ISSN NO: 2770-4491
Date of Publication:07-03-2022

Securing the Internet of Things

Safa Abood Nama.[1]
Assist. Prof. Kwther Abbood Neamah.[2]
Al Iraqia University.[1]
Baghdad College Of Ecunomics Sciences University Iraq.[2]

Abstract: There has been a surge in academic interest in the Internet of Things (IoT) in the last couple of years. There will be billions of "intelligent communications" "things" in the Internet of Things (IoT). The Internet of the future will be made up of a variety of devices that will connect to each other and extend the boundaries of the world. The Internet of Things (IoT) expands the functionality of devices that are already connected. Definition, architecture, key technologies and applications of the Internet of Things are all covered in depth in this study. There will be numerous definitions of IoT in the reports, to start with. After then, new means of implementing IoT will be explored. As a last step, several unsolved issues in IoT applications will be reviewed. Finally, the research community's most pressing challenges and possible solutions are discussed in this section.

Keywords: Internet of Things (IoT), Security Threats, and Challenges.

I. Introduction

The Internet of Things (IoT) is showing its promise by connecting an ever-increasing number of physical items [1]. Information may be exchanged and exchanged via the connectivity of numerous goods and networks, including sensors, brilliant meters, advanced cells; intelligent cars; radio-frequency identification labels; PDAs; and other things (including with gizmos, programming and actuators) [2].

The linking of several devices enables advanced IoT applications like item tracking and weather forecasting. This technology may also be used to undertake patient reconnaissance and energy management for CEOs [3]. Ready house is an IoT application that allows customers to open their garage, relax, order a coffee, and control lights, TV, and other gadgets automatically. Smart cities, light networks, healthcare, transportation, mechanical robotization, and disaster response all depend on IoT. (IoT). New types of human-machine cooperation will be available in the future. Applications, frameworks, and administrations get more flexibility, and our lives are enhanced. When IoT takes off, it will allow massive computational power, storage space, and connection rates. Cisco predicts a rise in connected devices from 50 billion in 2020 to 500 billion in 2025 [4]. Until 2019, people, machines, and "things" will create 500 zettabytes. Globally, 10.4 zettabytes of IP traffic would be created [5]. By then, IoT data would make up about half of all data held by a company [6]. Speed is vital in certain IoT applications. In certain circumstances, sensitive data must be kept locally. A few users' massive data transfers may adversely disrupt networks [7]. With the emergence of IoT-connected devices (such smart glasses or PDAs), fine-grained information, including media data, may be exchanged between devices (e.g., photographs, recordings, and voices) [8, 9]. A large amount of data causes organizational congestion and difficult handling demands on devices and control frameworks. We can bring services closer to end-users by pooling registration, storage, and systems management resources at the organization's edge. In this decentralized registration architecture, an IoT or client-side device is needed to transmit, administrate, and store data. Connections between mist hub and devices may reduce preparation challenges for asset-required devices and help meet transfer speed criteria for grouped administrations in mist registration [10]. On-demand administrations and programs for various gadgets, thick topographic suited and common inertness responses employing mist computing deliver a unique client experience and increase recurring business [11]. Concerns concerning security and safety are unavoidable as distributed computing evolves [12, 13]. Mist computation is provided by many haze specialists, making devices hackable. The rise of IoT devices has heightened security risks for Haze hubs [14]. IoT devices may be hacked, damaged, or stolen. Existing distributed computing arrangements might be adjusted to address numerous security and protection issues in haze modeling because to their decentralized foundation, adaptability assistance, area awareness, and minimum idleness. However, dispersed computing is less secure

ISSN NO: 2770-4491
Date of Publication:07-03-2022

than hazy processing because to local data storage and occasional data transfers with cloud foci. Mist hubs may operate as end-gadget intermediates in the absence of essential assets' gadgets [15]. Insufficient research has been done on security, protection, and mist registration security assets. So, before designing and deploying mist-assisted IoT applications, security and protection goals of moisture registering must be addressed. The study of IoT hazy registration security and protection is new. The benefits of mist for IoT applications, security problems, and cutting-edge configurations were discussed. Then comes the design and characteristics of mist processing. Clearly exhibited. Consistent administrations, transitory stockpiling, information dispersion, and decentralized calculation will be offered as security and protection threats and obstacles in mist registration. It is also feasible to investigate future methods of recognizing security and protection concerns and analyze the existing. We illustrate our awareness of the accomplishments and problems of haze figuring in IoT applications. The report's structure is shown below. A brief introduction to theory is given in Section 1, and research is discussed in Section 2. Three primary threats to security. Problems with IoT (IoT). Finally, in Section 5, we review our results and propose research suggestions.

