# Discovering and Understanding The Security Issues In IoT Cloud

***Nawaf Almolhis*** *almo3113@vandals.uidaho.edu*
[a] *Computer Science Department*
*University of Idaho*
*Moscow, ID, 83844, USA*
[b] *Computer Science Department*
*Jazan University*
*Jazan, 45142, Saudi Arabia*

**Michael Haney** *mhaney@uidaho.edu*
*Computer science department*
*University of Idaho*
*Idaho Falls, ID, 83401, USA*

**Fahad Alqahtani** *alqa0199@vandals.uidaho.edu*
[a] *Computer Science Department*
*University of Idaho*
*Moscow, ID, 83844, USA*
[b] *Computer Science Department*
*Prince Sattam Bin Abdulaziz University*
*Al-Kharj, 16278, Saudi Arabia*

**Khalid Makdi** *alma0138@vandals.uidaho.edu*
[a] *Computer Science Department*
*University of Idaho*
*Moscow, ID, 83844, USA*
[b] *Computer Science Department*
*Najran University*
*Najran, 66223, Saudi Arabia*

### Abstract

The rapid growth and adoption of IoT technologies in sectors of life are challenged by the resources constrained IoT devices. However, the growth of IoT technologies can be enhanced by integrating them with cloud computing. Hence, a new area of computing called IoT Cloud or CloudIoT has emerged. That is, the data collected from the IoT technologies are stored and processed in the cloud infrastructure so that IoT technologies are relived from resources constrained issue. As a result, some new classes of security and privacy issues are introduced. This paper presents security issues pertaining to IoT cloud.

**Keywords:** IoT, Cloud, Privacy, Security, CloudIoT.

## 1. INTRODUCTION

Internet of Things (IoT) is the fast-growing information technology paradigm of this digital era. The number of IoT consumers is increasing due to the deployment of IoT technologies in all sorts of life [1]. At present, the IoT technologies are vastly deployed in the health sector [2, 3], smart cities [4], and smart homes [5, 6]. However, IoT technology alone cannot fully satisfy the increasing number of consumers and their computational requirements. Hence, the need for offloading IoT computations to the cloud has become paramount.

The notion of IoT cloud computing (IoT-Cloud) is concerned with the integration of IoT technologies with cloud computing resources [7-9]. IoT technologies are integrated with cloud mainly for two reasons; first, the IoT providers want to benefit of characteristics of the cloud computing such as on-demand self-service, resource pooling, broad network, measured service, and rapid elasticity [10]; second, it is for the sake of alleviating the high demands of data storage and processing from the resource-limited IoT technologies [11]. As a result, from a high-level view, IoT technologies appear to be well-integrated with the cloud to establish a uniform infrastructure for IoT cloud applications [12]. This phenomenon of integrating IoT technologies with the cloud is also referred to as the Cloud of Things [13], CloudIoT [14], or Edge IoT [15]. Apart from alleviating the resources constrained behavior, and improving the system performance of IoT technologies, the IoT cloud also enables a new venue of designing and deploying security solutions for IoT technologies [15]. The amalgamation of IoT, cloud, and big data is currently trending [16].

In fact, IoT cloud has come with its own challenges including security issues that may dismay the whole paradigm. IoT cloud security issues are the aggregate of IoT technologies security [17, 18], cloud security [19, 20], and those arising from IoT cloud architecture. This paper surveys security issues that are specific to IoT cloud paradigm, and to our knowledge, it is the first paper of its kind.

The paper is organized as follows, Section 2 presents the background of the research, Section 3 discusses the security challenges related to the IoT cloud, and Section 4 concludes the paper.

## 2. BACKGROUND

This section discusses areas of intersection of the IoT and Cloud computing. Specifically, the drivers that make the integration of IoT technologies and the cloud more important, and the IoT cloud applications. Furthermore, some of the architectures proposed for IoT cloud are studied. Finally, challenges and issues related to the IoT Cloud are presented.

