Challenges of Blockchain Technology in Context Internet of Things: A Survey

Mohammad Qatawneh
The University of Jordan
Department of Computer Science, King Abdullah II School for Information Technology, KASIT, Amman, Jordan

Wesam Almobaideen
The University of Jordan
Department of Computer Science, King Abdullah II School for Information Technology, KASIT, Amman, Jordan

Orieb AbuAlghanam
The University of Jordan
Department of Computer Science, King Abdullah II School for Information Technology, KASIT, Amman, Jordan

ABSTRACT
The Internet of Things (IoT) is a combination of communication, information, and embedded technology that truly make up an IoT ecosystem. The designing of the IoT ecosystem that includes different technologies often be complex. This complexity introduces challenges to keeping the IoT secure, protecting the IoT from disclosure to unauthorized parties, ensuring information integrity and so on. This paper presents a comprehensive survey of the challenges and security consideration of the integration of both IoT architectures and blockchain technology which is basically a secure distributed database over a peer to peer architecture. It starts by discussing the characteristics of the IoT, its architectures, their limitations and the role of cloud and fog computing to overcome these limitations. Then it provides an overview of a blockchain technology, its applications, how does it work, and finally the contribution of an integrated blockchain as a solution to security and privacy challenges in IoT.

Keywords
Blockchain, Consensus, Decentralization, IoT, Immutability

1. INTRODUCTION
Today, Internet of Things (IoT) is being implemented in many fields like medical care, smart university, smart city, smart home, etc. [1][2]. It can be viewed as an information system made up of things, networks, data, and services. Such things may be wireless sensors, traditional computers, cameras, home appliances, tablets, smart phones, vehicles, humans, etc. that are connected over a network which can be wired or wireless. These things may gather, process, and upload a large amount of data to the internet and used to initiate service. The Internet of Things has many characteristics which are discussed below [1][2]:

1. **Interconnectivity**: interconnectivity empowers the internet of things to interconnect anything such as home appliances, smartphones, vehicles, sensors, traditional computers, etc. with different communication and information platforms.
2. **Heterogeneity**: The IoT comprises heterogeneous devices and networks that are based on different technologies.
3. **Dynamic nature**: The IoT devices collect a huge amount of data from the environment, this can be achieved with dynamic changes that take place around the IoT devices.
4. **Intelligence**: The IoT integrates different software, hardware, and computing that makes it smart, when dealing with any situation such as interacting with other devices to carry out a specific service.
5. **Scalability**: The Interconnectivity, heterogeneity, and dynamic nature makes the Internet of things scalable, so that the IoT must be capable to support a huge number of connected devices or things, various types of resources, users and applications.

The internet of things can be also defined from the ecosystem's point of view as a system of systems that combines the following three different technologies: communication, information, and embedded. The designing and implementing such systems that include various software, hardware, and applications will mostly be complex. Therefore, this complication leads to IoT security and privacy concerns such protecting data from disclosure, ensuring information integrity, etc. [54]. Among the IoT devices, wireless sensors are essential components because they are widely used in several applications [52][53]. However, sensors are resource-constrained devices with restricted battery power, memory size, communication bandwidth, and processing performance which involves shortcomings related to security and privacy. The classical IoT security and privacy techniques or mechanisms tend to be expensive in terms of high energy consumption and processing overhead. In addition to that authentication process in IoT is only done via the central server thereby leading to security and privacy concerns [54]. Therefore, device spoofing, false authentication, less reliability in data sharing are major concerns.

The paper's contribution is as follow:

- Discussing recent articles which investigate IoT architectures, their applications and challenges, and the integration of cloud and fog computing with IoT.
- Illustrating the benefits from the integration of the fog and cloud with the IoT.
- Discussing the contribution of Blockchain (BC) as a solution to IoT security and privacy concerns.

The rest of the paper is organized as follows. Section 2 presents and compare between different IoT architectures, and their challenges. Section 3 presents the theoretical background needed to understand how does BC work. Section 4 presents a study of Blockchain technology and the debate of whether BC technology is a good solution for addressing the IoT security

and privacy concerns. Section 5 concludes the paper.