II. Other Works

IoT or network of trainings refers to the systematic connectivity of common objects, many of which are endowed with ubiquitous knowledge [16]. A few noteworthy repercussions arise from such a plethora of developments; without a question, the IoT enhances the ubiquity of the network via inserted frameworks by integrating things with assistance capability [17]. The Internet of Things (IoT) is driving smart business[18], 'keen wellness'[19], and smart cities [20, 21].Organizations' supply and demand sides have been impacted [21]. Business measurement frameworks [22], and action plans (BM) [23] have been significantly improved [24]. The emergence of IoT technology has had a tremendous impact on company models. A detailed descriptive writing survey found no substantial influence on BMs (SLR) [25]. In order to identify, analyze and assess significant study pieces, and to generate aggregate experiences of knowledge from prior research, the flow focuses on writings on the influence of IoT on corporate BMs [26]. Word and substance research may be merged to get excellent results and prepare for the next test (RQs) the "Internet of Things" refers to the networked coordination of everyday things, many of which are intelligent. Although the word "IoT" is already widely used, no formal definition exists [27]. The phrase "web for things" appeared in a 1999 debate on structured radio-recurrence distinguishing proof architecture by the MIT Auto-ID Labs [28]. Interconnecting (physical and virtual) things based on current and upcoming interoperable data and communications improvements is what the ITU calls the Information Society's cornerstone. So many breakthroughs have a few (notable) negative effects. The Internet of Things (IoT) connects smart objects to embedded frameworks, extending the web's reach. As a result, the Internet of Things has created a vast network of gadgets that interact with people. The Internet of Things (IoT) is changing how businesses, governments, and leaders create wealth [29]. IDC predicts a $7.1 trillion market for IoT after 2020. (International Data Corporation). Smart cities and smart transportation systems are being driven by the Internet of Things. Both supply and demand are impacted. It has also shown considerable benefits to business measurement frameworks and BM structure squares. Model structure squares [30] and business measurements have both altered dramatically throughout the period that many firms have tried to implement IoT-driven changes [31]. It is organized into four categories: infrastructure [32], hierarchy, individual, and comprehensive. Every category affects a subset of support areas. Organizations have been influenced by non-incentives. During the time spent experimenting with IoT-driven changes, the SLR research team efficiently works with current publications [33]. To keep the cycle going, a defined interface for examining the writing must be included. As demonstrated in [34], academics have suggested several interaction models. These models all have several phases and stages. Using edge registration, organizations may move administrations, stockpiling, and processing assets from central personnel to the organization's edge. This reduces correspondence overhead between focal points and organizational edges by finishing information inspection or disclosure near information.

