International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Survey Paper Volume-7, Issue-9, September 2020 Regular Edition E-ISSN: 2349-7084

Block-Chain Compliance for IoT Security: A Survey

[1]G.Chandra Sekhar, [2]P. Balamurugan

[1] *Research Scholar, Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, Tamilnadu, India.*

[2]*Professor , Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, Tamilnadu, India.*

Email:[1]sekhar.gillala@gmail.com,[2] pookumbala@gmail.com

Available online at: http://www.ijcert.org

Received: 03/09/2020 *Revised: 17/09/2020* *Accepted: 23/09/2020* *Published: 29/09/2020*

Abstract: Internet of Things would soon become pervasive and ubiquitous due to its uses and easy to manage across various applications. Moreover, IoT has reached the extent of communicating the data from very close proximity to a distant place more than 10Kilometers. The extensive usage of the IoT devices makes the service provider overwhelming in terms of the revenue. It poses challenges to scale the technology to respond to the requests from numerous devices and instances for the actions and decisions to be taken. In addition to the IoT communication, security is a vital activity for every communication across IoT devices. In this paper, an exhaustive study has been conducted on the significance of IoT communication and the challenges involved and the span of security across various layers of the IoT. Furthermore, the survey on Blockchain and the possible integration for IoT communication has been discussed. Finally, the study expresses different integration challenges existing in the present times, which further helps to explore the blockchain adaptability for IoT security.

Keywords: Internet of Things, Blockchain, security, interoperability, scalability, Network Standards, IoT Communications.

1. Introduction

The evolution of IoT has created a lot of opportunities for the various industries to get benefitted from the services and also as service providers. Moreover, users of IoT were benefitted so that their devices collect the data and create the alerts through the analysis of the data. However, it was done at the remote locations and alerted through the integrated applications with the IoT devices. The most suitable use cases are the healthcare industry and large-scale manufacturing industry. Both of them have not only got benefitted but also posed challenges to the research and development community to redefine the solutions as well as to restructure the IoT infrastructure [1]. Moreover, blockchain technology has evolved in the user community to provide security solutions to a superior level beyond the thoughts earlier.

Though the Blockchain was started as a secure transaction service for cryptocurrency businesses [2][3], it has emerged as a tremendous assisting solution for the connected devices, especially IoT. Many kinds of research have proposed various solutions in the form of architectures, frameworks [4][5] with a combination of IoT and Blockchain. As an individual technology IoT and Blockchain had proven, the user community appreciates their services; however, they had posed challenges when the technologies were to be integrated. While the IoT devices have their constraints for resources such as computation, storage, and communication, etc., the industry needs suitable solutions. Furthermore, the tools and services might be

located at various geographic locations, which pose another solution in terms of communication. Communication elements [6] are growing in many ways, from a lower range to a higher range, including bandwidth. But few categories of IoT devices are constrained by the computation, storage, and bandwidth. They need the solutions to be lightweight to solve the issues individually or as a collection. Developing the IoT-blockchain integrated scenario solutions needs to address various constraints to be compatible with the solution to be practically implementable.

In the further work, section 2 discusses the work related to IoT, Blockchain, and attempts to study the adaptability; section 3 reviews the background work which addresses the IoT ecosystem, such as layers, protocols, security, and potential challenges; and section 4 concludes the work.

2. Related Work

The evolution of IoT has reached from the small-scale industries to large-scale industries. Solutions that are developed to address each of these industries vary due to the industry size and volume of operations on a periodical basis. Moreover, the sensitiveness of the generated data, operations carried out, and the genuineness of the files that are stored defines the IoT system's integrity. The use case of the IoT applications in agricultural irrigation systems, Industrial Applications, Traffic Surveillance, home automation, and several other medical and spatial-temporal applications home applications [7]. These applications are countless; furthermore, these IoT services are deployed to optimize application development and Implementation. In [8] Soumya et al. have concentrated on several kinds architecture level applications such as data-centric architecture, incorporation of the architecture constituents into one M2M standard, (iii) drawing chucks of DataTweet services and subsystems, assimilation of vehicular sensors as IoT data source and ITSG5 as "communication medium towards collective vehicle domain and assigned flavor of Named Data Networking (NDN) [9]" for the data broadcasting. Ferrari et al. [10] have experimentally considered the data transfer latency in IoT devices deployed in a wide-reaching scale.

The article focuses on overall data transfer and deliberately expands the cloud data to highlight the key investments associated with the distance and location of cloud servers. Khalid et al.[11] have created an idea of the MQTT topic as a simple "atlas topic" through which things can interact. In [12], Kovacs et al. describe the universal interoperable system for the IoT established on international standards. M2M is used as the data synchronization layer, and the FIWARE system is used as the background layer for data collection and use. Knowledge-based semantic processing agents can further process data.

