smart transportation systems as discussed in [61-62]. IoT-CPS based intelligent transport systems are proposed in [63] where smart and secure travel is addressed. More recently in-build sensors are suggested for detection of road conditions using AI concepts [64].

V. SECURITY THREATS IN IOT-CPS APPLICATIONS

Due to the rapid increase in data utility and network access, the present day IoT-CPS needs security mitigation techniques and combat methods for ensuring data reliability [65]. Some the major security challenges are discussed in this section.

5.1 Boot Process Vulnerability:-

In recent systems, the sequence of the booting process can be compromised by injecting boot process vulnerabiltiy and thus the subsequent operation may be interrupted. It usually disrupts the initial command in the device and alluring the hackers to deny the whole process (Ex. Google nest thermostat) [66-67]. It normally invades the second stage using boot loader. Several mitigation mechanisms are being performed in IoT-CPS against the vulnerability [68-69].

5.2 Hardware Exploitation:-

It usually occurs at the hardware level focusing on ports and flash cards by injecting the modified external devices and affirmed lines to modify the network lines thereby causes potential threats to the IoT-CPS models. Some timing attacks still exists by exploiting the kernel with older values as discussed in [70].

5.3 Chip-Level Exploitation:-

This attacks usually occurs in the chip of IoT-CPS. Hence the devices rely on the chip for processing, it alleviates the whole system and poses security threats to the devices that are connected to the network. So, to combat those issues, several security mechanisms are proposed for providing on-chip security. Some recent researches [71] are made on incorporating AES key in the chip level in order to enhance the security.

5.4 Software Exploitation:-

Some IoT-CPS are encountered with software level security threat. It usually occurs through the code reuse from general purpose computation software and thus easy injection of vulnerabilities might be occur. Recently these kinds of attacks are noticed in stack over flows and also some smart home devices also get compromised [72-73]. Several algorithms [74-75] are proposed but the absence of addressing the resource efficiency still remains challenging.

VI. BLOCK CHAIN CONCEPTS

Block chain technology are now becoming an interesting horizon in providing integrity, security and privacy in many complex applications. It mainly provides integrity among the users in the distributed networks by sharing a decentralized trust among them. Block chain is considered as the trusted party in that network. Moreover, it is the linked chain that consists of blocks connected cryptographically to keep the transactions in a secured way. Also, it is an open ledger that facilitates the “consensus” which is decentralized in nature in turn the modification of data is being restricted among the trusted parties. Hence, tampering of data can be avoided imposed by untrusted third parties and the transactions are virtualized [76-81]. Bitcoin is one among the popular use cases that are operating based on the blockchain technology. But the formal use of blockchain has been adopted by many complex applications and hence the core behind the block chain is too complex [82-92].

Block chain utilizes the concepts of public key cryptosystems for generating digital signatures [93]. For providing the consensus among the nodes, it often employs the proof-of-work algorithm to agree upon the correctness of the information. Mostly blockchain is considered as the peer-to-peer network which holds the duplicated data of the chain, and hence the messages are shared equally among all the peers. It eventually supports the node joining and leaving from the distributed network by accepting the proof-of-work chain even the nodes are in in offline [94]. Usually the nodes collect the new values to form a tree like structure consists of hashed transactions and it is shared with a proof-of-work. Node that are intended to join in the network is given for solving a difficult hash-based proof-of-work for its acceptance. The initial node which solves the problem then broadcasts the solution value among all peers in the network. The new block which solves the proof-of-work is considered as the Miner and it is offered with a reward. The general block structure is given in figure 3. It consists of a header and data with four essential information namely:

i. Hash of the previous block
ii. Timestamp
iii. Nonce
iv. Hash of the merkle tree root

Merkle tree root is the [95] is the hashed tree where each node is named with the hash value of the block. This tree is intended for secure data transfer in the distributed ledger. The output of the tree is then added to the header block accompanied with the hash of the previous block and the corresponding timestamp. Hence to generate 32-bit nonce for cryptographic process the new header is given as a input.

