OPEN ACCESS

Saudi Journal of Engineering and Technology
Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Review Article

The Security Challenges in Cloud IoT- A Review

Hasan Mahmood*

University of Sialkot, Sialkot, Pakistan

DOI: 10.36348/sjet.2021.v06i07.003 | **Received:** 22.05.2021 | **Accepted:** 28.06.2021 | **Published:** 14.07.2021

***Corresponding author:** Hasan Mahmood

Abstract

Internet-of-Things (IoT) has made ubiquitous computing a reality through extending Internet connectivity in numerous applications deployed throughout the globe. The combination of IoT-based cloud structures included with smart systems that offer smart objectives and programs are a promising future trend. Cloud computing is tremendously efficient, storage is becoming more and more vast, and a few groups are now changing their data from in house data to Cloud Computing Vendors' hubs. As a result, a few new classes of safety and privacy problems are introduced. This paper provides security problems relating to the IoT cloud.

Keywords: IoT, security, privacy, cloud IoT, Smart city, Cloud computing.

INTRODUCTION

Over the years, with the fast development of distributed computing, parallel computing, grid computing, network storage, and virtual system technique, computing resources have become greater abundant, cheaper, and more accessible than ever before. The improvement of the Information Technology (IT) industry and the influx of digital devices into the marketplace has increased the demand for computing and storage resources. In this context, a brand new computing model known as cloud computing was proposed. In this mode, resources (including networks, computing, storage, and applications) are supplied to customers to access on-demand at any time. Service vendors are divided into infrastructure companies that control cloud systems and lease resources based on pricing models and provider companies that hire resources from infrastructure companies to provide services to customers. Because of the maturity of cloud computing generation and its benefits consisting of low cost, easy access to information, fast deployment, data backup, and automated software integration [1-2], the cloud has been widely used.

The Internet of Things (IoT) allows user to link billions of Intelligent Machines and to exchange information, monitoring, and manage for services which include home automation systems, related to each other, health care, Agriculture, security surveillance, energy grid, or important infrastructure control and manipulate the IoT is the next contemporary approach [3]. In which the borders between artificial and real environments are always being reduced by dynamic digitalization of physical systems equipped to deliver value-added services for mobile devices [4].

The notion of IoT cloud computing (IoT-Cloud) is involved with the combination of IoT technology with cloud computing resources [5-6]. IoT technology is integrated with cloud especially for two reasons; first, the IoT companies need to gain characteristics of cloud computing which include on-demand self-service, resource pooling, large network, measured service, and rapid elasticity [7]; second, it is for the sake of alleviating the excessive needs of data storage and processing from the resource-limited IoT technology [8]. As a result, from a high-level view, IoT technology seems well-integrated with the cloud to establish a uniform infrastructure for IoT cloud applications [9]. This phenomenon of integrating IoT technology with the cloud is also known as the Cloud of Things [10], CloudIoT [11], or Edge IoT [12]. Apart from assuaging the sources constrained behavior, and enhancing the device performance of IoT technology, the IoT cloud also permits a new venue for designing and deploying security solutions for IoT technology [13]. The amalgamation of IoT, cloud, and large data is presently trending [14].

IoT cloud has come with its challenges such as security problems which could dismay the complete paradigm. IoT cloud security problems are the combination of IoT technology protection [15-16], cloud security [17-18], and those arising from IoT cloud architecture. This paper surveys security problems that are specific to the IoT cloud paradigm, and to our knowledge, it is the first paper of its kind.

This paper includes the following, Section II presents the background of the research, Section III discusses the security challenges in the IoT cloud, and Section IV gives security solutions in the literature. Finally, Section V discussion and Section VI conclude the paper.

Background

Cloud Computing services are implemented in many fields relevant to the IoT, such as Genomics Data Processing, Teaching, and Studying, Services for Small and Medium Businesses, E-Learning Method, Augmented Reality, Manufacturing, Emergency Recovery, Smart Cities and others, Remote Forensics, Hospitality Business, E-Government and Human Resource Administration, Internet of Cars [19-20]. Challenges in cloud computing and the IoT separately and in Application environments that might be unique [21]. Critical problems in researching how the IoT and Cloud Computing will be included yielded inconclusive findings.