ISSN NO: 2770-4491
Date of Publication:07-03-2022

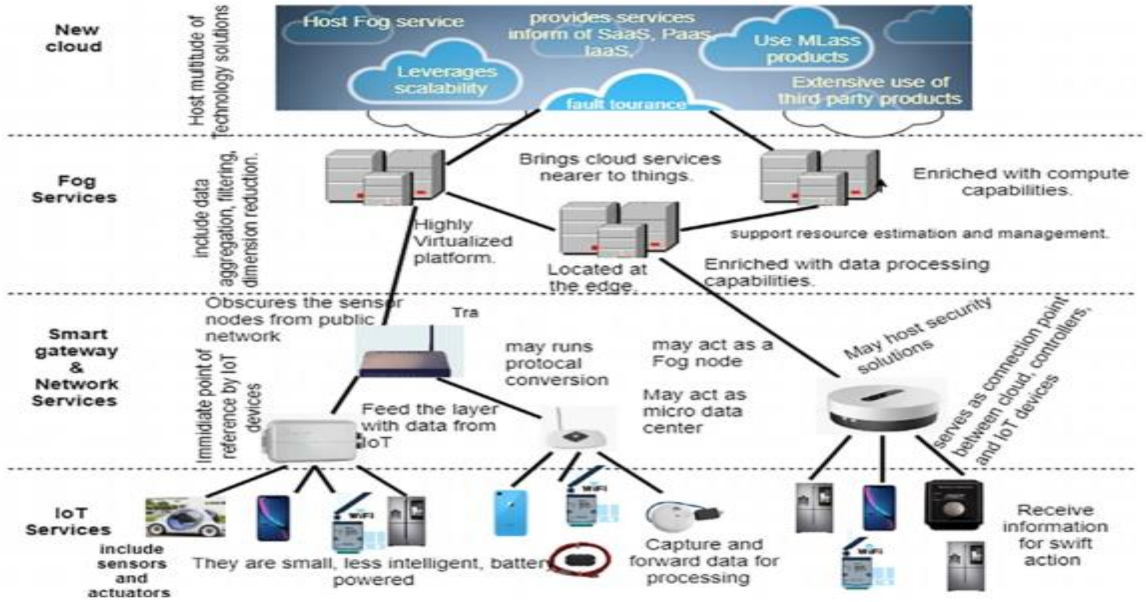
New cloud
Host multitude of Technology solutions
Host Fog service
provides services inform of SaaS, Paas, IaaS.
Use MLass products
Leverages scalability
fault tourance
Extensive use of third party products
Fog Services
include data aggregation, filtering, dimension reduction.
Brings cloud services nearer to things.
Enriched with compute capabilities.
Highly Virtualized platform.
Located at the edge.
support resource estimation and management.
Enriched with data processing capabilities.
Smart gateway & Network Services
Immidiate point of reference by IoT devices
Obscures the sensor nodes from public network
Tra
may runs protocol conversion
may act as a Fog node
May act as micro data center
May host security solutions
serves as connection point between cloud, controllers, and IoT devices
Feed the layer with data from IoT
IoT Services
include sensors and actuators
They are small, less intelligent, battery powered
Capture and forward data for processing
Receive information for swift action

Fig.1: Data acquired from various apps.

In the past, power lattice data information has been exchanged and communicated using explicitly specified organizational ways. Each application worker has its own assistance cycles and memory information bases, all thanks to the force lattice PC network structure. A normal Oracle data set is delivered exclusively to the server farm and the data set worker. There is a huge quantity of information exchanged and kept at the stockpile center. The data set becomes an entry bottleneck due to the amount of information that has been acquired exceeding the capacity of the data set. Organizational resources are depleted as a result of workers exchanging enormous amounts of information. To use the typical integrated cloud stage design, all data must be processed at the central hub and then transmitted and distributed, which is absurd, time-consuming and wasteful.

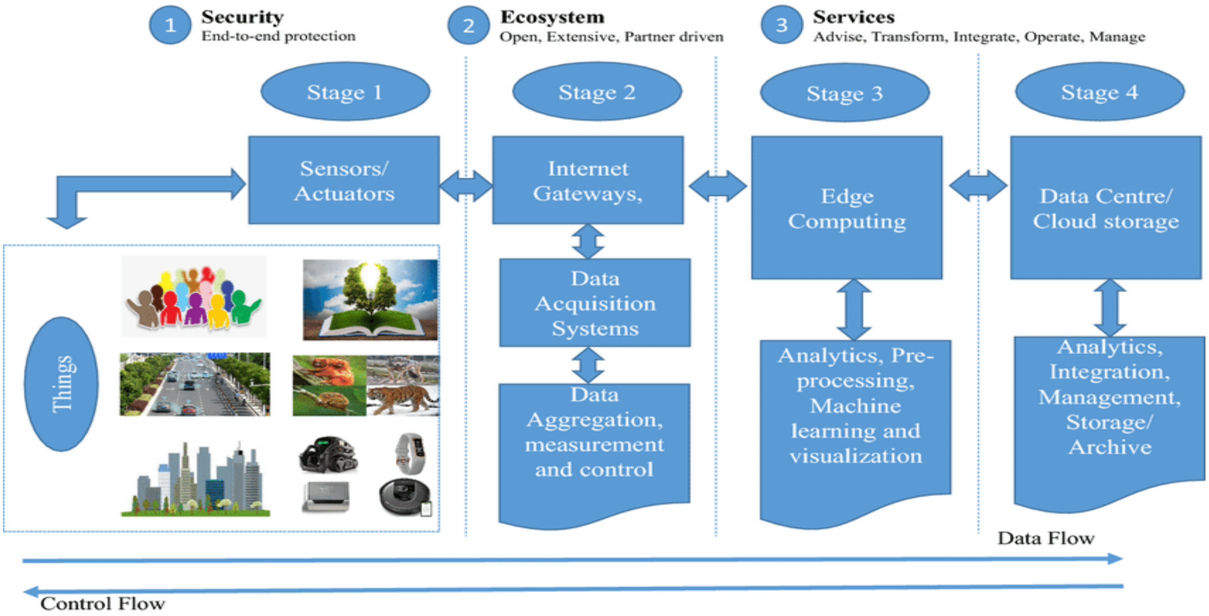
1 Security
End-to-end protection
2 Ecosystem
Open, Extensive, Partner driven
3 Services
Advise, Transform, Integrate, Operate, Manage
Stage 1
Stage 2
Stage 3
Stage 4
Sensors/ Actuators
Internet Gateways,
Edge Computing
Data Centre/ Cloud storage
Things
Data Acquisition Systems
Data Aggregation, measurement and control
Analytics, Pre-processing, Machine learning and visualization
Analytics, Integration, Management, Storage/ Archive
Data Flow
Control Flow