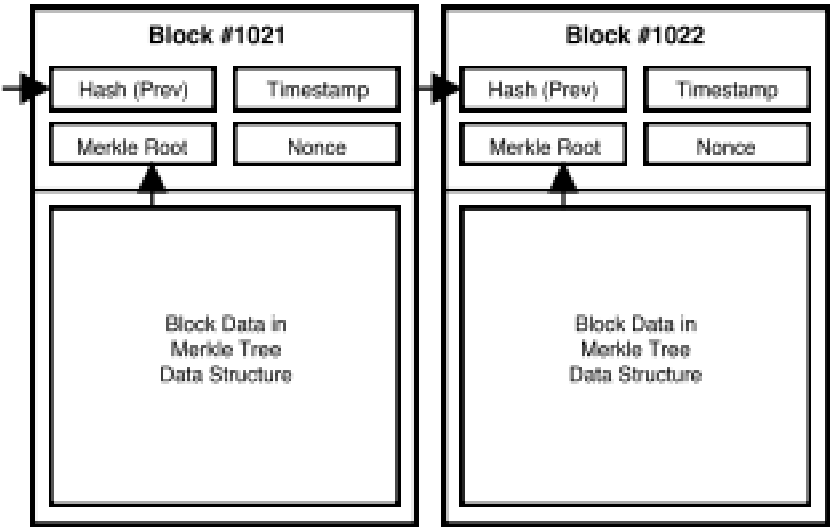

Figure 3. Block structure

VII. SECURITY THREAT ADDRESS USING BLOCK CHAIN

Since Blockchain is a distributed peer to network, each node is connected among the peers in a hashed fashion and the messages are transferred in a secure manner. As shown in figure 4, Block chain is applied to various IoT-CPS in a distributed fashion. Each CPS generates the machine data and its associated values. To implement the business logic in the CPS network, all the transactions are let entered into the smart contract [96] and to satisfy the consensus metric in the network, consensus algorithm [97] is modeled and utilized. Various IoT-CPS applications [98] gets facilitated by block chain technologies. The models proposed by authors in [99] and [100] are some of the industrial CPS applications relying block chain and IoT approaches. A secure way of message transfer using blockchain technologies with IoT-CPS framework is explained in [101-102].

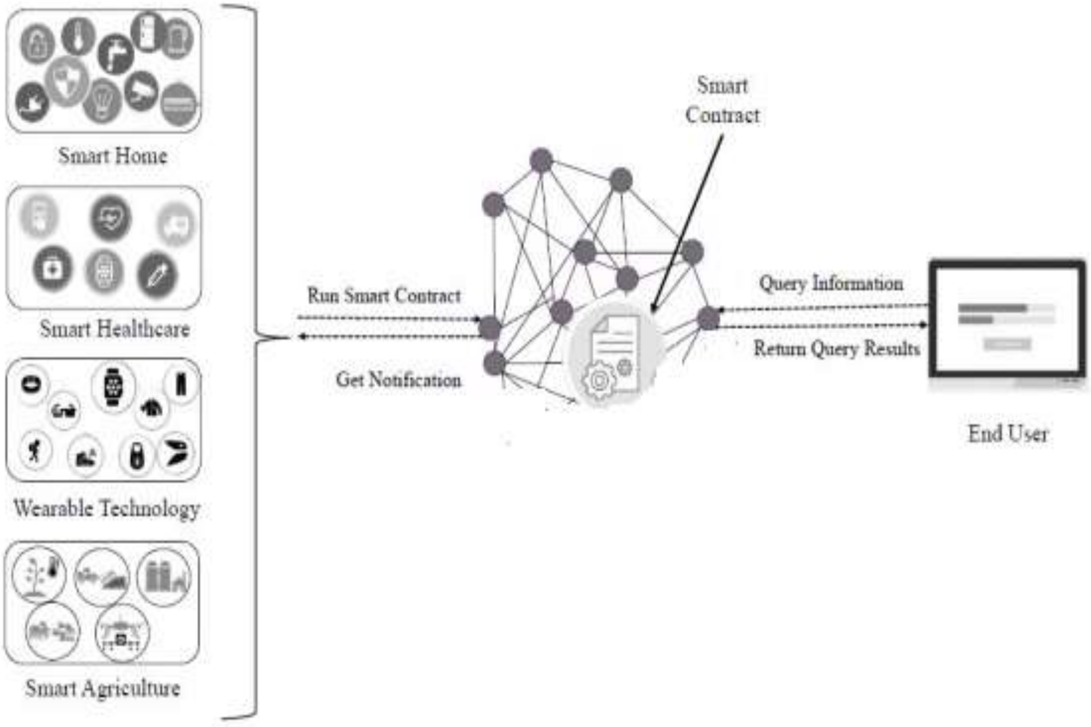

Figure 4. IoT-CPS using block chain technology

VIII. IOT-CPS USING BLOCK CHAIN APPLICATIONS

In [103] block chain methodology is applied in smart home where a single miner is intended to take control of the entire application and also to connect with the external source. IoT-CPS enabled Insurance companies uses the key-value pair for sharing the privacy preserving data that stored periodically in block chain. It then ensures the integrity by comparing the hash values of user data and company data [104]. Significantly, block chain can be applied in record management in hospital sectors where the records are kept secret by sharing the hash values among the peers in the network. It then assures for the feasibility and compliance for its security features in the decentralized applications [105]. Also, it enables transparency among the stack holders in the supply chain [106] in addition with access control, secure data sharing and robustness.