The concept of a semantic arbitration gateway allows the intelligent transfer of data from one system to another. In addition to semantic execution, we have shown that semantic verification [13] can test a system and ensure its proper functioning. To solve interoperability and scalability [14] [15], define the concept and IoT based on the composition of various IoT components employed in the form of micro-services. The micro-services methodology intends to address the challenge posed by the diversity of terminal functionality, including a consistent approach to physical and logical IoT devices and service models, including standard system address schemes [16]. This model enhances functionality and scalability by integrating various communication protocols into micro-service proxy components, making it easy to modify existing and new system mechanisms, laying the substance for open and dynamic IoT ecosystems.

Chung et al. [17] P2P cloud network services were offered for information on IoT-based disasters. The overall capacity of the system also has the potential to increase if disaster information is available to P2P cloud network service nodes or if the demand for the system increases because it is based on a P2P network that includes resources such as bandwidth, memory space, and so on provided by all customers. About the mobile cloud, "Sergio et al. [18] usually refer to two dimensions: (a) infrastructure-based and (b) short-term mobile cloud. In an infrastructure-based mobile cloud, the hardware infrastructure is stable and provides services to mobile users. Cloud computing can be used as a useful foundation for the Internet of Things and video surveillance technologies and improve their performance".

A comprehensive study was conducted by Razzaq et al. [19], which mentions the types of threats, their level, behaviour, and also have mentioned probable solutions. Cyber threats are increasing in IoT, too, due to its extensive communication usage among

various components. In [20], Samuel et al. have attempted the basis for research efforts to assess the vulnerability classifications of different inherent systems that expose IoT infrastructures and applications to different cyber threat vectors and this new technology. Their discussion will identify the various vulnerabilities inherent in the domains of IoT applications and services. In the configuration of the Smart Metering communication infrastructure, the author has implemented two different attack scenarios. Test results show that vectors created by various threat players can misuse malicious IoT systems.

Tanweer [21] has discussed Blockchain's role in IoT from which the author has derived that the combination of IoT and Blockchain is a novel approach for security. Consensus and characteristics were discussed by Viriyasitavat et al. [22] on variations of system configurations concerning centralization and openness. The study has explored Blockchain's transparency when compared with traditional distributed systems, and Blockchain has guaranteed the property. "Scalable access management in IoT with the combination of IoT was explored by Novo [23]. It provided insight into generic, scalable, and easy-to-manage access control systems for IoT and implemented a proof of concept (PoC) prototype that proves our design".

3. Background

Understanding IoT in its more profound sense elevates the communication's significance to be the inevitable part of the entire system. Subsequently, storage, analytics, decision support, and decision making play their role in keeping the IoT system's integrity. IoT anticipates the sensory system and its connected components to create ease of communication and assist in decision making. IoT offers various services for the applications to defined and deployed for its intention to be accomplished. In general, IoT services [24][25] include most of the networking services but are compatible with the tiny devices, and the communication requirement is a low-bandwidth. The figure depicts the IoT architecture and the significance of communication among various functions [26]. The data that is collected at *stage 1* would be communicated to *stage 2*, which applies the conversion of analog to digital and vice-versa. In *stage 3*, the data is preprocessed and used for subsequent analytics and sent in directions, communicating the decision towards *stage 1* and communicating the data for storage and business analytics towards the cloud data center. Though the communication scenario seems simple, it involves various artifacts such as communication hardware and communication software.

a. IoT ecosystem

The typical IoT ecosystem [27] can be acknowledged as a seven-level model: "marketing, procurement, interconnection, integration, analysis, applications, and services. At a lower level, the market layer or application domain can be Smart Grid, Connected Home, or Smart Health [28] [29]", and so on. The second layer contains "sensors and smart devices that can be considered the heart of the application. The type and distribution of sensors vary depending on the desired application". Illustrations of such sensors are temperature sensors,humiditysensors, electricity meters,orcameras.Thethird layer is aninter connected layer that allows the sensor to communicate with data in a datacenter orcloud.Thedata is combined with other known datasets ,such as geographic data, demographic data, or economic data. Besides, US data is verified using machine learning and data mining techniques.