Fig. 2: Depicts the current state of data center architecture [34].

By establishing an information and administration standard framework for the whole energy chain, the board hopes to extend the current information model and bring corporate belief along with the administration of all information. This framework must encompass the entire energy chain. Through the request and examination of around 90 critical business list information in six business areas (mechanical HR board; monetary administration; speculation project the executives; creation the board; advertising the executives and global business), it is acknowledged that information is integrated and that powerful sharing and opening of information is being framed. Organizational objectives were central to a record architecture that supported

ISSN NO: 2770-4491
Date of Publication:07-03-2022

the organization's immediate industrial activity checking and standardized the information leaders needed to make decisions.

III. Internet Things' Security Threats

The structure of distributed computing makes it susceptible to outside threats. Google, Amazon, and Yahoo have steadily started leaking enormous amounts of data. Cloud security fears have hindered the spread of distributed computing. Haze registration is more secure than distributed computing for the following reasons: In order to reduce the requirement for Internet connections, data gathered is promptly updated and broken down to the closest local mist hub. Because of local data storage, trading, and analysis, programmers cannot access client data. Data transfer between devices and the cloud is no longer consistent, making data monitoring more challenging for busybodies. Regardless, dispersed computing's intrinsic security flaws make mist computing insecure. It's a simple yet fascinating design feature. Vendors of mist and cloud give them to customers in order to supply them with distinctive services. They cannot deviate from the set criteria for financial reasons. The content of stored data and data on data owners may still be spied on. As a result, mist or cloud specialized co-ops may have access to customer data, posing a security risk. Programmers that employ every trick in the book to obtain what they want are likely to concentrate on mist hubs or cloud workers. So mist hubs and cloud workers may be simple, yet inquisitive, and even adversarial. An opponent may attempt to impede mist processing by:

Table 1: Attacks aimed at interfering with fog computing.

Threat categories	Descriptions
Forgery:	They may create their own personalities and profiles as well as phony data in order to deceive people into believing that they are dealing with real narcotics. False information would also waste the organization's transmission, storage, and energy resources.
Tampering	Disruption of mist processing may be caused by changing attackers discarding, postponing, or manipulating information sent to them.
spam	There are several types of spam information that include unwanted stuff like unnecessary data and information that is generated and distributed by enemies. There would be a waste of resources, a skewed social circle, and even security vulnerabilities as a consequence of spam.
Collusion	In order to make a little money, at least two organizations arrange to deceive, swindle, or entice other legal substances. Several parties, such as a few mist hubs, IoT devices, IoT devices in the cloud, or mist hubs with IoT devices, may intend to increase their attack capability in mist recording.
Man-in-the-Middle:	Two groups of people are approached by an evildoer who stays or stands between them in order to secretly transfer or alter trade information between the groups. It's clear that these two parties have made it clear that they're talking to each other.
Impersonation:	Malicious hackers pose as legitimate customers of mist hub services or mimic genuine mist hub administrators so they may scam consumers into paying for fake or phishing services.
Eavesdropping:	Criminals monitor communication lines to intercept and read packages being sent back and forth. This kind of organizational assault is more convincing if the data is encrypted.
Denial-of-Service:	By bombarding mist hub administrators with useless requests, an attacker prevents its intended customers from accessing the services supplied by mist hubs.