The IoT-CPS based industrial systems utilizes the block chain methodology for mission critical applications such as nuclear plants and irrigation systems. The industrial systems mostly consist of sensors, actuators and controllers where massive amounts of data are generated and transferred. By combining with blockchain, the industrial systems transfer the data among the nodes in a more auditable way by a framework namely Ethereum [107]. It usually adopted for share the information regarding electric usage among the peers by collecting data from home devices. For an efficient energy trading, blockchain technologies are used where the frequency of energy and utilization are considered as the consensus in order to generate the proof-of-work [108]. Also, in some IoT-CPS, blockchain is utilized for distributed control systems where the functional energy blocks are considered as smart contracts [109]. Autonomous vehicles are often considered as the technological innovation where the IoT-CPS plays a vital role in it. Key management in intelligent transport systems [110] is facilitated by blockchain in which key transfer is performed distributive and hash protective. Additionally, refueling instructions and reward based intelligent transportation [111-112] are accomplished by blockchain for security and integrity of services.

Though blockchain has its widespread in variety of IoT-CPS applications, yet it poses some security challenges and privacy issues. Some of the existing works address those issues and suggested some combat methods. For instance, to address the security and privacy issues distributed ledger based framework is proposed in [113], for resolve the time announcements issue in IoT-CPS authors[114] proposed a secure scheme based on blockchain, and high-level security management scheme based on blockchain for ensuring security and integrity is suggested in [115-116]. Also, design challenges and issues in integrating the blockchain and IoT-CPS for high-end applications are discussed in [117]. With the combination of machine learning algorithms, blockchain enhances security by means of device classification [118] in complex application for the detection of malicious nodes. Moreover, for better transaction efficiency and security, credit-based proof-of-work scheme is suggested in [119]. Also, promising security challenges and combat measures in IoT-CPS blockchain applications are discussed in [120].

IX. CONCLUSION

In this survey, an exploratory approach on the security of IoT-CPS framework using blockchain technologies is discussed. The survey starts with the underlying IoT protocols and infrastructures for IoT-CPS is analyzed with the present studies. Secondly, applications that utilized IoT and Cyber physical systems are reviewed with its features. Moreover, various security challenges and privacy issues in IoT-CPS are examined. Then the consideration of blockchain technologies in IoT-CPS for ensuring security and privacy is discussed with its applications. Though the blockchain technologies offered fascinating security features in many applications, some resource constrained applications still challenge blockchain by its complexity in implementing for complex processes.

REFERENCES

1. MahmoudAmmar[a], GiovanniRussello, [b]BrunoCrispo[a], Internet of Things: A survey on the security of IoT frameworks, *Journal of Information Security and Applications Volume 38, February 2018, Pages 8-27*
2. Andrade, Rossana & Maia, Rainara & Linhares de Araújo, Italo & Oliveira, Káthia & Maia, Marcio. (2017).
3. Kalyani, Vijay & Gaur, Priya & Priya, Shubhangi. (2015). IoT: 'Machine to Machine' Application A Future Vision. *Journal of Management Engineering and Information Technology. 2. 2394-8124.*
4. Ungurean, Ioan & Gaitan, Nicoleta-Cristina & Gaitan, Vasile. (2014). An IoT architecture for things from industrial environment. 1-4. *10.1109/ICComm.2014.6866713.*
5. M. Broy,. "Challenges in modeling cyber-physical systems", *Proceedings of the 12th international conference on Information processing in sensor networks, ACM, 2013.*
6. Shih, Chi-Sheng & Chou, Jyun-Jhe & Reijers, Niels & Kuo, Tei-Wei. (2016). Designing CPS/IoT Applications for Smart Buidlings and Cities. IET Cyber-Physical Systems: Theory & Applications. 1. 10.1049/iet-cps.2016.0025.
7. L. Sha, S. Gopalakrishnan, X. Liu and Q. Wang, "Cyber-Physical Systems: A New Frontier," 2008 *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008), Taichung, 2008, pp. 1-9, doi: 10.1109/SUTC.2008.85.*
8. H. He et al., "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence," 2016 *IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, 2016,* pp. 1015-1021, doi: 10.1109/CEC.2016.7743900.
9. EU FP7 E-Crime. The economic impacts of cyber rime, d2.2 executive summary and brief: *Cyber rime inventory and networks in nonict sectors. ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME Deliverable 2.2.pdf.* Accessed, *25 Mar 2016.*
10. H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster. Recommendations for implementing the strategic initiative industrie 4.0: Securing the future of german manufacturing industry, *final report of the industrie 4.0 working group. Forschungsunion, Apr 2013*.
11. A. Colakovi´c, M. Hadˇziali´c, Internet of things (iot): A review of enabling ˇ technologies, challenges, and open research issues, *Computer Networks 144 (2018)* 17–39
12. DanielMinoliBenedictOcchiogrosso, Blockchain mechanisms for IoT security, *Internet of Things, Elsevier,Volumes 1–2, September 2018, Pages 1-13*

13. Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," *Distributed Computing and Internet Technology.* , pp. 33-48, 2015.

14. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in *IEEE Access, vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.*

15. BhabenduKumar et.al, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology*, Internet of Things, Elsevier, Volume 11, September 2020, 100227*

16.] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: A review of system architecture, software, communications, privacy and security, *Internet of Things 1 (2018) 81–98.*

17. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, *Wireless Networks 20 (8) (2014) 2481–2501.*

18. A. Mosenia, N. K. Jha, A comprehensive study of security of internet-ofthings, *IEEE Transactions on Emerging Topics in Computing 5 (4) (2016) 586–602*

19. Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, A survey on security and privacy issues in internet-of-things, *IEEE Internet of Things Journal* 4 (5) (2017) 1250–1258.

20. P. I. R. Grammatikis, P. G. Sarigiannidis, I. D. Moscholios, Securing the internet of things: challenges, threats and solutions, *Internet of Things*.

21. A. K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, *Future Generation Computer Systems* 89 (2018) 110–125.

22. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, *IEEE Internet of Things Journal 4 (5) (2017) 1125–1142*

23. Kim, Nam Yong & Rathore, Shailendra & Ryu, Jung & Park, Jin & Park, Jong. (2018). A Survey on Cyber Physical System Security for IoT: Issues, Challenges, Threats, Solutions. *Journal of Information Processing Systems. 14. 1361 ~ 1384. 10.3745/JIPS.03.0105.*

24. Al-Omary, Alauddin & Alsabbagh, Haider & Al-Rizzo, Hussain. (2018). Survey of Hardware-based Security support for IoT/CPS Systems. *KnE Engineering. 3. 52. 10.18502/keg.v3i7.3072.*

25. H. Xu, W. Yu, D. Griffith and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," in *IEEE Access, vol. 6, pp. 78238-78259, 2018, doi: 10.1109/ACCESS.2018.2884906.*

26. M. Conti, E. Sandeep Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416-3452, Fourthquarter 2018, doi: 10.1109/COMST.2018.2842460.*

27. Rathore, & Mohamed, & Guizani,. (2020). A Survey of Blockchain Enabled Cyber-Physical Systems. Sensors. 20. 282. *10.3390/s20010282.*

28. Hong-Ning Dai, Blockchain for Internet of Things: A Survey, *IEEE Internet of Things Journal, 2019.*

29. S. Cho and S. Lee, "Survey on the Application of BlockChain to IoT," 2019 *International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 2019, pp. 1-2, doi: 10.23919/ELINFOCOM.2019.8706369.*

30. FranCasino et.al, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, *Elsevier, Volume 36, March 2019, Pages 55-81*

31. Lee, E.A., Seshia, S.A., 2011. Introduction to Embedded Systems - A Cyber-Physical Systems Approach. *LeeSeshia.org, First Edition, Version 1.08, 1-15.*

32. Suh, S.C., Carbone, J.N., Eroglu, A.E., 2014. Applied Cyber-Physical Systems. Springer: New York, Heidelberg, Dordrecht & London, 1-3. Tecaru, C.V., Blebea, I., Rad, C.-R., 2014. *Considerations Regarding the Integration-Intrication Process in the Nature and Technology. ACTA Universitatis Cibiniensis, 64(1):82-87.*

33. Mišiü, V., Mišiü, J., 2014. Machine-to-Machine Communications. Architectures, Technology, Standards, and Applications. *CRC Press, Taylor & Francis Group: Boca Raton, London & New York, 1-30.*