Cloud computing and IoT have spread globally and improved quickly in the latest years [22]. The characteristics they display can be excellent when combined. They are each unique and essential for each other [23]. Researchers scheduled several applications regarding Coordination of Cloud and IoT to develop and acquire information because it receives assistance from cloud storage and computational capability. In this part, then explain the Cloud-IoT (Cloud and IoT) architecture.

IoT cloud paradigm includes its new sets of programs and smart services most of which have been conventionally deployed as a machine to machine communications. This section, discusses, however, the set of programs that have been improved to be used in the IoT cloud paradigm.

Smart Home

The Internet of Things taking shape of companies is growing goods and products for making our living style more convenient and simpler[23]. This application of the Internet of things becomes as common as smartphones, Smart Home has come to be the modern development for succeeding in the residential areas and it is predicted. In a homeowner's life, the price of owning a house is the most significant expense. These utility's products are promised to store energy, money, and time [24].

Like the previous applications, the need of using IoT cloud sensors in smart houses is becoming mandatory[25]. An IoT cloud platform that enables analytics on data captured from smart homes [26]. The proposed data-driven carrier uses fog nodes and cloud systems for online data processing, storage, and classification. The researchers employ a policy-based access control mechanism to make sure trusted connectivity and protection of their platform. Some researchers proposed IoT cloud structure for specific aspects including sustainability in which the architecture is focusing on low electricity consumption and environmental friendliness of the things. A generic IoT cloud structure is provided by [27]. In which data collected from a smart city can be stored, processed and managed.

Smart Cities

Another powerful application of the Internet of things is smart cities that are producing curiosity among the world's population. Environmental monitoring, city security, water distribution, smarter electricity control systems, smart waste control system, computerized transportation, and smart surveillance are examples of many different Internet of Things applications for smart cities [28]. IoT cloud gives middleware for future-orientated smart city services by gathering data about the geographical area of various sensing technology and exposing that data uniformly. Some researchers have proposed crowdsourced and reputation based smart city frameworks that enforce sensing as a provider aimed at public safety [29-30].

Wearable Products

Wearable products can gather data and information about the users through sensors and software which might be installed within[31]. For extracting important insights about the user and consumers this information is later pre-processed. These wearable products widely cover entertainment, fitness, and fitness requirements. It is distinctly recommended that the IoT generation for wearable products is to be ultra-low energy or highly energy-efficient and small-sized [32]. The systems also use IoT cloud technology for their devices because with advanced systems their work becomes more efficient.

Healthcare

In case of emergency, it'll alert the neighborhood by calling an ambulance, patients can be handled in nearby hospitals and report their families in the emergency period automatically. It also monitors patient's document through Wi-Fi way over the internet [33]. It indicates various applications based on Cloud integrated IoT enabled sensors. As the technology evolves day by day, we want to provide a properly secured environment for information and it is inevitable to observe that a larger number of attackers arise to access important information. Thus it's far proposed to investigate numerous kinds of attacks in IoT enabled cloud computing environment and preventive measures for securing our information in the cloud surroundings.

Smart Retail

The ability of the Internet of Things in the retail location and sector may be huge. The Internet of Things presents a possibility for retailers for connecting and interchanging with the clients for enhancing the in-store experience. Indeed, even out of the shop the stores can continue and extent connection with their purchasers through taking advantage of smartphones. Using Beacon technology and interacting through smartphones should benefiting retailers for serving their purchasers better. They can moreover do enhancing the shop's layout and location premium products in high visitor's areas by monitoring consumer's paths through a store [34].