### 2.1 IoT Cloud Drivers

IoT and cloud computing are from two different worlds. However, their characteristics are complementary, and that is the main reason why in the literature their integration is seen beneficial for both. That is, IoT can benefit from some aspects of cloud, likewise, IoT can help cloud in some other aspects [21]. For instance, the virtually unlimited resources of cloud can compensate the IoT resource constrains and, IoT can extend cloud services in a more distributed manner and may bring about new real-world service [22]. The driving motivations towards the integration of cloud and IoT mainly lay on three categories including communication, storage, and computing. In communication, data and application sharing are the two main IoT Cloud drivers [23]. In regards to the storage, by definition IoT technologies normally produce large amounts of semi-structured or non-structured data that are generated frequently in large volumes and varieties. Hence, making use of the virtually unlimited storage capacity of the cloud such data can be stored in the cloud. On the other hand, in computing, IoT technologies normally suffer from limited processing and energy resources [24]. These do not allow IoT devices complex data processing. Using cloud computing resources, IoT devices will be able to process data on-site. These are the main motivations that are driving the integration of IoT and Cloud [25]. Table 1 shows aspects where cloud and IoT may complement each other.

| Criteria | IoT | Cloud |
|---|---|---|
| Displacement | pervasive | centralized |
| Reachability | limited | ubiquitous |
| Components | real-world things | virtual resources |
| Computational Capabilities | limited | virtual unlimited |
| Storage | limited or none | virtual unlimited |
| Role of the internet | point of convergence | means of delivering services |
| Big data | source | means to manage data |

**TABLE 1:** Complementary aspects of Cloud and IoT.

## 2.2 IoT Cloud Application

IoT cloud paradigm has come with its new sets of applications and smart services most of which were conventionally deployed as a machine to machine communications. This section, discusses, however, the set of applications that have been improved in order to be used in the IoT cloud paradigm. Figure 1 shows an abstract picture of the IoT cloud applications scenario.

### 2.2.1 Smart Cities

The adoption of the IoT cloud has generated services like smart city applications that can interact with the surrounding environment to create geographic awareness and contextualization opportunities. IoT cloud provides middleware for future-oriented smart city services by collecting information about the geographical location of different sensing technologies and exposing that information uniformly. Most of the current smart application frameworks consist of APIs of sensors and actuators that are directly connected to cloud platforms where they can get scalability, durable storage and processing resources for automatic management and control of large deployments of sensing devices. For example, some researchers have proposed crowdsourced and reputation based smart city frameworks that implement sensing as a service aimed at public safety [26, 27]. Likewise, mobile crowdsensing smart cities technology that uses cloud-based publish/subscribe middleware that collects data from mobile devices are proposed in [28, 29].