2. ARCHITECTURE OF IOT

The combination of things, networks, data and services forms the IoT architecture. However, IoT architectures may vary based on the type of application which intend to implement. Therefore, there is no common IoT architecture which is accepted universally. Consequently, various IoT architectures or models have been proposed by different authors. These architectures can be categorized into Five groups: Three-Layer Architecture, Four-Layer Architecture, Five-Layer Architecture, Cloud-based Architecture and finally, Fog-Based Architecture.

2.1. Three-Layer Architecture

This architecture is basic in design and comprises the perception layer, network layer, and the application layer as shown in Figure 1 (a) [2][3][4][5]. The perception layer which may have different IoT devices such wireless sensors, vehicles, etc. that are used for gathering, monitoring, uploading information, using different technologies. The Network layer: The role of this layer is perform the task of routing data to IoT hubs and other network devices through the internet using different communication technologies such as Wi-Fi, Bluetooth etc. [4][5]. Finally, the Application layer is responsible for delivering application specific services to the user [6][7]. This layer defines several IoT applications such as smart homes, smart cities, smart health etc. [52][53].This architecture represents the basic and the simple idea of the IoT technology and was introduced in the early stage of the emergence of this technology. Therefore, the simplicity of this architecture cannot be used for many applications that produces a huge amount of data [7]. This has given rise to a new architecture which called the four-layer architecture.

2.2. Four-Layer Architecture

The Four-Layer Architecture includes the following four layers: the perception layer, the network layer, the middleware layer, and application layer as shown in Figure 1 (b). The middleware layer is placed in between the network and application layers in order to improve the IoT services [1][2][8]. The perception layer comprises various IoT devices such as wireless sensors, traditional computers smart phones, etc. Both application and network layers accomplish similar functions to other architectures [53].

2.3. Five-Layer Architecture

This architecture comprises five layers [3-6], the perception, transport, processing, application, and business layers as shown in Figure 1 (c). The function of both sensing and application layers are the same as discussed in section 2.1. The transport layer responsible for transferring the data gathered by the sensing layer to the processing layer via 3G, LAN, NFC, etc. The fourth layer in five-layer architecture is the middle layer which responsible for storing, and processing the data. Finally, the business layer which responsible for managing the IoT applications. As the Internet of Things is characterized by limited battery power, memory size, communication bandwidth, and processing performance, it suffers from many challenges such as performance, high energy consumption, security, etc. Therefore, the integration of the IoT with the cloud, known as Cloud-Based Architecture, is one of the attracting architectures to handle these issues [22].

2.4. Cloud- based Architecture

Cloud computing can be viewed as a model which consists of a large shared pool of computer system resources such as servers, storage, etc. to provide different resource sharing services such as hosting, computation, etc. for businesses and users [1][9][10][11][26][28].