34. Tecaru, C.V., Blebea, I., Rad, C.-R., 2014. Considerations Regarding the Integration-Intrication *Process in the Nature and Technology. ACTA Universitatis Cibiniensis, 64(1):82-87*

35. Nie, J., Sun, R., Li, X., 2014. A Precision Agriculture Architecture with Cyber-Physical Systems Design Technology. *Applied Mechanics and Materials, 543-547:1567-1570.*

36. M. A. Pisching, F. Junqueira, D. J. Dos Santos Filho and P. E. Miyagi, "An architecture based on IoT and CPS to organize and locate services," *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, 2016, pp. 1-4, doi: 10.1109/ETFA.2016.7733506.*

37. M.A. Pisching, F. Junqueira, D.J. Santos Filho, and P.E. Miyagi, "Service Composition in the Cloud-based Manufacturing Focused on the Industry 4.0," *in DoCEIS 2015, IFIP AICT 450, 2015, pp. 65-72.*

38. M.A. Pisching, F. Junqueira, D.J. Santos Filho, and P.E. Miyagi, "An Architecture for Organizing and Locating Services to the Industry 4.0," *23rd ABCM International Congress of Mechanical Engineering, Rio de Janeiro, Dezembro 2015. pp. 1-8.*

39. Soni, Dipa & Makwana, Ashwin. (2017). *A SURVEY ON MQTT: A PROTOCOL OF INTERNET OF THINGS(IOT).*

40. L. Coetzee, D. Oosthuizen and B. Mkhize, "An Analysis of CoAP as Transport in an Internet of Things Environment," *2018 IST-Africa Week Conference (IST-Africa), Gaborone, 2018, pp. Page 1 of 7-Page 7 of 7.*

41. G. Caiza, E. S. Llamuca, C. A. Garcia, F. Gallardo-Cardenas, D. Lanas and M. V. Garcia, "Industrial Shop-Floor Integration Based on AMQP protocol in an IoT Environment," 2019 *IEEE Fourth Ecuador Technical Chapters Meeting (ETCM), Guayaquil, Ecuador, 2019, pp. 1-6, doi: 10.1109/ETCM48019.2019.9014858.*

42. Y. Liu and W. Lu, "Improved Fairness Using DCCP in Wireless Sensor Networks," *2009 International Conference on Networking and Digital Society, Guiyang, Guizhou,* 2009, *pp. 141-144, doi: 10.1109/ICNDS.2009.41.*

43. Tian He et al. "SPEED: A stateless protocol for real-time communication in sensor networks". In: *In Proceedings of 23rd International Conference on Distributed Computing Systems (2003), pp. 46–55.*

44. Emad Felemban, Chang-Gun Lee, and Eylem Ekici. "MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and Timeliness in wireless sensor networks*". In: Mobile Computing, IEEE Transactions 5 (2006), pp. 738–754*

45. Kemal Akkaya and Mohamed Younis. "An energy-aware QoS routing protocol for wireless sensor network". In: *In Proceedings of the Workshops in the 23rd International Conference on Distributed Computing Systems (2003), pp. 710–715.*

46. Charles E. Perkins and Pravin Bhagwat, Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for Mobile Computers, in *SIGCOMM Symposium on Communications Architectures and Protocols, (London, UK), pp. 212-225, Sept. 1994.*

47.] C. E. Perkins and E. M. Royer, Ad-hoc On Demand Distance Vector Routing. *In WMCSA'99, New Orleans, LA, February 1999.*

48. Saad Alharthi, Princy Johnson and Martin Randles (May 30th 2020). Secure and Energy-Efficient Communication in IoT/CPS [Online First], *IntechOpen, DOI:10.5772/intechopen.92039.*

49. Mouradian C et al. A comprehensive survey fog computing: State-of-the-art and research challenges. *IEEE Communication Surveys and Tutorials. 2018;20(1):416-464*

50. Alharthi S et al. IoT/CPS ecosystem for efficient electricity consumption. In: Tenth International Green and Sustainable Computing Conference (IGSC), *Alexandria, VA, USA. 2019. pp. 1-7*

51. K. Jaiswal, S. Sobhanayak, B. K. Mohanta, D. Jena, Iot-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi, in: *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2017, pp. 1–4. [23]*

52. S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, Sea: a secure and efficient authentication and 36 authorization architecture for iot-based healthcare using smart gateways*, Procedia Computer Science* 52 (2015) 452–459.