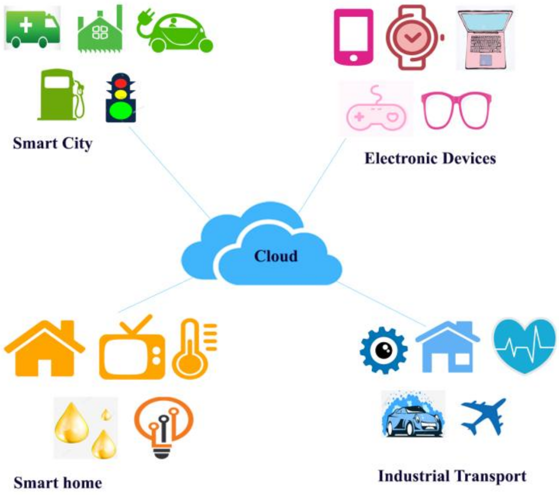

Fig-1: IoT Cloud computing

IoT Cloud Security Challenges

Cloud computing security is the main issue to be addressed nowadays. And information protection is the most important challenges in IoT cloud computing [35]. Data loss will have a severe impact on the brand business, and trust of an organization. If safety features aren't performed properly for information operations and transmission, the data is at high risk. The strongest safety features are to be carried out by identifying security challenges and solutions to deal with those challenges. Data security task in IoT cloud and it is clear that information leak presentation and information segregation and protection has a greater effect on protection challenges.

During the transfer process of the data from smart devices to the IoT cloud, access to the cloud is accomplished through Wi-Fi networks. Since the client does not have access to the data or can't have to manage the data, then there's a danger of unauthorized access to the offloaded content, subsequently, processing of the loaded data is carried out at the cloud, and then there may appear another incident in which the integrity of the data is violated.

The security incidents in IoT cloud applications are approximately compromising the integrity, confidentiality, and availability of each data and applications. Security problems specific to the IoT cloud paradigm are rarely mentioned in the literature. Nevertheless, the security challenges of IoT cloud programs may also appear at the IoT device level, and communication and networking level. Security problems related to IoT cloud systems for the smart home is very well discussed in [33].

Data from IoT was located in the Cloud for processing and retrieval. It involves encryption of data dispatched to or stored in cloud-based repositories and data protection throughout cloud access and use. [36-37]. The degree to which there's a loss of cloud computing statistics is such that data owners do not recognize their personal records' physical position. Today, data is associated with all around us, so data protection in the Cloud-IoT paradigm is the main topic [38].

LITERATE REVIEW ON IoT CLOUD SECURITY SOLUTION

This section presents the current solutions proposed in the literature of IoT cloud. There are a couple of researches that have deliberated to get solutions to the security problems specific to the IoT cloud paradigm. Moreover, a summary of the solutions is provided in Table 1. The solutions presented in Table 1 do not include those focusing on the IoT and cloud computing differently, rather they're the solutions that consider IoT cloud as one region and, hence, trying to propose their solutions in that aspect. Table highlight the security characteristic in every solution as well as the target area of the paradigm.