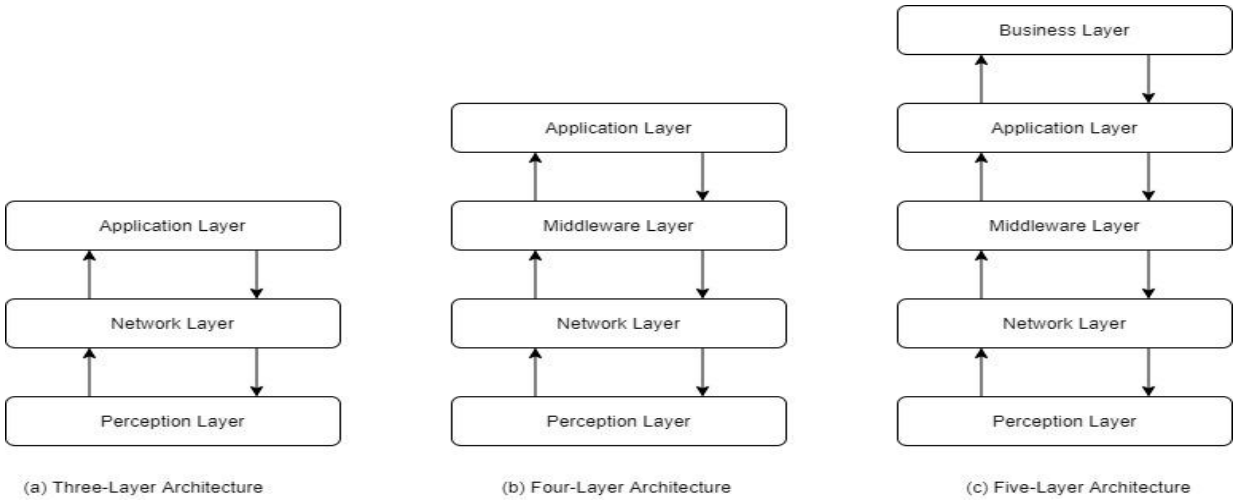

Figure 1: Architectures of IoT

Cloud computing can be classified into private, public, community, and hybrid. Cloud-Based Architecture has into three layers: The cloud layer, gateway layer, and the perception layer as shown in Figure 2. The cloud layer is responsible for controlling and managing different IoT services as well as storing and processing the data [17]. The perception layer comprises different IoT devices such as sensors for data gathering and control. The gateway layer comprises various communication devices, such as gateways, routers, etc. that perform data transmission between cloud and IoT devices in perception layer [14] [17].

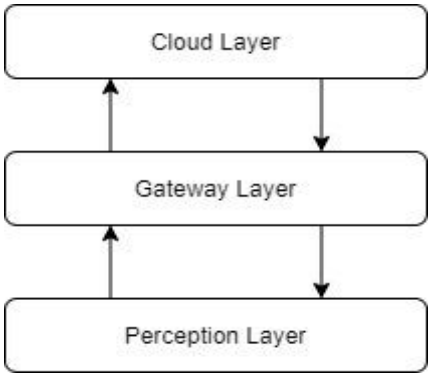

Figure 2: Cloud-based Architecture

The idea of integration of both IoT and cloud computing can be applied because their properties are complementary [9], as shown in Table 1.

Table 1. Complementary properties of Cloud and Internet of Things

Parameter	**Cloud**	**IoT**
Displacement	Centralized	Distributed
Reachability	Everywhere	Restricted
Element of the system	Virtual hardware and software resources.	Things such as wireless sensors, computers, etc.
Storage	Unlimited storage	Restricted
Data	Means to manage data	Source of data
Role of the system.	Acts as a means for delivering services.	Point of gathering different technologies

The cloud-based architecture has contributed significantly to the improvement of various applications such as healthcare, smart environment, etc. [52][53]. However, the Cloud-Based Architecture faces many challenges such as latency, network bandwidth, intermittent connectivity, and resource dependent devices. These challenges are discussed below:

1. Low latency: Many IoT real time applications such as vehicle-to-vehicle communication requires the latency between the IoT devices like sensor node and control node to be below milliseconds [17].
2. Network bandwidth: Gathering, processing and uploading a huge amount of data require more network bandwidth. Moreover, as the number of devices connected to the internet of things, the need for high network bandwidth increases.
3. Intermittent Connectivity: Sometimes it is difficult for the cloud provider to provide uninterrupted services to IoT devices that require continual connectivity to the cloud [17].

The integration of IoT technology with cloud computing brings many benefits to different IoT applications. However, Cloud-Based Architecture is not an optimal solution that can handle the above challenges. Therefore, it is better to put some kind of devices (gateways, bridges, routers, and so on) close to sensors that provide high storage, and processing power [23] [24] in order to minimize or avoid the network latency, intermittent connectivity, and resource dependent devices. Therefore, a new architecture is need to overcome these issues, fog-based architecture comes into play.

2.5. Fog-based Architecture

The fog computing paradigm was introduced in 2012 [12]. It can be defined as a logical extension of the cloud computing that provides services to IoT systems such as processing, storage, and networking services between end devices and traditional cloud servers. The main goals of fog computing in the internet of things is to improve performance, reduce the amount of data transferred to the cloud [25]. Fog-Based Architecture has three layers, the perception layer, the fog layer and the cloud layer as show in Figure 3. The perception layer comprises mobile such as smart phone, laptop, tracker, camera etc. and fixed IoT devices like home appliances, wireless sensors, etc. These devices may gather and upload a huge amount of data.