53. Karnouskos, Stamatis. (2011). Cyber-Physical Systems in the SmartGrid. *IEEE International Conference on Industrial Informatics (INDIN). 20 - 23. 10.1109/INDIN.2011.6034829.*

54. A. Meloni, P. A. Pegoraro, L. Atzori, A. Benigni, S. Sulis, Cloud-based IoT solution for state estimation in smart grids: Exploiting virtualization and edge-intelligence technologies*, Computer Networks 130 (2018) 156–165.*

55. Yasin Kabalci et.al, Internet of Things Applications as Energy Internet in Smart Grids and Smart Environments, *electronics*, 2019.

56. Moness, M.; Moustafa, A.M. A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy. *IEEE Internet Things J. 2016, 3, 134–145.*

57. K. Bing, L. Fu, Y. Zhuo, L. Yanlei, Design of an internet of things-based smart home system, in: 2011 *2nd International Conference on Intelligent Control and Information Processing, Vol. 2, IEEE, 2011, pp. 921–924. [19]*

58. U. Satapathy, B. K. Mohanta, D. Jena, S. Sobhanayak, An ecc based lightweight authentication protocol for mobile phone in smart home, in: *2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), IEEE, 2018, pp. 303–308. [20]*

59. S. S. Panda, D. Jena, B. K. Mohanta, A remote device authentication scheme for secure communication in cloud based iot, in: 2019 *2nd International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), IEEE*, 2019, pp. *165–171.*

60. R. K. Kodali, V. Jain, S. Bose, L. Boppana, Iot based smart security and home automation system, in: *2016 international conference on computing, communication and automation (ICCCA), IEEE, 2016, pp. 1286–1289*

61. A. J. Neto, Z. Zhao, J. J. Rodrigues, H. B. Camboim, T. Braun, Fogbased crime-assistance in smart IoT transportation system, *IEEE Access 6 (2018) 11101–11111.*

62. L. F. Herrera-Quintero, J. C. Vega-Alfonso, K. B. A. Banse, E. C. Zambrano, Smart ITS sensor for the transportation planning based on IoT approaches using serverless and microservices architecture, *IEEE Intelligent Transportation Systems Magazine 10 (2) (2018) 17–27.*

63. S. Muthuramalingam, A. Bharathi, N. Gayathri, R. Sathiyaraj, B. Balamurugan, et al., IoT based intelligent transportation system IoT-ITS for global perspective: A case study, in: *Internet of Things and Big Data Analytics for Smart Generation, Springer, 2019, pp. 279–300.*

64. M. R. Dey, U. Satapathy, P. Bhanse, B. K. Mohanta, D. Jena, Magtrack: Detecting road surface condition using smartphone sensors and machine learning, in: *TENCON 2019-2019 IEEE Region 10 Conference (TENCON), IEEE, 2019, pp. 2485–2489.*

65. K. Ly and Y. Jin, "Security Challenges in CPS and IoT: From End-Node to the System," *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, 2016, pp. 63-68, doi: 10.1109/ISVLSI.2016.109.*

66. G. Hernandez, O. Arias, D. Buentello, and Y. Jin, “Smart nest thermostat: A smart spy in your home,” *in Black Hat USA, 2014.*

67. O. Arias, J. Wurm, K. Hoang, and Y. Jin, “Privacy and security in internet of things and wearable devices,” *IEEE Transactions on MultiScale Computing Systems, vol. 1, no. 2, pp. 99–109, 2015.*

68. B. Parno, J. M. McCune, and A. Perrig, “Bootstrapping trust in commodity computers,” in Security and privacy (SP), *2010 IEEE symposium* on, *2010, pp. 414–429.*

69. A. Cui, J. Kataria, and S. Stolfo, “Killing the myth of cisco ios diversity: Recent advances in reliable shellcode design,” in *USENIX Worshop on Offensive Technologies (WOOT*), *2011*

70. “Xbox 360 timing attack,” 2007, [Online]. *http://beta.ivc.no/wiki/index.php/Xbox 360 Timing Attack.*

71. S. Skorobogatov, “Fault attacks on secure chips: from glitch to flash,” *in Design and Security of Cryptographic Algorithms and Devices (ECRYPT II), 2011.*

72. “Critical security flaw: glibc stack-based buffer overflow in getaddrinfo() *(cve-2015-7547),” 2015, [Online]. https://access.redhat.com/articles/2161461.*

73. M. Smith, “Security holes in the 3 most popular smart home hubs and honeywell tuxedo touch,”2015,[Online*].http://www.networkworld.com/article/2952718/microsoftsubnet/security-holes-in-the-3-most-popular-smart-home-hubs-andhoneywell-tuxedo-touch.html.*

74. C. Cowan, C. Pu, D. Maier, J. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, and H. Hinton, “Stackguard: Automatic adaptive detection and prevention of buffer-overflow attacks.” in *Usenix Security, vol. 98, 1998, pp. 63–78.*

75. C. Cowan, S. Beattie, J. Johansen, and P. Wagle, “Pointguard tm: protecting pointers from buffer overflow vulnerabilities,” in *Proceedings of the 12th conference on USENIX Security Symposium, vol. 12, 2003, pp. 91–104*.