Table-1: Literate on IoT Cloud security solution

Paper	Problems	Solutions
[39]	Internet of Things (IoT) turning into so pervasive that it is becoming essential to integrate it with cloud computing.	IoT's and cloud computing integration isn't always that easy and bears some key troubles. Those key troubles alongside their respective potential solutions were highlighted.
[40]	Integration of the Internet of Things with Cloud Computing is gaining importance, with the way the trend is going on in the ubiquitous computing world and its products so many problems for this system.	In this paper, the researcher focuses on some of the key challenges involved in CoT and the proposal of smart gateway based communication.
[41]	Internet of Things (IoT) and cloud computing (CC) had been extensively studied and carried out in many fields, as they could provide a brand new method for smart perception and connection from M2M and on-demand use. It's produced so many security challenges for user's data.	A CC- and IoT-based cloud manufacturing (CMfg) service system and its architecture are proposed because these systems can overcome security challenges in IoTCloud.
[42]	A novel paradigm in which Cloud and IoT are merged is foreseen as disruptive and as an enabler of a large range of software scenarios.	A new CloudIoT paradigm, which involves completely new applications, challenges, and research issues and this system provide effective usability.
[43]	The limitations of associated devices in the IoT require technology like Cloud Computing to supplement this field because this technology can provide these services for users.	A survey of integration components: Cloud platforms, Cloud infrastructures and IoT Middleware helps to understand about IoTCloud technology.
[44]	Lack of investigating on powerful and efficient evaluations and measurements for safety and trustworthiness of numerous social media tools, systems and applications.	Propose a hierarchical architecture for crowd evaluations based on signaling theory and crowd computing that can work properly.
[45]	The issues of continuity, resilience and survivability of data on smart devices and these issues also have an impact on smart devices.	It allows securing of devices Personal Zone Proxy (PZP) and Personal Zone Hub (PZH) while utilizing relevant contextual data in the device environment to provide higher service and extra secure communication environment.
[46]	The IoT gateway depends only on the type of the IoT network and these networks have different types of security challenges.	The security architecture is based on the standards of network function virtualization (NFV) and service function chaining (SFC) for composing safety services.
[47]	IoT and cloud computing technology are very effective for neuroscientist but on other hand, data security is also an issue.	Introduces a Neuro-Fuzzy based Brain-inspired trust management model (TMM) to secure IoT devices and relay nodes, and to ensure data reliability for the data providers
[48]	It does not provide the customer sufficient method of performing reasonableness checks to confirm that the provider is not accidentally or maliciously contaminating the evidence.	A common cloud forensic system proposed by researchers is 'Cloud-Forensic-as-a-Service' in which consumers have to get entry to it as a service to acquire forensic information from cloud environments.

DISCUSSION

Based on the security challenges presented in this paper, it is apparent that security problems about IoT cloud entail a new set of security challenges from the emerging usage of the paradigm. This new set of security challenges have become tougher to deal with for the integration of IoT technology and the cloud. Despite the existence of some security solutions in the literature, there are still a few open problems that deserve the attention of the safety community. A first secure reference structure is wanted to coin maximum of the security requirements that IoT cloud need. The cost-effectiveness of the solutions proposed inside the literature is not mentioned in most cases, hence, the deployment of such solutions isn't on the real horizon, thus not cost-effective. In addition, the IoT cloud architecture introduces communications among different technology. Such communications tend to be secured as well they can for users. Here, lightweight secure communication protocols are recommended which can be used for security purpose. There is also a need for algorithms that may create trust between IoT technology and the cloud. More researches on lightweight solutions for securing digital machines in the IoT cloud is an added value.

CONCLUSION

In recent years, both academia and business agencies have drawn an interest in IoT technology. It is now an essential element of our lives. It can link almost everything in our global to everything else. IoT systems are complicated in design and have restricted capacities for storage and retrieval. The integration of cloud computing with IoT could provide multiple benefits to numerous IoT programs. We have mentioned in this article the modern cloud infrastructure, together with cloud features, architecture, and benefits. The topic also focused on numerous technology for IoT that could be increased throughout the Cloud. Challenges of cloud IoT deployment and transparent issues also are mentioned. In general, this paper's purpose was to include an outline to summarize up to date studies contributions on cloud computing and the IoT and its programs in our environment and illustrate potential research directions and real issues regarding the integration with the IoT of cloud computing security.