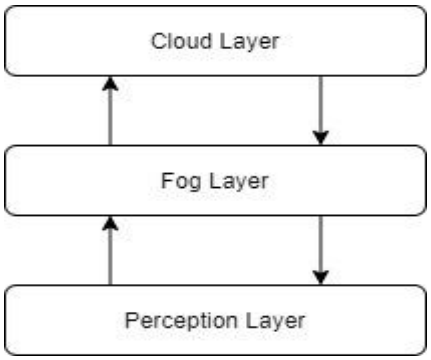

Figure 3: Fog-based Architecture

The fog layer includes several network equipment's like routers, bridges, gateways, switches, etc. augmented with computational power, and servers that can be deployed anywhere [3]. The cloud layer is responsible for controlling and managing IoT different services and applications. It also provides centralized storage, processing, analyzing and access for huge data. Table 2 shows a summary of related articles that have discussed the integration of the IoT with fog and cloud computing. The integration of fog computing with IoT brings many benefits such as service continuum, low latency, heterogeneity, scalability, etc. Table 3 shows the differences between cloud and for computing.

The benefits of integration fog computing with IoT are summarized below:

1) Fog Enables a Service Continuum: The integration of fog computing with IoT provides and enables a service continuum for different real time application [13][14][17].
2) Low latency: Due to the fact that fog is closer to end IoT devices, it provides lower latency when processing the data of end devices [24] [15].
3) Scalability: The closeness of fog layer (fog devices) to perception layer (IoT devices) enables scaling a huge number of connected things, applications and services.
4) Heterogeneity: The integration of fog computing and IoT enriches one of the key characteristics of IoT which is heterogeneity by allowing the collaboration of different hardware platforms among multiple services [14] [16].

Table 2. A summary of related works that discussed the integration of both cloud and fog with IoT

Author	Year	Fog	Cloud	Contribution
Flavio B. et al [16]	2014	X		Suggests a distributed architecture for fog computing.
Alessio B. et al [9]	2015		X	Presents a literature survey about the integration of both cloud computing and internet of things.
Rukhsana T. et al [17]	2018	X		Provide a comprehensive discussion about the architecture and security of fog computing.
Azhra G.	2017		X	Presents a literature review on cloud security issues.
Hany A. et al [25]	2017		X	Provides an overview of the integration of cloud with IoT.
Liu Y. et al [14]	2017	X		Presents the characteristics of fog computing and differences from other similar computing models.
Rashid D. et al [27]	2018		X	Presents a study on cloud computing paradigm.
Yashpalsinha J. [28]	2012		X	Presents a study of challenges in cloud.
Jianli P. et al [12]	2018	X	X	Provide a literature survey about the challenges in of Cloud and fog computing paradigms.
Babatunji Q. et al. [1]	2018	X		Provides fog/edge computing-based IoT framework.

Table 3. The differences between cloud and fog computing

Parameter	Cloud Computing	Fog Computing
Service Continuum	Difficult to provide uninterrupted connectivity	Easy to provide uninterrupted connectivity
Response Time	High	High to Moderate
Device Coupling	Tightly Coupled	Loosely Coupled
Connectivity	Distributed	Fully distributed
Deployment	Centralized	Distributed

3. THEORETICAL BACKGROUND

This section introduces various theoretical concepts needed to understand how does BC technology work?

The security model, which includes confidentiality, Integrity, and availability are considered as an important principles to ensure any form of security [27][29]. Moreover, another terms like Accountability, Authorization, and Authentication are needed for enforcing policy and controlling access.

- Confidentiality: Confidentiality means the ability to hide data from unauthorized users. The common method of guaranteeing confidentiality in private BC is cryptography and encryption methods.
- Integrity: It takes care of the consistency and accuracy of data during its entire life-cycle. Hashing and digital signature techniques are used to ensure data integrity in private BC.
- Availability: It ensures that data is available to the users at a required range of performance in any situations. The common way of guaranteeing availability in public BC is by allowing any participant in the network to read, write and audit and maintain the blocks. In private BC only the preselected nodes can read or write.
- Authentication: It deals with personal identification in order to validate requests. Only the participants or preselected nodes who have the private keys can perform transactions [30] [31].
- Authentication: It ensures that the user includes the permission to perform a certain action.
- Accountability: It offers administrators, the ability to track the activities that users performed at a certain situation.
- Non-repudiation: It guarantees that a sender cannot deny an action in a system. In BC the non-repudiation can be achieved via the use of digital signature and timestamp.