Running such large-scale distributed applications requires new application-level communication and collaboration software. Examples include "software-defined networking(SDN),service-oriented architecture (SOA), and so on". Finally, the upper-tier consists of services such as energy management, health management,education, transport, etc. Privacy-preserving is essentialfor each of these 7 layers,builton topof each other,so they are shown side by side . Each of the layers was defined with the set of functions and services to be performed, so every protocol, too, was designed but to be performed under certain circumstances. IoT communication requires the protocols to be entirely defined at the data link layer, network layer, and session layer, which considers potential services and functions.

b. IoT Communication Artifacts

Under the definition of the Internet of Things, data communication within each stage and among various stages is a vital activity apart from data processing and data storage. The communication between the IoT modules can either be wired and wireless; hence multiple communication methods are followed by various industries and corporates based on the requirement and performance.

 https://doi.org/10.22362/ijcert/2020/v7/i9/v7i903

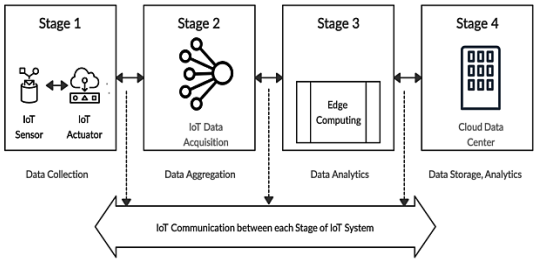

Figure 1. IoT Stages and Communication

c. IoT Communication-specific Protocols

The applications of IoT has reached many sectors such as "Wearables, Smart Home Applications, Health Care, Smart Cities [30][31], Agriculture, Industrial Automation". Every application differs in implementing the hardware and the software; hence the protocols [32] also vary when the system changes.

Table 1. Network Standards and features for IoT communication

Network Standard	Technology	Physical Range*	Features	Battery Life
LWPA	LoRA [33]	10Kms	energy management, pollution control, infrastructure efficiency, disaster prevention	Up to 20 Years
LWPA	NWave	Up to 30Kms	Highest detection accuracy eliminates tripping hazards due to its slender size	Up to 20 Years
LWPA	RPMA	48Kms	Low power consumption, Standalone broadcast channel, Private or public networks	Up to 20 Years
LWPA	SigFox	Upto 50Kms	Plug and play devices and require no pairing or additional infrastructure	Up to 20 Years
3GPP / LTE	LTE-M	Upto 50Kms	The higher data rate, mobility, and works voice over the network	Up to 5 Years
3GPP / LTE	NB-IoT	Upto 22Kms	Low power consumption, low cost	More than 10 Years
3GPP / LTE	NB-CIoT	Up to 100Kms	Low power consumption, low cost, more coverage area	More than 10 Years
3GPP / LTE	NB-LTE	Up to 11Kms	Low power consumption and extended autonomy, Interoperability with LTE network	Up to 10Years
Bluetooth	Bluetooth	100Mts	Low power consumption, Integration with Smartphones	Up to 10Years
802.15.4	ZigBee	Up to	Long battery low	Minimum of 2 Years

 https://doi.org/10.22362/ijcert/2020/v7/i9/v7i903

		100Mts	power consumption, easy to install	
802.15.4	Thread	Up to 20Mts	Long battery low power consumption, easy to install	Up to 2 Years
802.11	WiFi	50Mts	data rate scalability, interference immunity, easy to use	Very Low
802.11ah	WiFiHaLow	Up to 1Km	deficient power consumption and low latency	Low
802.11ax	HEW	Up to 1Km	IoT friendly	Low

d. IoT Layers and Protocols

First IoT layers comprise the "data link, network, and Session/Transport layers", In this regards communication is established among the two IoT elements by data link layer which might be two sensors and gateway device furthermore there are multiple sensors to communicate and aggregate the information before initiates the internet services. The network layer concentrate on the routing information among sensors and part of the network layer. Similarly, session layer protocols authorize the messaging between the several elements of the IoT Communication subsystem.

Table 2. Communication layers in IoT framework

IoT communication layer	Standard	Features
Data Link MAC Layer	IEEE 802.15.4e	Time frame structure, scheduling, synchronization, channel hopping, networking
Data Link MAC Layer	IEEE 802.11ah	Sync frame, efficient bidirectional packet exchange, smaller MAC frame, zero data packet - increased sleep time
Data Link MAC Layer	WirelessHART	Comprehensive, one-off or peer - to - peer security policies
Data Link MAC Layer	Z-Wave	The master controls the slaves, sends them commands, and maintains a schedule for the entire network.
Data Link	ZigBee Smart Energy	Improved security through the symmetric key exchange, scalability with random addressing, and efficient routing from multiple routing systems
Data Link MAC Layer	DASH7	Filter, address, frame format
Network Layer Routing Protocol	RPL	Routing protocol for low power and loss networks
Network Layer Routing Protocol	CARP and E-CARP	Easy packet transfer protocol
Session Layer Protocol	Message queue telemetry transport (MQTT)	Provides connectivity between applications and users at one end, network and communications at the other end, and publishes/joins the structure
Session Layer Protocol	Secure MQTT	Provide easy, feature-based encryption
Session Layer Protocol	Advanced message	Works over TCP and uses a publish/join