REFERENCES

1. Aazam, M., Hung, P. P., & Huh, E.-N. (2014). Smart gateway based communication for cloud of things. 2014 {IEEE} Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing ({ISSNIP}). https://doi.org/10.1109/issnip.2014.6827673
2. Aazam, M., Khan, I., Alsaffar, A. A., & Huh, E.-N. (2014). Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved. Proceedings of 2014 11th International Bhurban Conference on Applied Sciences {\&} Technology ({IBCAST}) Islamabad, Pakistan, 14th - 18th January, 2014. https://doi.org/10.1109/ibcast.2014.6778179
3. Abdullah, P. Y., Zeebaree, S. R. M., Jacksi, K., & Zeabri, R. R. (2020). {AN} {HRM} {SYSTEM} {FOR} {SMALL} {AND} {MEDIUM} {ENTERPRISES} ({SME})S {BASED} {ON} {CLOUD} {COMPUTING} {TECHNOLOGY}. International Journal of Research - {GRANTHAALAYAH}, 8(8), 56–64. https://doi.org/10.29121/granthaalayah.v8.i8.2020.926
4. Abdulraheem, A. S., Zeebaree, S. R. M., & Abdulazeez, A. M. (n.d.). Design and Implementation of Electronic Human Resource Management System for Duhok Polytechnic University.
5. Adel, A. (2020). Utilizing technologies of fog computing in educational {IoT} systems: privacy, security, and agility perspective. Journal of Big Data, 7(1). https://doi.org/10.1186/s40537-020-00372-z
6. Al-athwari, B., & Azam, H. M. (2020). Resource Allocation in the Integration of IoT, Fog, and Cloud Computing: State-of-the-Art and Open Challenges. International Conference on Smart Computing and Cyber Security: Strategic Foresight, Security Challenges and Innovation, 247–257.
7. Aliyu, F., Sheltami, T., Mahmoud, A., Al-Awami, L., & Yasar, A. (2021). Detecting Man-in-the-Middle Attack in Fog Computing for Social Media. Computers, Materials {\&} Continua, 69(1), 1159–1181. https://doi.org/10.32604/cmc.2021.016938
8. Alzakholi, O., Haji, L., Shukur, H., Zebari, R., Abas, S., & Sadeeq, M. (2020). Comparison Among Cloud Technologies and Cloud Performance. Journal of Applied Science and Technology Trends, 1(2), 40–47. https://doi.org/10.38094/jastt1219
9. Arabo, A. (2014, November). Privacy-aware {IoT} cloud survivability for future connected home ecosystem. 2014 {IEEE}/{ACS} 11th International Conference on Computer Systems and Applications ({AICCSA}). https://doi.org/10.1109/aiccsa.2014.7073283
10. Araujo, V., Mitra, K., Saguna, S., & Åhlund, C. (2019). Performance evaluation of {FIWARE}: A cloud-based {IoT} platform for smart cities. Journal of Parallel and Distributed Computing, 132, 250–261. https://doi.org/10.1016/j.jpdc.2018.12.010
11. Bhawiyuga, A., Kartikasari, D. P., Amron, K., Pratama, O. B., & Habibi, M. W. (2019). Architectural design of {IoT}-cloud computing integration platform. {TELKOMNIKA} (Telecommunication Computing Electronics and Control), 17(3), 1399.
12. binti Mohamad Noor, M., & Hassan, W. H. (2019). Current research on Internet of Things ({IoT}) security: A survey. Computer Networks, 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025
13. Ezzat, M. A., Ghany, M. A. A. El, Almotairi, S., & Salem, M. A.-M. (2021). Horizontal Review on Video Surveillance for Smart Cities: Edge Devices, Applications, Datasets, and Future Trends. Sensors, 21(9), 3222. https://doi.org/10.3390/s21093222
14. Fernández-Caramés, T., & Fraga-Lamas, P. (2018). Towards The Internet-of-Smart-Clothing: A Review on {IoT} Wearables and Garments for Creating Intelligent Connected E-Textiles. Electronics, 7(12), 405. https://doi.org/10.3390/electronics7120405
15. Gómez, J., Oviedo, B., & Zhuma, E. (2016). Patient Monitoring System Based on Internet of Things. Procedia Computer Science, 83, 90–97. https://doi.org/10.1016/j.procs.2016.04.103
16. H., Z., A., H., & M., M. (2015). Internet of Things ({IoT}): Definitions, Challenges and Recent

Research Directions. International Journal of Computer Applications, 128(1), 37–47. https://doi.org/10.5120/ijca2015906430