IV. Future Research Challenges

The usage of blockchain in IoT systems and frameworks raises privacy issues. Researchers are aiming to incorporate blockchain technology into IoT devices. A few challenges, lingering issues, and probable research pathways linked to confidentiality while using blockchain technology with various IoT applications are discussed below.

A. IoT in Industry

The openness and transparency of blockchain technology is growing its adoption in industrial IoT systems. IIoT detectors may be more effective in a decentralized industrial facility [35, 36]. This is because data may be delivered to any IIoT blockchain node by updating the shared ledger. Several studies have been undertaken to solve IIoT privacy challenges including as confidentiality and differential privacy. These ideas will need to be significantly modified to work on the blockchain. Thus, researchers should concentrate on maintaining the privacy of blockchain-based IIoT systems [35, 36].

B. IoT in Agriculture

An IoT supply chain model uses real-time monitoring of agricultural production, manufacturing, transportation, storage, and distribution. This traceability scheme would improve agriculture sector protection, supervision, growing, and processing procedures. Using blockchain in agriculture and IoT systems increases monitoring and tracking. One example is the location and function of any agricultural product [37]. This holds great potential for blockchain-based IoT agriculture. Secret codes may be used to avoid data leakage during dissemination. Smart contracts and privacy protection techniques should be the focus of future research [38].

C. New Urbanism

Researchers are using blockchain with emerging smart city technology to improve smart city ideas. Blockchain's decentralized nature may remove many smart city safety issues, say academics. Blockchain's decentralized structure may be a negative for privacy-conscious users. A hacker might get access to a smart city's shared blockchain and attempt to collect or infer personal information about its people, causing major privacy issues. Privacy and security cannot be restricted in blockchain-based smart cities. Anonymization, smart contracts, and differential privacy may be used to assure data transmission across processes in numerous smart city applications. Simple privacy protection in smart cities offers privacy differentiation. It protects privacy while offering consumers control over their data [39, 40].

D. Mobile Crowd Sensing

To take use of the growing number of smart devices and the benefits of IoT technology for large-scale sensing, "mobile crowdsensing" was developed. Thus, MCS applications are vulnerable to hacking. Because data is delivered in real time, the crowd detector must be clear. To preserve privacy and security, any blockchain-based crowdsensing system must ensure that no MCS users' personal information is released. Anonymization may help protect MCS sufferers' privacy. Even if an adversary obtains sensitive data, the original identities are safeguarded. A differential privacy security solution might also be used to decrease noise in MCS users' data. When users input data in real-time, maintaining the trade-off between accuracy and privacy may be difficult.

V. The Permanent Challenge of The Internet of Things

Also covered in this part are the security issues associated with hazy registration and the current solutions that may be utilized to address them.

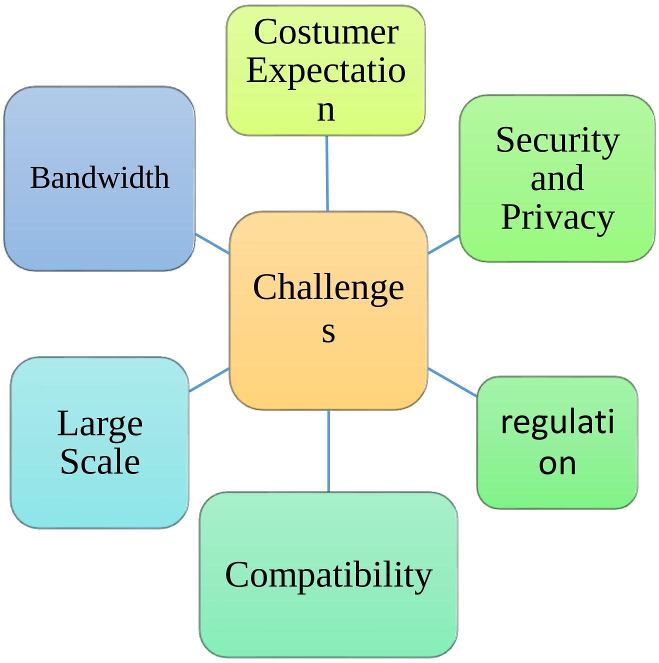

Fig. 3: Challenges and Security of Internet Things

Another aspect of mechanical advances is the assessment of the degree of innovation by government authorities. The public sector is frequently compelled to make up for lost time due to the rapid evolution of the Internet of Things (IoT). Decisions must be made.