	queuing protocol (AMQP)	structure
Session Layer Protocol	Extensible messaging and presence protocol (XMPP)	Supports both insert/join and request/response structure
Session Layer Protocol	Data distribution service (DDS)	Provides various quality standards, such as safety, necessity, priority, durability, reliability

e. Security of IoT Layers and Protocols

Another challenge is to ensure IoT platforms' security, taking in to account all the network layers discussed in the previous sections. Traditional security policies such as cryptography and PKI are not possible on IoT platforms due to their complexity and resource usage. Therefore, new standards are being developed with a lightweight security design. Besides, some IoT standards specialize in security. In this section, we discuss these security standards, drafts, and research. We refer the reader for more information on IoT security standards.

f. Security in IoT Layers

IoT security threats cover all layers ,including data links , network, session, and application layers, that activate the criteria described in this article to incorporate security into their design. Protocols such as "802.15.4e", Wireless Heart, 6Lovpan, and RPL provide certain security features to ensure communication at the appropriate layers. MAC 802.15.4e provides various security modes using "Bit Security Enabled" in the header frame check field. Security requirements include confidentiality, authentication, integrity, access control policies, and secure, time-synchronized communications. The wireless heart standard provides robust security features using the latest and most widely used security techniques. These methods AES-128 encryption for each message, data integrity and authentication, channel hopping protection, data access failure indication and message integrity reporting, and authentication failures. Therefore, it offers different levels of security using the latest working methods, depending on the application.

Some IETF documents related to 6LoWPAN address security threats and 6LoWPAN requirements and offer solutions. For example, "RFC4944" discusses the possibility of duplicating "EUI-64" interface addresses that are considered unique. RFC 6282 addresses security issues caused by issues introduced by "RFC 4944". RFC 6568 discusses possible policies for implementing the security of limited wireless reception devices. Besides, some recent projects [36] discuss tools that ensure the security of 6loWPAN. RPL offers different levels of security through the "Security" field in the name. The ... in this field indicates the security level and the cryptographic algorithm used to encrypt the message. RPL supports data authentication, financial security, re-attack protection, confidentiality, and key management. "Security levels RPL: insecure, pre-installed, and authenticated. RPL threats include selective redirection, bottom hole, sibyl, healthy flooding, whirlwind, and service attacks. RFC 7416 [37]" discusses security threats and potential attacks on RPLs, including their adverse actions, including attacks on confidentiality, availability, and integrity.

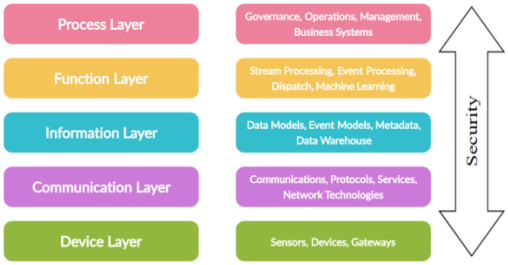

Figure 2. Span of Security in Operations of IoT Layers

g. Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS)

"TLS and DTLS" are two commonly used security standards. They primarily ensure validation, integrity, and privacy in the transport layer, primarily when employed in CoAP protocols. TLP brings security services in excess of TCP transmission, while DTLS provides these services over "UDP or Datagram transmission". TLS and DTLS consist of two sub-layers, registration, and handshake, are which are liable to encapsulation and authentication, correspondingly. "RFC 7925 discusses the detailed procedures used in these standards to ensure security and confidentiality [38]". These standards can provide credentials, signatures, and debugging using traditional security

measures, but they can be modified to accommodate the limited resources used by IoT. Another challenge is to ensure IoT platforms' security across all network layers deliberated in the earlier sections. Traditional security policies such as cryptography and public key infrastructure are not possible on IoT stands due to their difficulty and source usage. Therefore, different standards are being established with an inconsequential security design. Also, some IoT standards specialize in security. This section enlightens to the reader and scholars on several security standards.

h. Trusted Computing Group (TCG)

The "Trusted Computing Group (TCG)" guides providing different IoT applications through various use cases and security policies. Authentication by specific identifiers, shield against middleware contagion via TLS, availability, confidentiality, and integrity using various methods has been proven. These methods comprise the "root of trust for update (RTU) and the Trusted Platform Module (TPM) used in TCG-compliant devices". Classifications support IoT developers choose the mechanisms that support their applications; though, it restrict to the knowledge of the developer to organize the system security with challenges and resources requirements.

i. Simple Authentication and Security Layer (SASL)

A different IETF security system to support authentication in IoT applications on "Simple Authentication and Security Layer (SASL) servers". It separates the request from the verification process and uses diffident messages to confirm clients using application-specific authentication methods. In general, IoT, this structure supports session layer protocols that support "TLS and SSL, MQTT, and AMQP".

j. Authentication and authorization in constrained environments (ACE)

ACE is a security mechanism designed for resource-constrained devices so that it can be used on IoT platforms. It's conceptually like OAuth. However, it is based on "CoAP"-based messaging, which is more compatible with the Internet of Things.

k. IoT Challenges

Despite IoT's effort and principles, evolving an effective IoT application is still not an easy task due to several challenges [39]. These challenges comprise "mobility, reliability, scalability, governance, accessibility, interoperability [40]", costs, and energy development. We will briefly define each of these challenges below.