76. 43] M. Pilkington, Blockchain technology: principles and applications, in: F.X. Olleros, M. Zhegu (Eds.), *Research Handbook on Digital Transformations, Edward Elger Publishing, Northampton, MA, 2016.*

77. D. Tapscott, A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, *Penguin Random House LLC, New York, NY, 2016.*

78. A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: the blockchain model of cryptography and privacy-preserving smart contracts, in: *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, May 2016, doi:10.1109/SP.2016.55.*

79. A. Wright, P. De Filippi, Decentralized blockchain technology and the rise of Lex cryptographia. *https://ssrn.com/abstract=2580664, March 2015*.

80. X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: *Proceedings of the 2016 Thirteenth Working IEEE/IFIP Conference on Software Architecture (WICSA), Venice, Italy, April 2016,* doi:10.1109/WICSA.2016.21.

81. R.C. Merkle, "A digital signature based on a conventional encryption function". Proceedings of the Advances in Cryptology, CRYPTO '87. *Lecture Notes in Computer Science*. vol. 293. p. 369. doi:10.1007/3-540-48184-2_32.

82. I. Bashir, Mastering Blockchain, *Packt Publishing, Birmingham, UK*, 2017 ISBN 978-1-78712-544-5.

83. N. Atzei, M. Bartoletti, S. Lande, R. Zunino, "A formal model of bitcoin transactions" *eprint.iacr.org*. Available online at https://eprint.iacr.org/2017/1124. pdf

84. K. Brünnler, D. Flumini, T. Studer T., A Logic of Blockchain Updates, in: S. Artemov, A. Nerode (Eds*.), Logical Foundations of Computer Science, Lecture Notes in Computer Science, 10703, Springer, Cham*, 2018.

85. S. N.Artemov, Explicit provability and constructive semantics, Bull. *Symb. Logic 7* (1) (2001) 1–36.

86. C. Decker, R. Wattenhofer, Information propagation in the Bitcoin network, in: *Proceedings of the Thirteenth IEEE International Conference on Peer– to-Peer Computing*, 2013, pp. 1–10.

87. S.I. Matsuo, How formal analysis and verification add security to blockchain-based systems, in: *Proceedings of the Formal Methods in Computer Aided Design (FMCAD), 2017, Vienna, Austria*, Oct. 2017.

88. J. Garay, A. Kiayias, N. Leonardos, The bitcoin backbone protocol: analysis and applications, in: *Proceedings of Eurocrypt*, 2015.

89. R. Dennis, G. Owenson, B. Aziz, A temporal blockchain: a formal analysis, in: *Proceedings of the 2016 International Conference on Collaboration Technologies and Systems (CTS*), Orlando, FL, USA, Nov. 2016.

90. B. Huang, Z. Liu, J. Chen, et al., Behavior pattern clustering in blockchain networks, *Multimed. Tools Appl. 76* (2017) 20099. https://doi.org/10.1007/ s11042-017-4396-4.

91. M.K. Awan, A. Cortesi, Blockchain transaction analysis using dominant sets, in: K. Saeed, W. Homenda, R. Chaki (Eds.), *Proceedings of the Computer Information Systems and Industrial Management. CISIM, Lecture Notes in Computer Science, 10244, Springer, Cham*, 2017.

92. A. Ouaddah, A.A. Elkalam, A.A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT, Europe and MENA Cooperation Advances in Information and Communication Technologies, *Springer International Publishing*, 2017, pp. 523–533.

93. Merkle RC. Protocols for public key cryptosystems. In: 1980 IEEE symposium on security and privacy. *IEEE, 1980*. https:// doi.org/10.1109/SP.1980.10006.

94. Nakamoto S. Bitcoin: *A peer-to-peer electronic cash system*. 2008.

95. M Yu, S Sahraei, S Li, S Avestimehr, S Kannan, Coded Merkle Tree: Solving Data AvailabilityAttacks in Blockchains, *arXiv, 2019 - ui.adsabs.harvard.edu*

96. B. K. Mohanta, S. S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology, in: *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE*, 2018, pp. 1–4.