It's no secret that the Internet of Things (IoT) market is flooded with competitors eager to get their hands on a slice of the pie. This is a great thing since it encourages buyers to make better choices. However, it may lead to misunderstanding. Another cause of annoyance will be the home cross-section networks. For a long time, Bluetooth was the de facto Internet of Things (IoT) standard. Harald Bluetooth, a historical ruler who brought together warring tribes, was the inspiration for the name. Zigbee and Z-Wave have emerged to compete with Bluetooth's network contributions in home automation. The market may take a long time to settle on a single standard for home IoT. It may be difficult to maintain IoT devices the same if consumers don't keep them serviced and updated. Different IoT device programming languages might lead to execution and security concerns. Keeping your IoT devices up-to-date and maintained is essential because of this.

The IoT test of network bandwidth is more important than you would think. IoT video real-time streaming apps may compete for space on the current worker-customer paradigm as the IoT sector grows, some observers believe. An IoT traffic monitor and organizer are deployed as a consequence of the worker customer model. These companies, on the other hand, often have difficulty keeping up as the number of connected devices grows. Therefore, IoT firms need to carefully choose service providers with a demonstrated track record of administration and growth. You may design a more robust and easy-to-understand IoT product by using cross-MNO functionalities.

It is better to under-promise and over-deliver than to promise more than you can deliver. It's no secret that many Internets of Things (IoT) manufacturers have tackled this problem in the most difficult manner conceivable, with new IoT businesses appearing daily and confusing customers. Client disappointments, delays, and income losses may occur when expectations and reality don't match.

The fierce competition in the IoT industry means that customers who aren't happy will not hesitate to leave. Those who want to join this highly competitive and innovative business should be prepared for a market that never sleeps and customers who always demand clarifications. People's lives, work, and leisure might be transformed by technology. For the Internet of Things (IoT) to work properly, all parties involved in the IoT must agree on safety and execution problems.

Conclusion

This article describes a decentralized architecture that moves asset collection, registration, and coordination to the periphery of the organization. Consequently, users face extra security and protection issues. An IoT application haze processing was examined in this study. Engineering and pollution followed. Mist hub components have also been studied for some interesting IoT applications in this regard. The processing of mist has uncovered a variety of security issues and exposes concerns around security. Following that, there was a debate on the remaining obstacles to future research into security and protection issues in IoT applications. Mist processing's open examination issues have been identified as a result of addressing security and protection concerns.

References

1. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," 2015.
2. A. Saif *et al.*, "Internet of Fly Things For Post-Disaster Recovery Based on Multi-environment," 2021.
3. D. J. O. a. g. g. c. Evans, "The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Cisco IBSG," 2011.
4. F. Köylü *et al.*, "Review of internet of things of security threats and Challenges," 2021.
5. M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT)," in *2015 Internet Technologies and Applications (ITA)*, 2015, pp. 219-224: IEEE.
6. C. MacGillivray *et al.*, "IDC future scape: Worldwide internet of things 2017 predictions," in *IDC Web Conference*, 2016.
7. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. J. I. i. o. t. j. Xu, "Edge computing: Vision and challenges," vol. 3, no. 5, pp. 637-646, 2016.
8. H.-S. J. I. J. o. C. Kim, "Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are," 2016.
9. L. M. Vaquero and L. J. A. S. c. c. R. Rodero-Merino, "Finding your way in the fog: Towards a comprehensive definition of fog computing," vol. 44, no. 5, pp. 27-32, 2014.
10. T. J. C. B. Zhang, "Fog boosts capabilities to add more things securely to the internet," 2016.
11. Q. Abdullah *et al.*, "Real-time Autonomous Robot for Object Tracking using Vision System," 2021.
12. R. Roman, J. Lopez, and M. J. F. G. C. S. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," vol. 78, pp. 680-698, 2018.
13. J. Granjal, E. Monteiro, J. S. J. I. C. S. Silva, and Tutorials, "Security for the internet of things: a survey of existing protocols and open research issues," vol. 17, no. 3, pp. 1294-1312, 2015.
14. A. Saif, K. Dimyati, K. A. Noordin, S. H. Alsamhi, and A. J. I. T. L. Hawbani, "Multi-UAV and
15. A. Alrawais, A. Alhothaily, C. Hu, and X. J. I. I. C. Cheng, "Fog computing for the internet of things: Security and privacy issues," vol. 21, no. 2, pp. 34-42, 2017.
16. T. Abbate, F. Cesaroni, M. C. Cinici, M. J. T. F. Villari, and S. Change, "Business models for developing smart cities. A fuzzy set qualitative comparative analysis of an IoT platform," vol. 142, pp. 183-193, 2019.
17. A. Alcayaga, M. Wiener, and E. G. J. J. o. c. p. Hansen, "Towards a framework of smart-circular systems: An integrative literature review," vol. 221, pp. 622-634, 2019.
18. A. Saif *et al.*, "Unmanned Aerial Vehicle and Optimal Relay for Extending Coverage in Post-Disaster Scenarios," 2021.
19. K. Dar, A. Taherkordi, H. Baraki, F. Eliassen, K. J. P. Geihs, and M. Computing, "A resource oriented integration architecture for the Internet of Things: A business process perspective," vol. 20, pp. 145-159, 2015.
20. K. J. R. j. Ashton, "That 'internet of things' thing," vol. 22, no. 7, pp. 97-114, 2009.
21. E. de Senzi Zancul, S. M. Takey, A. P. B. Barquet, L. H. Kuwabara, P. A. C. Miguel, and H. J. B. P. M. J. Rozenfeld, "Business process support for IoT based product-service systems (PSS)," 2016.
22. W. H. J. i. Dutton, "Putting things to work: Social and policy challenges for the Internet of things," 2014.