Mobility: IoT devices need to allocation freely in the background, so they need to change IP addresses and associate to networks according to their location. Therefore, routing protocols require DODAG modification when a node leaves or joins a system, which incurs much overhead.

***Reliability*:** It is essential for emergency response applications that the system works perfectly and correctly delivers all of its specifications. Therefore, the IoT system must be extremely reliable and fast to collect data, communicate with them, and make decisions.

***Scalability*:** With huge number of devices joined in a single IoT application, scalability [41] becomes a major significant challenge. IoT applications need to bring new services and devices that are always connected to the network during device distribution and operation.

***Management*:** Although many protocols for remote device management are discussed, these protocols do not apply to all IoT applications, and therefore management remains a significant challenge. Providers must manage failures, configuration, accounting, performance, and security (FCAPS) of interconnected devices.

***Availability*:** The convenience of IoT platforms have to ensure software and hardware availability to system users and service subscribers. Also, the protocols must be compact so that they can be integrated into compatible IoT devices.

***Interoperability*:** Interoperability requires a variety of tools and protocols to work with each other. This is difficult because IoT systems have many different platforms.

***Complexity and Cost*:** In the face of the relatively low cost of IoT devices such as smart sensors and converters, building an IoT application is still expensive. The complex integration of different protocols and standards does not make Io applications available to the general public.

***Energy Harvesting*:** IoT devices have limited resources, so energy is a critical IoT problem because they must be battery-free for years and can be integrated into the body or environment, making it difficult to replace them. Therefore, get-together energy from free sources or any other energy source and

converting into storage energy seems essential for such devices.

l. Blockchain for IoT

A proven choice of research in IoT security is the use of Blockchain in the development of smart contracts and the security of IoT platforms [42] [43]. "Blockchain is a standard ledger technology that delivers design security starved of relying on a centralized or trusted third party authority [44]. It is conventionally used in Bitcoin and other virtual cryptocurrency platforms but has recently been studied in many different fields, including IoT. IBM and other IoT companies plan to offer blockchain solutions for IoT security. Blockchains can also be used to provide privacy on IoT platforms [45] [46]". Several authors have suggested ways to exchange data between IoT devices and organizations using blockchains securely. Also, there are proposals to build smart contracts using blockchain technology.

m. Challenges using Blockchain for IoT

While the integration of the Blockchain for IoT has been done for few applications successfully, other applications suffer from various compatibility hazards. Various compatibility-level hazards include:

a. Lack of qualitative and quantitative analysis for smart cities when the blockchain framework [47] is used.
b. Lack of extraction of the specifications while pushing the blockchain transmission.
c. Lack of a standard to deal with a single point of failure while using a Blockchain cloud system.
d. Lack of protection blockchain against data forgery attacks while accessing the blocks without PoW [48].
e. Lack of PoC to guarantee reliability.
f. Most of the IoT protocols suffer from computation cost hence degrades the performance, while the integration of Blockchain with IoT seems inevitable [49].

4. Conclusion

The paper has extensively discussed the significance of communication in the Internet of Things. While IoT offers the ease of work for the customers, but they pose the same degree of challenges when a new device or technology is added for the purpose to be served. While scalability addresses such problems, it, in turn, generates other problems such as security for the devices as well as the data that is in the communication across devices. Various IoT standards and protocols were studied to understand the communication insights to develop a scalable system without causing any side effects. In the process, the study has also explored the possibility of the integration of IoT and Blockchain because of the advantage of the later to provide security. Proven with Blockchain's credibility as an individual technology integrating with another needy technology would develop a novel and secure system that would be widely accepted.

5. Acknowledgements

This survey was completed under the guidance and continuous support of our Research guide in selecting the papers and analysis the concept and understanding the subject line we thank to all the peoples who are directly and indirectly helped me to write this research survey paper.

References

[1] Zhu, Yongxu, Gan Zheng, and Kai-Kit Wong. "Blockchain-Empowered Decentralized Storage in Air-to-Ground Industrial Networks." IEEE Transactions on Industrial Informatics15, no. 6 (2019): 3593-601. doi:10.1109/tii.2019.2903559.