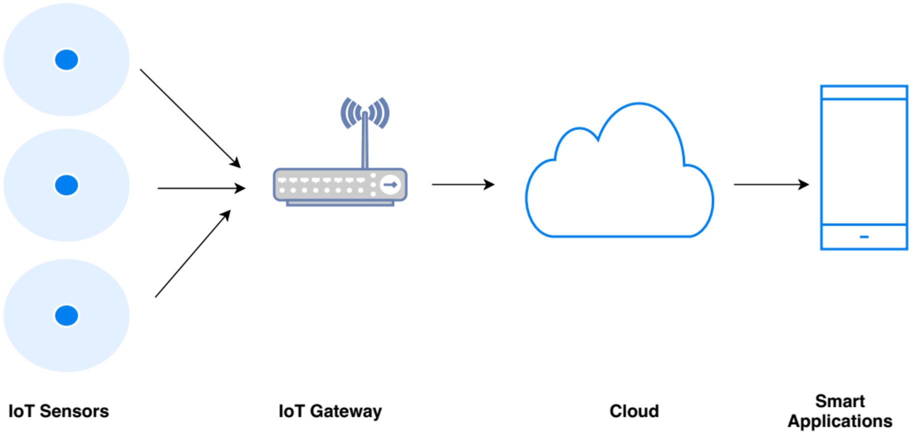

**FIGURE 1:** IoT Cloud Application Scenario.

### 2.2.2 Healthcare

In the healthcare industry, things like sensors and devices used for health monitoring are increasing and hugely impacting on patients and health professionals. According to IoT Forbes and Gartner, in 6 years' time from 2016-2020, the healthcare IoT market will be invested with $117 billion [30]. IoT cloud applications are immensely developed for this aspect. Some of the recent works of IoT cloud applications proposed for health care are discussed here. For example, Syed et al. have proposed an asthma patient health monitoring system that connects to the cloud using wireless body area networks [30]. For security, the researchers have watermarked the recorded signal before sending it to the cloud. Douglas et al. also proposed an efficient healthcare IoT cloud architecture for ambient assisted living environments [31]. The advantages of using IoT cloud in healthcare are discussed in [32].

### 2.2.3 Smart Home

In recent years, high development of smart home applications that use different sensors such as motion, light, and fire detector sensors, etc have been observed. Data collected from these sensors are used for decision making. Hence, like the preceding applications, the necessity of employing IoT cloud sensors in smart homes is becoming mandatory [33]. For instance, Yassine et al. proposed an IoT cloud platform that enables analytics on data captured from smart homes [34]. The proposed data-driven service uses fog nodes and cloud systems for online data processing, storage, and classification. The researchers employ a policy-based access control mechanism to ensure trusted connectivity and security in their platform.

## 2.3 IoT Cloud Architecture

There are efforts made towards the definition of a reference architecture for IoT cloud. For example, Jenjira Jaimunk proposed Data Bank, an IoT cloud architecture that allows users to customize their data collection policies at the IoT device level and data sharing policies at the cloud level, as suited to their privacy needs [35]. Similarly, some researchers proposed IoT cloud architecture for different aspects such as for sustainability [36] where the architecture is focusing on low power consumption and environmental friendliness of the things. A generic IoT cloud architecture is provided by Araujo et al. [37], where data collected from a smart city can be stored, processed and managed.

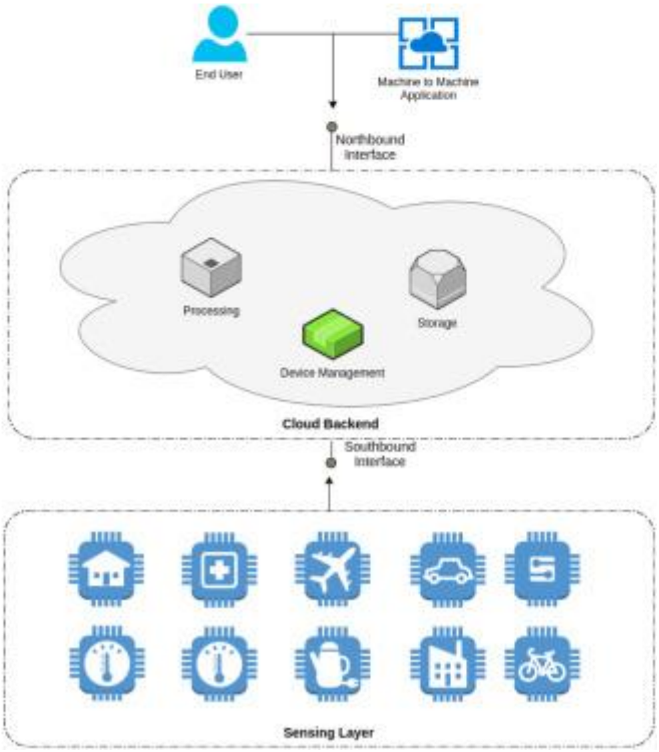

**FIGURE 2:** A Generic IoT Cloud Architecture [37].

As can be seen in Figure 2, the architecture provides a southbound interface where IoT technologies interact with the cloud and a northbound interface where higher-level services such as M2M applications and end consumers interact with the IoT cloud.