The privacy can be maintained in public BC by using one-time accounts, similar to zerocash (Zcash) which is a protocol that provides a decentralized crypto-currency, in order to store funds and generate a new private key for every new account. [32] [33] [34][35][36].

3.1. Digital Signature (Signing Process)

Each time a transaction is made by any participant or node in the network, it is broadcasted to the all nodes in the network after performing a so-called signing process which includes two steps: hashing and encryption to produce a digital signature. The digital signature is created as follows:

- The hash value/digital digest is created by hashing the message/transaction using any hash function such as ShA-256.
- The resulted hash value is encrypted by the sender's private key which results digital signature.
- The digital signature and the message/transaction are broadcasted to the entire network.

3.2. Digital Signature (Validation Process)

This section explains the process of validation Blockchain transactions. A Blockchain validator/miner is responsible for verifying transaction within a Blockchain. After taking a set of transactions, the miners can start the validation process by applying the following steps to ensure they are legal (not malicious and double spends) as follows:

- The miners decrypt the digital signature using sender's public key which results a decrypted hash value.
- The miners apply the same hash function on the received message which results a new hash value.
- If the new hash value matches the decrypted hash value, then the message/transaction has not been altered and the Integrity, authentication and non-repudiation are achieved.
- Each miner puts validated transactions into a block.
- The validation process is finished.

3.3. Blockchain Consensus

Miners can building their blocks by applying the consensus such as Proof of work [14][18][20], and they compete each other to solve a cryptographic puzzle. The miner generates a nonce value (random value) and add it to the transaction and preform the hash function of this data to generate a new hash value. The new hash value is compared with a target value (predefined value) to check the validity of the transaction. If the new hash value is less than target value, then the miner validates the transaction and broadcasts a solution to the other miners to validate it, else the miner increments nonce value and try again. The other miners validate solution by hashing it and generate another hash which should be less than target value, if it is less, then the solution is accepted and the consensus reach by approving it from all the miners in the network, otherwise it is not accepted and the transaction is rejected. The miner has 10 minutes to solve the puzzle otherwise the transaction is rejected.

4. BLOCKCHAIN TECHNOLOGY

A Blockchain can be defined as a distributed and shared ledger that maintains a continuously growing list of blocks, which are linked and secured using cryptography [19][37][38][39]. Before exploring the operation of BC, it is important to know something about BC elements. A Blockchain comprises two transactions, which are the actions created by any participant in the system. The recorded transaction might be payment history, e.g. Bitcoin [37], or a contract or even personal data [21], and blocks that used to record the transactions. Based on the data management, the Blockchain can be categorized into public, private, and consortium BC [40]. Table 4 shows the differences between the three classes of BC.

Table 4: The differences between Public, Private and Consortium BC

	Public BC	**Private BC**	**Consortium BC**
BC Visibility	Completely open.	Closed or open to a certain number of nodes.	Open to a certain number of nodes (preselected nodes)
Who is allowed to participate in the network?	Anyone can join the network.	The participant needs a permission to join the network.	The participant needs a permission to join the network.
Who is allowed to read, write and audit.	Any participant in the network.	Preselected nodes.	Preselected participants
Who would be the miners of a BC?	Any participant can be a miner.	Preselected node or nodes.	Preselected nodes.
Speed	Slower	Faster	Faster
Power Consumption	Large energy consumption	Low energy consumption	Low energy consumption
Privacy	No privacy	High level of privacy	High level of privacy
Computational overhead	High	Low-Moderate.	Moderate
Decentralized	Fully decentralized	Centralized–some form of decentralization.	Centralized–some form of decentralization
Risk of Forking	Forks occur regularly.	Risk of forking is reduced by using a consensus mechanism.	Risk of forking is reduced by using consensus mechanism.
Double Spending	Prohibited	Not applicable	Not applicable
Finality	Not supported	Supported	Supported
Scalability	A high concern	A low to medium concern	A low to medium concern

In spite of both IoT and BC are two different technologies, the BC technology can be one of the attracting solutions to deal with the security and privacy challenges in IoT, because their properties are complementary as shown in Table 5. Such complementarity is the main reason why many researchers sand academics have proposed many research papers that suggest the idea of integration of Blockchain and Internet of thing [46] in order to deal with the shortcomings of the classical security and privacy mechanisms. Most of IoT security and privacy frameworks are centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, traffic, and single point of failure [47]. In addition to that, chances of device spoofing, false authentication, less reliability in data sharing could happen.