[2] Kogure, K. Kamakura, T. Shima, and T. Kubo, "Blockchain Technology for Next Generation ICT," Fujitsu Sci. Tech. J., vol. 53, no. 5, pp. 56–61, 2017.

[3] Tosh, Deepak K., Sachin Shetty, Xueping Liang, Charles A. Kamhoua, Kevin A. Kwiat, and Laurent Njilla. "Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack." 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), 2017. https://doi.org/10.1109/ccgrid.2017.111.

[4] Ding, Sheng, Jin Cao, Chen Li, Kai Fan, and Hui Li. "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT." IEEE Access7 (2019): 38431-8441. doi:10.1109/access.2019.2905846.

[5] Xu, Xiwei, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, and Paul Rimba. "A Taxonomy of Blockchain-Based Systems for Architecture Design." 2017 IEEE

International Conference on Software Architecture (ICSA), 2017. https://doi.org/10.1109/icsa.2017.33.

[6] Al-Sarawi, Shadi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi. "Internet of Things (IoT) Communication Protocols: Review." 2017 8th International Conference on Information Technology (ICIT), 2017. https://doi.org/10.1109/icitech.2017.8079928.

[7] Gigli, Matthew, and Simon Koo. "Internet of Things: Services and Applications Categorization." Advances in Internet of Things 01, no. 02 (2011): 27–31. https://doi.org/10.4236/ait.2011.12004.

[8] Datta, Soumya Kanti, Christian Bonnet, Rui Pedro Ferreira Da Costa, and Jerome Harri. "DataTweet: An Architecture Enabling Data-Centric IoT Services." 2016 IEEE Region 10 Symposium (TENSYMP), 2016. https://doi.org/10.1109/tenconspring.2016.7519430.

[9] Zhu, Konglin, Zhicheng Chen, Wenke Yan, and Lin Zhang. "Security Attacks in Named Data Networking of Things and a Blockchain Solution." IEEE Internet of Things Journal6, no. 3 (2019): 4733-741. doi:10.1109/jiot.2018.2877647.

[10] Ferrari, P., E. Sisinni, D. Brandao, and M. Rocha. "Evaluation of Communication Latency in Industrial IoT Applications." 2017 IEEE International Workshop on Measurement and Networking (M&N), 2017. https://doi.org/10.1109/iwmn.2017.8078359.

[11] Khaled, Ahmed E., and Sumi Helal. "Interoperable Communication Framework for Bridging RESTful and Topic-Based Communication in IoT." Future Generation Computer Systems 92 (2019): 628–43. https://doi.org/10.1016/j.future.2017.12.042.

[12] Kovacs, Erno, Martin Bauer, Jaeho Kim, Jaeseok Yun, Franck Le Gall, and Mengxuan Zhao. "Standards-Based Worldwide Semantic Interoperability for IoT." IEEE Communications Magazine 54, no. 12 (2016): 40–46. https://doi.org/10.1109/mcom.2016.1600460cm.

[13] Qu, Chao, Ming Tao, Jie Zhang, Xiaoyu Hong, and Ruifen Yuan. "Blockchain Based Credibility Verification Method for IoT Entities." Security and Communication Networks2018 (2018): 1-11. doi:10.1155/2018/7817614.

[14] Novo, Oscar. "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT." IEEE Internet of Things Journal 5, no. 2 (2018): 1184–95. https://doi.org/10.1109/jiot.2018.2812239.

[15] Vresk, Tomislav, and Igor Cavrak. "Architecture of an Interoperable IoT Platform Based on Microservices." 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016. https://doi.org/10.1109/mipro.2016.7522321.

[16] Negka, Lydia, Georgios Gketsios, Nikolaos A. Anagnostopoulos, Georgios Spathoulas, Athanasios Kakarountas, and Stefan Katzenbeisser. "Employing Blockchain and Physical Unclonable Functions for Counterfeit IoT Devices Detection." Proceedings of the International Conference on Omni-Layer Intelligent Systems - COINS 19, 2019. doi:10.1145/3312614.3312650.

[17] Chung, Kyungyong, and Roy C. Park. "P2P Cloud Network Services for IoT Based Disaster Situations Information." Peer-to-Peer Networking and Applications 9, no. 3 (2015): 566–77. https://doi.org/10.1007/s12083-015-0386-3.

[18] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure Integration of IoT and Cloud Computing." Future Generation Computer Systems 78 (2018): 964–75. https://doi.org/10.1016/j.future.2016.11.031.