## 2.4 Security IoT Cloud Challenges

Even though the IoT cloud is advantageous for both consumers and providers, it is still facing some issues that threaten its usage. The heterogeneity of the IoT technologies, clouds, operating systems, network protocols from different vendors generates a more challenging environment that may result in a lack of interoperability and portability in IoT cloud [32, 38]. In addition, in IoT cloud, cloud elasticity and scalability is required. If for instance, IoT cloud provider resources do not meet the increased demand for IoT technologies, interruption or unavailability of the services may result in problem [39]. Security challenges pertaining to the IoT cloud environment are more volatile compared to the security issues in conventional cloud computing. For example, due to the limited resource of IoT technologies, it is not practical to run anti-virus on the IoT devices.

## 3. SECURITY CHALLENGES IN IOT CLOUDS

After having seen the basics of IoT clouds, this section discusses security challenges within IoT cloud. Such security issues may usually result from different parts of technologies constituting the IoT cloud.

### 3.1 Security Challenges Related To Data

The data security issues are mainly introduced as the consequence of when smart home owner data are transferred, stored, and processed at clouds that are not part of his network and belong to a third person. The data related security issues that may happen include data loss and data breach. The data loss refers to the data damage that may happen to consumer data. On the other hand, data breach means when the consumer data is taken by an unauthorized individual.

### 3.2 Offloading Security Challenge

During the transfer process of the data from smart devices to the IoT cloud, access to the cloud is accomplished through wireless networks. Since the consumer does not have access to the data or cannot have control over the data, then there is a risk of unauthorized access to the offloaded content, subsequently, processing of the loaded data is done at the cloud, then there may happen another incident where the integrity of the data is violated.

### 3.3 Virtualization Security Challenge

The IoT cloud service is provided by using some virtualization techniques. Hence, at the provider side of the IoT cloud, the consumer data is stored and processed on a virtual machine. However, in the cloud, there may be a number of virtual machines abstracted from the same physical server. Hence, a rogue user of a virtual machine may get unauthorized access to a neighboring virtual machine that stores the smart home consumer data.

### 3.4 IoT Cloud Applications Security Challenges

The security incidents in IoT cloud applications are about compromising the integrity, confidentiality, and availability of both data and applications. Security issues specific to the IoT cloud paradigm are hardly discussed in the literature. Nevertheless, the security challenges of IoT cloud applications may happen at IoT device level, and communication and networking level. Security issues associated with IoT cloud platforms for the smart home is thoroughly discussed in [40]. Likewise, security issues related to the IoT cloud-based healthcare systems can be found in [41].

Another main security issue arises due to a lack of trust in the service provider or the knowledge about service level agreement and knowledge about the physical location of data. Some other security challenges may include heterogeneity, performance, reliability, big data, and monitoring related. For example, the heterogeneity of devices involved in this integrated area may be focusing on the operating system, platform, and services availability [42, 43]. Likewise, those that may come with the performance are those threatening the availability of services such as communication, computation, and storage. Reliability issues may arise when mission-critical applications involving in IoT cloud may suffer from device failure due to a resource-constrained environment[44, 45]. Usually, thousands of smart devices (big data) networked with the cloud would create transportation, storage, access and processing of huge amounts of data that may scrutinize the limited resources of the IoT environment [46, 47]. Having no sophisticated authentication approaches also exacerbates the security associated with IoT cloud. Furthermore, intrusion-related security issues are of most importance for IoT Cloud. In the future as the adoption of cloud-connected IoT technologies increases, security concerns of this area are anticipated to be automatically added on top of currently known security issues.