Most of IoT security and privacy frameworks are centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, traffic, and single point of failure [47][48][49]. Consequently, a Blockchain can be one of the remedy for addressing the security and privacy issues by providing a distributed and immutable system of record for sharing data across a network, hashing, encryption and decryption for verification and authentication, and consensus and agreement algorithms such as Proof of Work (POW) [50] or Proof of Stake (POS) [51] for detecting bad users and mitigating threats.

Table 5. Complementary Features of IoT and Blockchain

	Blockchain	**IoT**
Resource	Resource consuming	Mostly devices are resource restricted.
Time Consuming	Block mining is time consuming.	Demands low latency.
Scalability	Blockchain scale poorly with large networks.	IoT is expected to contain a large number of nodes.
Bandwidth	High bandwidth consumption.	Limited bandwidth.
Big data	Source	Means to manage

5. CONCLUSION

An IoT ecosystem has several challenging regarding security and privacy issues. This is because the IoT integrates different technologies, hardware, and software. Therefore, many researchers and academics have suggested the integration of IoT with blockchain technology to address security, and privacy challenges. This survey dealt the role of cloud and fog computing to overcome the IoT devices shortcomings regarding security and other challenges. With the security and privacy challenges in IoT. Blockchain technology is explored as one of the solutions for addressing different issues and challenges in IoT. This paper can serve as a primer for researchers to understand the concepts of IoT and the importance of integration of blockchain with IoT for addressing the security and other IoT challenges. Because in our opinion, the blockchain technology can fill IoT security gaps when it integrates with BC technology.

6. REFERENCES

[1] B. Omoniwa, R. Hussain, M.A. Javed, S. H. Bouk, and S. A. Malik, "Fog/Edge Computing-based IoT(FECIoT): Architecture, applications, and Research issues," IEEE Internet of Things Journal, Vol. x, No. x, Oct. 2018.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[3] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT)- When social networks meet the Internet of Things: Concept, architecture and network characterization," Computer Networks, vol. 56, no. 16, pp. 3594-3608, Nov. 2012.

[4] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 10th IEEE International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 336-341.

[5] N. Reijers, K. J. Lin, Y. C. Wang, C. S. Shih, and J. Y. Hsu, "Design of an intelligent middleware for flexible sensor configuration in M2M systems", Proc. Second Int. Conf. on Sensor Networks (SENSORNETS), February 2013, pp. 1-6.

[6] M. A. Razzaque, M. Milojevic-Jevric, A. Palade and S. Clarke, "Middleware for Internet of Things: A Survey," IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, Feb. 2016.

[7] Amathul Hadi Shakara, Md. Traeqhasan, "Solutions of common challenges in IoT", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 19, no. 5, Ver. V, pp. 57-65, 2017.

[8] Feng Wang, Liang Hu, Jin Zhou, and Kuo Zhao, "A Data Processing Middleware Based on SOA for the Internet of Things", Journal of Sensors, January, 2015.

[9] A. Botta, W. Donato, V. Persico, and A. Pescape, "Integration of Cloud Computing and Internet of Things: A Survey", Future generation Computer Systems, September 2015.

[10] Zhang, Q., Cheng, L., Boutaba, R., "Cloud computing: state-of-the-art and research challenges", Journal of internet services and applications 1 (1), 7–18, 2010.

[11] Mell, P., Grance, T., "The NIST definition of cloud computing", National Institute of Standards and Technology 53 (6), 50, 2009.

[12] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439-449, Feb. 2018.

[13] Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are. White Paper. 2016. Available online: http://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-overview. pdf (accessed on 8 April 2018).