17. Haji, L. M., Ahmad, O. M., Zeebaree, S. R. M., Dino, H. I., Zebari, R. R., & Shukur, H. M. (2020). Impact of cloud computing and internet of things on the future internet. Technology Reports of Kansai University, 62(5), 2179–2190.
18. Haji, L. M., Zeebaree, S. R., Ahmed, O. M., Sallow, A. B., Jacksi, K., & Zeabri, R. R. (2020). Dynamic resource allocation for distributed systems and cloud computing. TEST Engineering \& Management, 83, 22417–22426.
19. Haji, S. H., Zeebaree, S. R. M., Saeed, R. H., Ameen, S. Y., Shukur, H. M., Omar, N., Sadeeq, M. A. M., Ageed, Z. S., Ibrahim, I. M., & Yasin, H. M. (2021). Comparison of Software Defined Networking with Traditional Networking. Asian Journal of Research in Computer Science, 1–18. https://doi.org/10.9734/ajrcos/2021/v9i230216
20. Hussan, B. K. (2020). Comparative Study of Semantic and Keyword Based Search Engines. Advances in Science, Technology and Engineering Systems Journal, 5(1), 106–111. https://doi.org/10.25046/aj050114
21. Jiang, J., Li, Z., Tian, Y., & Al-Nabhan, N. (2020). A Review of Techniques and Methods for {IoT} Applications in Collaborative Cloud-Fog Environment. Security and Communication Networks, 2020, 1–15. https://doi.org/10.1155/2020/8849181
22. Kandan, S. R., Dhanasekar, N., & Avirajamanjula, P. (2020). Unifying Cloud Computing with Internet of Things Using Secured Protocol. In Internet of Things (pp. 153–164). CRC Press.
23. Kantarci, B., & Mouftah, H. T. (2014). Trustworthy Sensing for Public Safety in Cloud-Centric Internet of Things. {IEEE} Internet of Things Journal, 1(4), 360–368. https://doi.org/10.1109/jiot.2014.2337886
24. Khan, M. A., & Salah, K. (2018). {IoT} security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411. https://doi.org/10.1016/j.future.2017.11.022
25. Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1–48. https://doi.org/10.1016/j.cosrev.2019.05.002
26. Mahmud, M., Kaiser, M. S., Rahman, M. M., Rahman, M. A., Shabut, A., Al-Mamun, S., & Hussain, A. (2018). A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based {IoT} Framework for Neuroscience Applications. Cognitive Computation, 10(5), 864–873. https://doi.org/10.1007/s12559-018-9543-3
27. Massonet, P., Deru, L., Achour, A., Dupont, S., Croisez, L.-M., Levin, A., & Villari, M. (2017, August). Security in Lightweight Network Function Virtualisation for Federated Cloud and {IoT}. 2017 {IEEE} 5th International Conference on Future Internet of Things and Cloud ({FiCloud}). https://doi.org/10.1109/ficloud.2017.43
28. Mishra, J. K. (2020). Cloud-Based Internet of Things: Security and challenges of The Integrated Environment. Solid State Technology, 63(2s).
29. Mohamed, K. S. (2019). {IoT} Cloud Computing, Storage, and Data Analytics. In The Era of Internet of Things (pp. 71–91). Springer International Publishing. https://doi.org/10.1007/978-3-030-18133-8_4
30. Moussa, A. N., Ithnin, N., & Zainal, A. (2018). {CFaaS}: bilaterally agreed evidence collection. Journal of Cloud Computing, 7(1). https://doi.org/10.1186/s13677-017-0102-3
31. Nadeem, M. W., Goh, H. G., Hussain, M., a/p Ponnusamy, V., Hussain, M., & Khan, M. A. (2021). Internet of Things for Green Building Management. In Role of {IoT} in Green Energy Systems (pp. 156–170). {IGI} Global. https://doi.org/10.4018/978-1-7998-6709-8.ch007
32. P.Saharan, K., & Kumar, A. (2015). Fog in Comparison to Cloud: A Survey. International Journal of Computer Applications, 122(3), 10–12. https://doi.org/10.5120/21679-4773
33. R, P. M. B., and Vaishnavi K R, & Gowda, D. N. (2019). {IoT} Based Home Automation System over Cloud. International Journal of Trend in Scientific Research and Development, Volume-3(Issue-4), 966–968. https://doi.org/10.31142/ijtsrd24005
34. Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 48, 204–209. https://doi.org/10.1016/j.procs.2015.04.171
35. Sadeeq, M. A., Abdulla, A. I., Abdulraheem, A. S., & Ageed, Z. S. (2020). Impact of Electronic Commerce on Enterprise Business. Technol. Rep. Kansai Univ, 62(5), 2365–2378.
36. Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R. M., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). {IoT} and Cloud Computing Issues, Challenges and Opportunities: A Review. Qubahan Academic Journal, 1(2), 1–7. https://doi.org/10.48161/qaj.v1n2a36
37. Serrano, D., Bouchenak, S., Kouki, Y., Ledoux, T., Lejeune, J., Sopena, J., Arantes, L., & Sens, P. (2013, May). Towards {QoS}-Oriented {SLA} Guarantees for Online Cloud Services. 2013 13th {IEEE}/{ACM} International Symposium on Cluster, Cloud, and Grid Computing. https://doi.org/10.1109/ccgrid.2013.66
38. Sha, K., Yang, T. A., Wei, W., & Davari, S. (2020). A survey of edge computing-based designs for iot security. Digital Communications and Networks, 6(2), 195–202.
39. Sharma, S., Chang, V., Tim, U. S., Wong, J., & Gadia, S. (2018). Cloud and {IoT}-based emerging services systems. Cluster Computing, 22(1), 71–91.