### 3.5 IoT Cloud Security Solutions In The Literature

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 issues specific to the IoT cloud paradigm [48-64]. Moreover, the summary of the solutions is presented in Table 2. The solutions presented in Table 2 do not include those focusing on the IoT and cloud computing differently, rather they are the solutions that consider IoT cloud as one area and, hence, trying to propose their solutions in that aspect. Table highlight the security feature in each solution as well as the target area of the paradigm.

### 3.6 Discussions and Future Directions

Based on the security challenges presented in this paper, it is obvious that security issues pertaining to IoT cloud entail a new set of security challenges from the emerging usage of the paradigm. This new set of security challenges are becoming more difficult to handle for the integration of IoT technologies and cloud. Despite the existence of some security solutions in the literature, there are still some open issues that deserve the attention of the security community. A first secure reference architecture is needed to coin most of the security requirements that IoT cloud need. The cost-effectiveness of the solutions proposed in the literature is not discussed in most cases, hence, the deployment of such solutions is not on the real horizon, thus not cost-effective. In addition, the IoT cloud architecture introduces communications between different technologies. Such communications tend to be secured as well. Here, lightweight secure communication protocols are recommended. There is also a need for algorithms that can create trust between IoT technologies and the cloud. More researches on lightweight solutions for securing virtual machines in the IoT cloud is an added value.

So far researchers have indicated that improving or integrating existing solutions may to some extent handle some of the discussed security issues. However, there is also a need for developing new and dedicated security solutions for the area. What makes different the cloud-connected IoT architecture is that two (cloud and IoT) broadly different areas of technologies are involved. Each has its security issues and challenges where researchers are striving to get solutions. Nevertheless, getting an end to end security solution that would protect personal data collected from IoT end devices and stored or processed in the cloud is alarming.

Converging towards a common security platform for providing APIs to auditing IoT clouds will enable new research efforts in the direction of standard rules and policies that would hold consumers and providers accountable. Similarly, security solutions of IoT cloud would benefit from efficient and flexible technologies that can create a network and virtual machine isolation. Solutions that detects manipulation of data based on IoT clouds will enable enhanced context-based security services.

| Source | Title | Focus Area |
|---|---|---|
| [48] | Intrusion detection in Cloud Internet of Things Environment | Network security |
| [49] | A software defined network-based security assessment framework for cloudIoT | Network security |
| [50] | Secure Self-Destruction of Shared Data in Multi-CloudIoT | Data security |
| [51] | Secure and Parallel Expressive Search over Encrypted Data with Access Control in Multi-CloudIoT | Data security |
| [52] | PRTA: A Proxy Re-encryption based Trusted Authorization scheme for nodes on CloudIoT | Access control |
| [53] | A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment. | Network security |
| [54] | A Data Security Storage Method for IoT Under Hadoop Cloud Computing Platform | Data security |
| [55] | Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications | Access control |
| [56] | Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach | Access control |
| [57] | Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service | Management |
| [58] | Privacy-aware IoT cloud survivability for future connected home ecosystem | Privacy |
| [59] | Security in Lightweight Network Function Virtualisation for Federated Cloud and IoT | Network security |
| [60] | A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications | Trust |
| [61] | A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres | Digital forensics |
| [62] | A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services | Access control |
| [63] | IoT–Cloud collaboration to establish a secure connection for lightweight devices | Network security |
| [64] | Identity-based encryption with authorized equivalence test for cloud-assisted IoT | Access control |

**TABLE 2:** Solutions in Te Literature.

## 4. CONCLUSION

In this paper, we review the security challenges pertaining to the IoT cloud. The basics of the IoT cloud are reviewed, followed by the security challenges that a consumer may encounter when using smart devices that are connected to the cloud are discussed. Moreover, solutions in the literature are studied and presented. Open security research issues that need immediate attention from the research community are discussed and some prospect solutions that may work conveniently with the IoT cloud paradigm are recommended. Finally, we hope that this paper will be a good entry in enabling a secure integration of IoT technologies and cloud computing.