ISSN NO: 2770-4491
Date of Publication:07-03-2022

23. J. A. Guerrero-Ibanez, S. Zeadally, and J. J. I. W. C. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," vol. 22, no. 6, pp. 122-128, 2015.
24. A. Gilchrist, *Industry 4.0: the industrial internet of things*. Springer, 2016.
25. E. Hakanen, R. J. J. o. B. Rajala, and I. Marketing, "Material intelligence as a driver for value creation in IoT-enabled business ecosystems," 2018.
26. L. Guo, Y. S. Wei, R. Sharma, and K. J. I. J. o. P. E. Rong, "Investigating e-business models' value retention for start-ups: the moderating role of venture capital investment intensity," vol. 186, pp. 33-45, 2017.
27. G. Kortuem, F. Kawsar, V. Sundramoorthy, and D. J. I. I. C. Fitton, "Smart objects as building blocks for the internet of things," vol. 14, no. 1, pp. 44-51, 2009.
28. A. Salh *et al.*, "Trade-off Energy and Spectral Efficiency in 5G Massive MIMO System," 2021.
29. Y. Lu, S. Papagiannidis, E. J. T. F. Alamanos, and S. Change, "Internet of Things: A systematic review of the business literature from the user and organisational perspectives," vol. 136, pp. 285-297, 2018.
30. Q. Abdullah *et al.*, "Pilot Contamination Elimination for Channel Estimation with Complete Knowledge of Large-Scale Fading in Downlink Massive MIMO Systems," 2021.
31. G. G. Meyer, K. Främling, and J. J. C. i. i. Holmström, "Intelligent products: A survey," vol. 60, no. 3, pp. 137-148, 2009.
32. A. Osterwalder and Y. Pigneur, *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons, 2010.
33. M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons, 2008.
34. S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, 12/09 2019.
35. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. J. I. i. o. t. j. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," vol. 4, no. 5, pp. 1125-1142, 2017.
36. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*, 2016, pp. 1392-1393: IEEE.
37. C. Yin, S. Zhang, J. Xi, J. J. C. Wang, C. Practice, and Experience, "An improved anonymity model for big data security based on clustering algorithm," vol. 29, no. 7, p. e3902, 2017.
38. P. Barbosa, A. Brito, and H. J. I. S. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," vol. 370, pp. 355-367, 2016.
39. L. Ruiz-Garcia, L. J. C. Lunadei, and E. i. Agriculture, "The role of RFID in agriculture: Applications, limitations and challenges," vol. 79, no. 1, pp. 42-50, 2011.
40. O. Bermeo-Almeida, M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, "Blockchain in agriculture: A systematic literature review," in *International Conference on Technologies and Innovation*, 2018, pp. 44-56: Springer.