97. S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, T. K. Patra, Study of blockchain based decentralized consensus algorithms, in: TENCON 2019-2019 *IEEE Region 10 Conference (TENCON), IEEE,* 2019, pp. 908–913.

98. B. K. Mohanta, D. Jena, S. S. Panda, S. Sobhanayak, Blockchain Technology: A Survey on Applications and Security Privacy Challenges, *Internet of Things* (2019) 100107.

99. M. Banerjee, J. Lee, K.-K. R. Choo, A blockchain future for internet of things security: A position paper, *Digital Communications and Networks 4* (3) (2018) 149–160.

100. D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, *Internet of Things 1* (2018) 1–13.

101. U. Satapathy, B. K. Mohanta, S. S. Panda, S. Sobhanayak, D. Jena, A secure framework for communication in internet of things application using hyperledger based blockchain, in: *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT),* IEEE, 2019, pp. 1–7.

102. T. M. Fern´andez-Caram´es, P. Fraga-Lamas, A Review on the Use of Blockchain for the *Internet of Things, IEEE Access 6* (2018) 32979–33001.

103. A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops),* IEEE, 2017, pp. 618–623.

104. Prof. Salil Kanhere, Ali Dorri, Blockchain for Cyberphysical Systems: Applications, Opportunities and Challenges, *UNSW Sydney, -https://tinyurl.com/icbc2019*.

105. Zhang P., Walker M.A., White J., Schmidt D.C., Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps; *Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom);* Dalian, China. 12–15 October 2017; pp. 1–4

106. Zhang P., Walker M.A., White J., Schmidt D.C., Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps; *Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking,* Applications and Services (Healthcom); Dalian, China. 12–15 October 2017; pp. 1–4

107. Huh S., Cho S., Kim S. Managing IoT devices using blockchain platform; *Proceedings of the 19th International Conference on IEEE Advanced Communication Technology (ICACT);* PyeongChang, Korea. 19–22 February 2017; pp. 464–467

108. Liu H., Zhang Y., Yang T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw*. 2018;32:78–83. doi: 10.1109/MNET.2018.1700344.

109. Stanciu A. Blockchain based distributed control system for edge computing; *Proceedings of the IEEE 21st International Conference on Control Systems and Computer Science (CSCS);* Bucharest, Romania. 29–31 May 2017; pp. 667–671

110. Lei A., Cruickshank H., Cao Y., Asuquo P., Ogah C.P., Sun Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, *EEE Internet Things* J. 2017;4:1832–1843. doi: 10.1109/JIOT.2017.2740569.

111. Pedrosa A.R., Pau G. ChargeltUp: On blockchain-based technologies for autonomous vehicles; Proceedings of the ACM *1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems; Munich, German*y. 15 June 2018; pp. 87–92.

112. Singh M., Kim S. Blockchain based intelligent vehicle data sharing framework. *arXiv. 20171708.09721* [Google Scholar] [Ref list]

113. N. M. Kumar, P. K. Mallick, Blockchain technology for security issues and challenges in IoT, *Procedia Computer Science 132* (2018) 1815–1823.

114. K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, Y. Yang, Blockchain based secure time protection scheme in IoT, *IEEE Internet of Things Journal*, 2018

115. Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustiˇsek, Towards decentralized IoT security enhancement: A blockchain approach, *Computers & Electrical Engineering 7*2 (2018) 266–273.

116. B. K. Mohanta, U. Satapathy, S. S. Panda, D. Jena, A novel approach to solve security and privacy issues for iot applications using blockchain, in: *2019 International Conference on Information Technology (ICIT), IEEE,* 2019, pp. 394–399.

117. V. Dedeoglu, R. Jurdak, A. Dorri, R. Lunardi, R. Michelin, A. Zorzo, S. Kanhere, Blockchain technologies for iot, in: Advanced Applications of Blockchain Technology, *Springer, 2020,* pp. 55–89.

118. A. Dorri, C. Roulin, R. Jurdak, S. S. Kanhere, On the activity privacy of blockchain for iot, in: 2019 *IEEE 44th Conference on Local Computer Networks (LCN), IEEE*, 2019, pp. 258–261.

119. J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism, *IEEE Transactions on Industrial Informatics.*

120. A. R. Rao, D. Clarke, Perspectives on emerging directions in using IoT devices in blockchain applications, *Internet of Things (2019)* 100079.