## 5. REFERENCES

[1] Alabady, S.A., F. Al-Turjman, and S. Din, *A novel security model for cooperative virtual networks in the IoT era.* International Journal of Parallel Programming, 2018: p. 1-16.

[2] Adhikary, T., et al. *The Internet of Things (IoT) Augmentation in Healthcare: An Application Analytics*. in *International Conference on Intelligent Computing and Communication Technologies*. 2019. Springer.

[3] da Silveira, F., et al., *Analysis of Industry 4.0 Technologies Applied to the Health Sector: Systematic Literature Review*, in *Occupational and Environmental Safety and Health*. 2019, Springer. p. 701-709.

[4] Arasteh, H., et al. *Iot-based smart cities: a survey*. in *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*. 2016. IEEE.

[5] Park, D.-M., S.-K. Kim, and Y.-S. Seo, *S-mote: SMART Home Framework for Common Household Appliances in IoT Network.* Journal of Information Processing Systems, 2019. 15(2).

[6] Mahmud, S., S. Ahmed, and K. Shikder. *A Smart Home Automation and Metering System using Internet of Things (IoT)*. in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*. 2019. IEEE.

[7] Mohamed, K.S., *IoT Cloud Computing, Storage, and Data Analytics*, in *The Era of Internet of Things*. 2019, Springer. p. 71-91.

[8] Zamora-Izquierdo, M.A., et al., *Smart farming IoT platform based on edge and cloud computing.* Biosystems engineering, 2019. 177: p. 4-17.

[9] Bhawiyuga, A., et al., *Architectural design of IoT-cloud computing integration platform.* Telkomnika, 2019. 17(3).

[10] Mircea, M., M. Stoica, and B. Ghilic-Micu, *Using Cloud Computing to Address Challenges Raised by the Internet of Things*, in *Connected Environments for the Internet of Things*. 2017, Springer. p. 63-82.

[11] Ali, Z.H., H.A. Ali, and M.M. Badawy, *A new proposed the internet of things (IoT) virtualization framework based on sensor-as-a-service concept.* Wireless Personal Communications, 2017. 97(1): p. 1419-1443.

[12] Nikolov, N. and O. Nakov. *Creating Architecture and Software of Embedded Systems with Constrained Resources and Their Communication to the IoT Cloud*. in *2019 X National Conference with International Participation (ELECTRONICA)*. 2019. IEEE.

[13] Aazam, M., et al. *Cloud of Things: Integrating Internet of Things and cloud computing and the issues involved*. in *Proceedings of 2014 11th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 14th-18th January, 2014*. 2014. IEEE.

[14] Serrano, D., et al. *Towards qos-oriented sla guarantees for online cloud services*. in *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*. 2013. IEEE.

[15] Sha, K., et al., *A survey of edge computing based designs for IoT security.* Digital Communications and Networks, 2019.

[16] Sharma, S., et al., *Cloud and IoT-based emerging services systems.* Cluster Computing, 2019. 22(1): p. 71-91.

[17] Hassan, W.H., *Current research on Internet of Things (IoT) security: A survey.* Computer Networks, 2019. 148: p. 283-294.

[18] Khan, M.A. and K. Salah, *IoT security: Review, blockchain solutions, and open challenges.* Future Generation Computer Systems, 2018. 82: p. 395-411.

[19] Kumar, R. and R. Goyal, *On cloud security requirements, threats, vulnerabilities and countermeasures: A survey.* Computer Science Review, 2019. 33: p. 1-48.

[20] Wang, Z., et al., *An empirical study on business analytics affordances enhancing the management of cloud computing data security.* International Journal of Information Management, 2019.

[21] Gomes, M.M., R.d.R. Righi, and C.A. da Costa. *Future directions for providing better IoT infrastructure*. in *Proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing: Adjunct Publication*. 2014. ACM.