[19] Abdur, Mirza, Sajid Habib, Muhammad Ali, and Saleem Ullah. "Security Issues in the Internet of Things (IoT): A Comprehensive Study." International Journal of Advanced Computer Science and Applications 8, no. 6 (2017). https://doi.org/10.14569/ijacsa.2017.080650.

[20] Tweneboah-Koduah, Samuel, Knud Erik Skouby, and Reza Tadayoni. "Cyber Security Threats to IoT Applications and Service Domains." Wireless Personal Communications 95, no. 1 (2017): 169–85. https://doi.org/10.1007/s11277-017-4434-6.

[21] Alam, Tanweer. "Blockchain and Its Role in the Internet of Things (IoT)," 2019. https://doi.org/10.31219/osf.io/cmza5.

[22] Viriyasitavat, Wattana, and Danupol Hoonsopon. "Blockchain Characteristics and Consensus in Modern Business Processes." Journal of Industrial Information Integration 13 (2019): 32–39. https://doi.org/10.1016/j.jii.2018.07.004.

[23] Kaivan Karimi, Gary Atkinson, "What the Internet of Things (IoT) Needs to Become a

Reality", *White paper of free scale and Arm*. 2014. p. 1–16.

[24] Zhang, Yu, and Jiangtao Wen. "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things." Peer-to-Peer Networking and Applications 10, no. 4 (2016): 983–94. https://doi.org/10.1007/s12083-016-0456-1.

[25] Kum, Seung Woo, Jaewon Moon, Taeboem Lim, and Jong Il Park. "A Novel Design of IoT Cloud Delegate Framework to Harmonize Cloud-Scale IoT Services." 2015 IEEE International Conference on Consumer Electronics (ICCE), 2015. https://doi.org/10.1109/icce.2015.7066399.

[26] Angin, Pelin, Melih Burak Mert, Okan Mete, Azer Ramazanli, Kaan Sarica, and Bora Gungoren. "A Blockchain-Based Decentralized Security Architecture for IoT." Lecture Notes in Computer Science Internet of Things – ICIOT 2018, 2018, 3-18. doi:10.1007/978-3-319-94370-1_1.

[27] T. Salman, and R. Jain, "A Survey of Protocols and Standards for Internet of Things," Advanced Computing and Communications, Vol. 1, No. 1, March 2017.

[28] Lee, Jay, Moslem Azamfar, and Jaskaran Singh. "A Blockchain Enabled Cyber-Physical System Architecture for Industry 4.0 Manufacturing Systems." Manufacturing Letters20 (2019): 34-39. doi:10.1016/j.mfglet.2019.05.003.

[29] Ali, Jawad, Toqeer Ali, Yazed Alsaawy, Ahmad Shahrafidz Khalid, and Shahrulniza Musa. "Blockchain-based Smart-IoT Trust Zone Measurement Architecture." Proceedings of the International Conference on Omni-Layer Intelligent Systems - COINS 19, 2019. doi:10.1145/3312614.3312646.

[30] Ganchev, I., Zhanlin Ji, and M. Odroma. "A Generic IoT Architecture for Smart Cities." 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014), 2014. https://doi.org/10.1049/cp.2014.0684.

[31] T. hoon Kim, C. Ramos, S. Mohammed, Smart city and iot, Future Generation Computer Systems 76 (2017) 159 – 162. https://doi.org/10.1016/j.future.2017.03.034

[32] Skouby, K E, and P Lynggaard. "Smart Home and Smart City Solutions Enabled by 5G, IoT, AAI and CoT Services." 2014 International Conference on Contemporary Computing and Informatics (IC3I), 2014. https://doi.org/10.1109/ic3i.2014.7019822.

[33] Lauridsen, Mads, Huan Nguyen, Benny Vejlgaard, Istvan Z. Kovacs, Preben Mogensen, and Mads Sorensen. "Coverage Comparison of GPRS, NB-IoT, LoRa, and SigFox in a 7800 km² Area." 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), 2017. https://doi.org/10.1109/vtcspring.2017.8108182.

[34] Chen, Hao, Xueqin Jia, and Heng Li. "A Brief Introduction to IoT Gateway." IET International Conference on Communication Technology and Application (ICCTA 2011), 2011. https://doi.org/10.1049/cp.2011.0740.

[35] Rasid, M F A, W M W Musa, N A A Kadir, A M Noor, F Touati, W Mehmood, L Khriji, A Al-Busaidi, and A Ben Mnaouer. "Embedded Gateway Services for Internet of Things Applications in Ubiquitous Healthcare." 2014 2nd International Conference on Information and Communication Technology (ICoICT), 2014. https://doi.org/10.1109/icoict.2014.6914055.

[36] Chze, Paul Loh Ruen, and Kan Siew Leong. "A Secure Multi-Hop Routing for IoT Communication." 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014. https://doi.org/10.1109/wf-iot.2014.6803204.