https://doi.org/10.1007/s10586-018-2821-8

40. Shukur, H. M., Zeebaree, S. R. M., Zebari, R. R., Hussan, B. K., Jader, O. H., & Haji, L. M. (2021). Design and Implementation of Electronic Enterprise University Human Resource Management System. Journal of Physics: Conference Series, 1804(1), 12058. https://doi.org/10.1088/1742-6596/1804/1/012058
41. Shukur, H., Zeebaree, S., Zebari, R., Zeebaree, D., Ahmed, O., & Salih, A. (2020). Cloud Computing Virtualization of Resources Allocation for Distributed Systems. Journal of Applied Science and Technology Trends, 1(3), 98–105. https://doi.org/10.38094/jastt1331
42. Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454–1464. https://doi.org/10.1016/j.jclepro.2016.10.006
43. Tao, F., Cheng, Y., Xu, L. Da, Zhang, L., & Li, B. H. (2014). {CCIoT}-{CMfg}: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System. {IEEE} Transactions on Industrial Informatics, 10(2), 1435–1442. https://doi.org/10.1109/tii.2014.2306383
44. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). {IoT} Privacy and Security: Challenges and Solutions. Applied Sciences, 10(12), 4102. https://doi.org/10.3390/app10124102
45. Wang, Z., Wang, N., Su, X., & Ge, S. (2020). An empirical study on business analytics affordances enhancing the management of cloud computing data security. International Journal of Information Management, 50, 387–394. https://doi.org/10.1016/j.ijinfomgt.2019.09.002
46. Yassine, A., Singh, S., Hossain, M. S., & Muhammad, G. (2019). {IoT} big data analytics for smart homes with fog and cloud computing. Future Generation Computer Systems, 91, 563–573. https://doi.org/10.1016/j.future.2018.08.040
47. Zarko, I. P., Antonic, A., & Pripužic, K. (2013, September). Publish/subscribe middleware for energy-efficient mobile crowdsensing. Proceedings of the 2013 {ACM} Conference on Pervasive and Ubiquitous Computing Adjunct Publication. https://doi.org/10.1145/2494091.2499577
48. Zhou, W., Jia, Y., Yao, Y., Zhu, L., Guan, L., Mao, Y., Liu, P., & Zhang, Y. (2019). Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms. 28th {USENIX} Security Symposium ({USENIX} Security 19), 1133–1150. https://www.usenix.org/conference/usenixsecurity19/presentation/zhou