[22] Alhakbani, N., et al. *A framework of adaptive interaction support in cloud-based internet of things (iot) environment*. in *International conference on internet and distributed computing systems*. 2014. Springer.

[23] Aitken, R., et al. *Device and technology implications of the Internet of Things*. in *2014 Symposium on VLSI Technology (VLSI-Technology): Digest of Technical Papers*. 2014. IEEE.

[24] Botta, A., et al., *Integration of cloud computing and internet of things: a survey.* Future generation computer systems, 2016. 56: p. 684-700.

[25] Ray, P.P., *A survey of IoT cloud platforms.* Future Computing and Informatics Journal, 2016. 1(1-2): p. 35-46.

[26] Kantarci, B. and H.T. Mouftah. *Mobility-aware trustworthy crowdsourcing in cloud-centric Internet of Things*. in *2014 IEEE Symposium on Computers and Communications (ISCC)*. 2014. IEEE.

[27] Kantarci, B. and H.T. Mouftah, *Trustworthy sensing for public safety in cloud-centric internet of things.* IEEE Internet of Things Journal, 2014. 1(4): p. 360-368.

[28] Podnar Zarko, I., A. Antonic, and K. Pripužic. *Publish/subscribe middleware for energy-efficient mobile crowdsensing*. in *Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication*. 2013. ACM.

[29] Antonic, A., et al. *A mobile crowdsensing ecosystem enabled by a cloud-based publish/subscribe middleware*. in *2014 International Conference on Future Internet of Things and Cloud*. 2014. IEEE.

[30] Shah, S.T.U., et al., *Cloud-Assisted IoT-Based Smart Respiratory Monitoring System for Asthma Patients*, in *Applications of Intelligent Technologies in Healthcare*. 2019, Springer. p. 77-86.

[31] de Macedo, D.D.J., et al., *Toward an efficient healthcare CloudIoT architecture by using a game theory approach.* Concurrent Engineering, 2019: p. 1063293X19844548.

[32] Darwish, A., et al., *The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems.* Journal of Ambient Intelligence and Humanized Computing, 2019. 10(10): p. 4151-4166.

[33] Madhu, B., et al., *IoT Based Home Automation System over Cloud.* 2019.

[34] Yassine, A., et al., *IoT big data analytics for smart homes with fog and cloud computing.* Future Generation Computer Systems, 2019. 91: p. 563-573.

[35] Jaimunk, J. *Privacy-preserving cloud-IoT architecture*. in *Proceedings of the 6th International Conference on Mobile Software Engineering and Systems*. 2019. IEEE Press.

[36] Singh, A., U. Sinha, and D.K. Sharma, *Cloud-Based IoT Architecture in Green Buildings*, in *Green Building Management and Smart Automation*. 2020, IGI Global. p. 164-183.

[37] Araujo, V., et al., *Performance evaluation of FIWARE: A cloud-based IoT platform for smart cities.* Journal of Parallel and Distributed Computing, 2019.

[38] Kanchi, R.R., V.P. Sreeramula, and D.V. Palle. *Implementation of Smart Agriculture using CloudIoT and its Geotagging on Android Platform*. in *International Conference on Intelligent Computing and Communication Technologies*. 2019. Springer.

[39] Malik, A. and H. Om, *Cloud computing and internet of things integration: Architecture, applications, issues, and challenges*, in *Sustainable Cloud and Energy Services*. 2018, Springer. p. 1-24.

[40] Zhou, W., et al. *Discovering and understanding the security hazards in the interactions between IoT devices, mobile apps, and clouds on smart home platforms*. in *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 2019.

[41] Ahmed, A., et al., *Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review.* Multimedia Tools and Applications, 2018. 77(17): p. 21947-21965.

[42] Grozev, N. and R. Buyya, *Inter‐Cloud architectures and application brokering: taxonomy and survey.* Software: Practice and Experience, 2014. 44(3): p. 369-390.