[14] Liu, Y.; Fieldsend, J.E.; Min, G.A Framework of Fog Computing: Architecture, Challenges and Optimization. IEEE Access 2017, 4, 1–10. [CrossRef].

[15] Peralta, G.; Iglesias-Urkia, M.; Barcelo, M.; Gomez, R.;

Moran, A.; Bilbao, J. Fog computing based efficient IoT scheme for the Industry 4.0. In Proceedings of the 2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their application to Mechatronics, San Sebastian, Spain, 24–26 May 2017; pp. 1–6.

[16] Bonomi, F.; Milito, R.; Natarajan, P.; Zhu, J. Fog Computing: A Platform for Internet of Things and Analytics. In Big Data and Internet of Things: A Roadmap for Smart Environments; Studies in Computational Intelligence; Springer: Cham, Switzerland, 2014; Volume 546, pp. 169–186.

[17] Rukhsana T., Ysera F. K., and Shafqat M., "Fog Approach in Internet of Things: a Reviews", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 4 | Issue 1.

[18] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, "in Security and Privacy(SP),2016IEEESymposium on. IEEE, 2016, pp. 839–858.

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[20] M. Vukoli´c, "The quest for scalable blockchain fabric: Proof-of work vs. bit replication," in International Workshop on Open Problems in Network Security. Springer, 2015, pp. 112–125.

[21] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, p. 218, 2016.

[22] McKinsey_FACI_Blockchain_in_Insurance.pdf [27] L. Bahack, "Theoretical Bitcoin attacks with less than half of the computational power," Dec. 2013, arXiv:1312.7013v1. [Online]. Available: https://arxiv.org/pdf/1312.7013.pdf.

[23] Ai, Y.; Peng, M.; Zhang, K. Edge cloud computing technologies for internet of things: A primer. Digit. Commun. Netw. 2017, in press. [CrossRef].

[24] Hany F. A, Robert J. W., and Gary B. W., Fog Computing and the Internet of things: A Review. Big Data Cogn. Comput. 2018, 2, 10.

[25] Wen, Z.; Yang, R.; Garraghan, P.; Lin, T.; Xu, J.; Rovatsos, M. Fog orchestration for internet of things services. IEEE Internet Comput. 2017, 21, 16–24. [CrossRef].

[26] Rashid D., Ravindran D., A comprehensive study on cloud computing paradigm. International journal of advanced research in science and engineering. 2018, Vol. 7,4.

[27] Yashpalsinha J., Kirit M. Cloud Computing-Concepts, Architecture and Challenges. 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].

[28] Azhra G., A literature review on cloud computing security issues. International Journal of Information, Security and systems management, 2017, Vol. 6, No.1, pp. 637-640.

[29] Mais Haj Qasem, Mohammad Qatawneh. Parallel Hill Cipher Encryption Algorithm. International Journal of Computer Applications. Vol. 179, No.19, pp. 16-26, 2018.

[30] Sanad AbuRass, Mohammad Qatawneh. Performance Evaluation of AES algorithm on Supercomputer IMAN1. International Journal of Computer Applications. Vol. 179, No. 48, 2018.

[31] Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, and Antônio A. de A. Rocha. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Security and Communication Networks Volume 2018.

[32] Maha Saadeh, et al., "Authentication Techniques for the Internet of Things: A Survey", in Cybersecurity and Cyberforensics Conference (CCC), 2016, IEEE, 2016, pp. 28– 34.

[33] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, pp. 557-564.

[34] Ouaddah, A.; Elkalam, A.A.; Ouahman, A.A. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In Europe and MENA Cooperation Advances in Information and Communication Technologies; lvaro Rocha, Á., Serrhini, M., Felgueiras, C., Eds.; Springer: Cham, Germany, 2016; pp. 523–533

[35] Ola M Surakhi, Mohammad Qatawneh, A Hussein. A Parallel Genetic Algorithm for Maximum Flow Problem. International Journal of Advanced Computer Science and applications, 2017.