[37] Reyna, Ana, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. "On Blockchain and Its Integration with IoT. Challenges and Opportunities." Future Generation Computer Systems88 (2018): 173-90. doi:10.1016/j.future.2018.05.046.

[38] Pustišek, Matevž, Dejan Dolenc, and Andrej Kos. "LDAF: Low-Bandwidth Distributed Applications Framework in a Use Case of Blockchain-Enabled IoT Devices." Sensors19, no. 10 (2019): 2337. doi:10.3390/s19102337.

[39] Makhdoom, Imran, Mehran Abolhasan, and Wei Ni. "Blockchain for IoT: The Challenges and a Way Forward." Proceedings of the 15th International Joint Conference on E-Business and Telecommunications, 2018. doi:10.5220/0006905604280439.

[40] Desai, Pratikkumar, Amit Sheth, and Pramod Anantharam. "Semantic Gateway as a Service Architecture for IoT Interoperability." 2015 IEEE International Conference on Mobile Services, 2015. https://doi.org/10.1109/mobserv.2015.51.

[41] Duncan, Bob, Andreas Happe, and Alfred Bratterud. "Enterprise IoT Security and

Scalability." Proceedings of the 9th International Conference on Utility and Cloud Computing - UCC 16, 2016. https://doi.org/10.1145/2996890.3007875.

[42] Ahram, Tareq, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba. "Blockchain Technology Innovations." 2017 IEEE Technology & Engineering Management Conference (TEMSCON), 2017. https://doi.org/10.1109/temscon.2017.7998367.

[43] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things." IEEE Access 4 (2016): 2292–2303. https://doi.org/10.1109/access.2016.2566339.

[44] Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Chi Yang. "The Blockchain as a Decentralized Security Framework [Future Directions]." IEEE Consumer Electronics Magazine 7, no. 2 (2018): 18–21. https://doi.org/10.1109/mce.2017.2776459.

[45] Biswas, Sujit, Kashif Sharif, Fan Li, Boubakr Nour, and Yu Wang. "A Scalable Blockchain Framework for Secure Transactions in IoT." IEEE Internet of Things Journal6, no. 3 (2019): 4650-659. doi:10.1109/jiot.2018.2874095.

[46] Košťál, Kristián, Pavol Helebrandt, Matej Belluš, Michal Ries, and Ivan Kotuliak. "Management and Monitoring of IoT Devices Using Blockchain." Sensors19, no. 4 (2019): 856. doi:10.3390/s19040856.

[47] Risius, Marten, and Kai Spohrer. "A Blockchain Research Framework." Business & Information Systems Engineering 59, no. 6 (2017): 385–409. https://doi.org/10.1007/s12599-017-0506-0.

[48] Gervais, Arthur, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. "On the Security and Performance of Proof of Work Blockchains." Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS16, 2016. https://doi.org/10.1145/2976749.2978341.

[49] Maroufi, M., Abdolee, R., & Tazekand, B. (2019). "On the Convergence of Blockchain and Internet of Things (IoT) Technologies". Journal of Strategic Innovation and Sustainability, 14(1). https://doi.org/10.33423/jsis.v14i1.990.

AUTHOR PROFILES

G Chandra Sekhar received M.Tech Degree in Computer Science and Engineering from Jawaharlal Nehru Technological University Hyderabad. He is pursuing Ph.D degree from Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, Tamilnadu, India. He is working as an Assistant Professor in the department of Computer Science and Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad. His current research interests include IoT, Blockchain, Wireless Sensors Networks and Network Security.

Dr. P. Balamurugan is Professor of Department of Computer Science and Engineering at Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Chennai, Tamilnadu, India. He passed BE in Computer Science and Engineering from Madurai Kamaraj University in 2003 and ME in Computer Science and Engineering from Manonmaniam Sundaranar University in 2006. He completed his doctorate from Anna University in 2013. He obtained GATE score in 2003. He is recognized as a Supervisor for Ph.D Programme and M.Tech(By Research) in Information and Communication Engineering for ANNA UNIVERSITY and Vel Tech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology. He is the member of IEEE, ACM, ISTE etc... He is trained certificate holder of 'High Impact Teaching Skills' through WIPRO MISSION 1OX and Trained Evaluator of NBA and ABET. He is in the reviewer member of 6 International/National Journals. His research interest is mainly in networks, ad hoc and sensor networks, and data structures. He has filed and published more than five patents. He published books "Theory of Computation" and "Problem Solving and python Programming". He published a number of research papers in international journal and presented papers in international conferences. He has done a number of consultancy works at various organizations. He has delivered a number of guest lectures at various organizations. He also organized number of workshop, conference and seminars.