[43] Moussa, A.N., et al. *A Consumer-Oriented Cloud Forensic Process Model*. in *2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC)*. 2019. IEEE.

[44] Rao, B.P., et al. *Cloud computing for Internet of Things & sensing based applications*. in *2012 Sixth International Conference on Sensing Technology (ICST)*. 2012. IEEE.

[45] Moussa, A.N., N. Ithnin, and A. Zainal, *CFaaS: bilaterally agreed evidence collection.* Journal of Cloud Computing, 2018. 7(1): p. 1.

[46] Dobre, C. and F. Xhafa, *Intelligent services for big data science.* Future Generation Computer Systems, 2014. 37: p. 267-281.

[47] Moussa, A.N., N.B. Ithnin, and O.A. Miaikil. *Conceptual forensic readiness framework for infrastructure as a service consumers*. in *2014 IEEE Conference on Systems, Process and Control (ICSPC 2014)*. 2014. IEEE.

[48] Rebbah, M., D.E.H. Rebbah, and O. Smail. *Intrusion detection in Cloud Internet of Things environment*. in *2017 International Conference on Mathematics and Information Technology (ICMIT)*. 2017. IEEE.

[49] Han, Z., et al., *A software defined network-based security assessment framework for cloudIoT.* IEEE Internet of Things Journal, 2018. 5(3): p. 1424-1434.

[50] Guechi, F.A. and R. Maamri. *Secure Self-Destruction of Shared Data in Multi-CloudIoT*. in *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. 2017. IEEE.

[51] Guechi, F.A. and R. Maamri. *Secure and Parallel Expressive Search over Encrypted Data with Access Control in Multi-CloudIoT*. in *2018 3rd Cloudification of the Internet of Things (CIoT)*. 2018. IEEE.

[52] Su, M., et al., *PRTA: A Proxy Re-encryption based Trusted Authorization scheme for nodes on CloudIoT.* Information Sciences, 2019.

[53] Jin, B.-W., J.-O. Park, and H.-J. Mun, *A design of secure communication protocol using RLWE-based homomorphic encryption in IoT convergence cloud environment.* Wireless Personal Communications, 2019. 105(2): p. 599-618.

[54] Mo, Y., *A Data Security Storage Method for IoT Under Hadoop Cloud Computing Platform.* International Journal of Wireless Information Networks, 2019: p. 1-6.

[55] Sharma, G. and S. Kalra, *Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications.* Journal of Ambient Intelligence and Humanized Computing, 2019: p. 1-24.

[56] Li, X., et al., *Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach.* IEEE Access, 2019. 7: p. 9368-9383.

[57] Choi, C. and J. Choi, *Ontology-Based Security Context Reasoning for Power IoT-Cloud Security Service.* IEEE Access, 2019. 7: p. 110510-110517.

[58] Arabo, A. *Privacy-aware IoT cloud survivability for future connected home ecosystem*. in *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*. 2014. IEEE.

[59] Massonet, P., et al. *Security in lightweight network function virtualisation for federated cloud and IoT*. in *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. 2017. IEEE.

[60] Mahmud, M., et al., *A brain-inspired trust management model to assure security in a cloud based IoT framework for neuroscience applications.* Cognitive Computation, 2018. 10(5): p. 864-873.

[61] Gupta, P.K., B.T. Maharaj, and R. Malekian, *A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres.* Multimedia Tools and Applications, 2017. 76(18): p. 18489-18512.

[62] Sharma, G. and S. Kalra, *A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services.* Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2019. 43(1): p. 619-636.

[63] Park, J., H. Kwon, and N. Kang, *IoT–Cloud collaboration to establish a secure connection for lightweight devices.* Wireless Networks, 2017. 23(3): p. 681-692.

[64] Elhabob, R., et al., *Identity-based encryption with authorized equivalence test for cloud-assisted IoT.* Cluster Computing, 2019: p. 1-17.