[36] Munsing, E.; Mather, J.; Moura, S. Blockchains for decentralized optimization of energy resources in microgrid networks. In Proceedings of the IEEE Conference on Control Technology and Applications (CCTA 2017), Kohala Coast, HI, USA, 27–30 August 2017; pp. 2164–2171

[37] Shafagh, H.; Hithnawi, A.; Duquennoy, S. Towards blockchain-based auditable storage and sharing of IoT data. In Proceedings of the 9th ACM Cloud Computing Security Workshop (CCSW 2017), Dallas, TX, USA, 3 November 2017; pp. 45–50

[38] Bahga, A.; Madisetti, V.K. Blockchain platform for industrial internet of things. J. Softw. Eng. Appl. 2016, 9, 533–546

[39] Lombardi, F.; Aniello, L.; De Angelis, S.; Margheri, A.; Sassone, V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids. In Proceedings of the Living in the Internet of Things 2018: Cybersecurity of the IoT-A PETRAS, IoTUK & IET Event, London, UK, 28–29 March 2018.

[40] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proceedings of the 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2016, IEEE, Agadir, Morocco, December 2016.

[41] T. M. Fernández-Caramés and P. Fraga-Lamas, "A

review on the use of blockchain for the internet of things," IEEE Access, pp. 1–23, May 2018.

[42] Mohammad Qatawneh; Wesam Almobaideen; Mohammed Alkhanafseh. DFIM: A New Digital Forensics Investigation Model for Internet of Things. Journal of Theoretical and Applied Information Technology. 2019, Vol.97. No.24.

[43] Mohammed Khanafseh, Mohammad Qatawneh, Wesam Almobaideen. A Survey of Various Frameworks and Solutions in all Branches of Digital Forensics with a Focus on Cloud Forensics. (IJACSA) International Journal of Advanced Computer Science and Applications, 2019.

[44] Guan, Z.; Si, G.; Zhang, X.; Wu, L.; Guizani, N.; Du, X.; Ma, Y. Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. arXiv 2018, arXiv:1806.01056.

[45] O. Abualghanam, M. Qatawneh andW. Almobaideen, "A Survey of Key Distribution in the Context of Internet of Things," Journal of Theoretical and Applied Information Technology, vol. 97, no. 22, pp. 3217–3241, 2019.

[46] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Čapkun, "On the security and performance of Proof of Work blockchains," in Proceedings of the 23rd ACM Conference on Computer and Communications Security, CCS 2016, pp. 3–16, Austria, October 2016.

[47] Maha Saadeh, Huda Saadeh, Mohammad Qatawneh. Performance Evaluation of Parallel Sorting Algorithms on IMAN1 Supercomputer. International Journal of Advanced Science and Technology, 2016

[48] Almobaideen, W., Krayshan, R., Allan, M., and Saadeh, M. (2017). Internet of Things: Geographical Routing based on healthcare centers vicinity for mobile smart tourism destination. Technological Forecasting and Social Change, 123, 342–350. https://doi.org/10.1016/j.techfore.2017.04.016.

[49] Wesam Almobaideen, Mohammad Qatawneh, Orieb Abualghanam. Virtual Node Schedule for Supporting QoS in Wireless Sensor Network. 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)

[50] Saadeh, M., Sleit, A., Qatawneh, M., and Almobaideen, W. (2016). Authentication techniques for the internet of things: A survey. In Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016. https://doi.org/10.1109/CCC.2016.22.

[51] Reem Saadeh, Mohammad Qatawneh. PERFORMANCE EVALUATION OF PARALLEL BUBBLE SORT ALGORITHM ON SUPERCOMPUTER IMAN1. International Journal of Computer Science & Information Technology (IJCSIT). 2019.

[52] Ahmad Bany Doumi, Mohammad Qatawneh (2019). Performance Evaluation of Parallel International Data Encryption Algorithm On IMAN1 Super Computer. International Journal of Network & Its Applications (IJNSA), 11(1).

[53] Asassfeh Mahmoud Rajallah, Mohammad Qatawneh, Feras Mohamed AL-Azzeh (2018). Performance Evaluation of Blowfish Algorithm on supercomputer IMAN1. International Journal of Computer Networks & Communications (IJCNC) 10(2).

[54] Amaal Shorman, Mohammad Qatawneh (2018). Performance Improvement of Double Data Encryption Standard Algorithm using Parallel Computation. International Journal of Computer Applications, 179(25).