Integration of the Internet of Things and Cloud:

Security Challenges and Solutions – A Review

Chellammal Surianarayanan, Centre for Distance and Online Education, Bharathidasan University, India*

Pethuru Raj Chelliah, Reliance Jio Pvt. Ltd., India

https://orcid.org/0000-0001-5220-0408

ABSTRACT

The integration of IoT and cloud poses increased security challenges. Implementing security mechanisms in IoT systems is challenging due to the availability of limited resources, large number of devices, heterogeneity of devices, generation of bulk data, etc. Likewise, cloud resources are also vulnerable to security issues due to virtualization, insider threats, data loss, data breaches, insecure APIs, etc. Security is of major concern with the integration of IoT and cloud. The primary objective of this review is to highlight the security issues associated with an IoT system and cloud system and with the integration of the two, as well as to highlight solutions in each case. The secondary objective is to describe popular IoT-cloud platforms and also to highlight how such platforms facilitate secure integration. Ultimately a highlight on a shared responsibility model of implementing security is emphasized as both IoT users and cloud service providers have to cooperatively share the responsibility to deploy secure cloud-based IoT applications.

KEYWORDS

Cloud Security, IoT-Cloud Platforms, IoT-Cloud Security, IoT Security

INTEGRATION OF THE INTERNET OF THINGS AND CLOUD: SECURITY CHALLENGES AND SOLUTIONS: A REVIEW

The Internet of Things (IoT) sensors purposefully interact with other connected entities in the real world to acquire different operational parameters and share the data to other devices and systems over the Internet or any other communication network without human intervention (Mercado Herrera et al., 2023). The advancement in hardware and wireless communication technologies promotes the usage of IoT devices across various domains. In 2025, the number of IoT devices in the world will be approximately 75.44 billion (Alam, 2018). Artificial intelligence (AI) makes the IoT networks intelligent and increases the scope of IoT connectivity and vast data streams (Khanam et al., 2022). The rapid growth of IoT sensors and the corresponding generation of a large volume of data are obviously in need of huge resources for storage and processing (Qabil et al., 2019). There are several popular

DOI: 10.4018/IJCAC.325624

*Corresponding Author

approaches like on-premises private clouds and edge device clouds for data capture, storage, analysis, and visualization. But with the public cloud environment (off-premises, on-demand, and online) emerging as the most optimized and affordable option for large-scale data storage and processing, IoT data gets transmitted over the Internet to faraway cloud centers. There are automated tools for data storage, analysis, management, observability, and maintenance in the public cloud environment.

With its rapid and flexible resource provisioning at low cost (Truong & Dustdar, 2015) cloud can fulfill the major deficiencies of IoT, namely limited storage, low computing power, and deficient processing capabilities (Atlam et al., 2017; Botta et al., 2016). Cloud can provide the required scalability to an application while allowing the provisioning of resources to instantly scale up or down according to the demands of the applications (Righi et al., 2020). Machine learning tools and platforms that are available in public cloud make descriptive, predictive, prescriptive, and adaptive analytics easier (Adi et al., 2020). Rough set theory can efficiently select optimized cloud services for different tasks, namely inductive reasoning, automatic classification, pattern recognition, learning algorithms, and data reduction (Tiwari & Garg, 2022). Cloud provides monitoring and management of remote IoT sensors (Lineswala & Swali, 2020) in a centralized manner along with a robust Identity Access Management (IAM). Also, it offers services to store the security credentials of IoT devices.

Already IoT has revolutionized the way that different industries like healthcare, manufacturing, agriculture, oil and energy, transportation, and logistics are enhancing their processes by using IoT technology. In addition, cloud computing assists the IoT systems by providing adequate resources and ensures business continuity. Ultimately, the integration of IoT and cloud has led to the development of various useful applications like smart grid automation, smart energy, smart city, transportation and logistics, manufacturing, healthcare, agriculture (Alam, 2021; Dahiya et al., 2022; Guida et al., 2021; Haghnegahdar et al., 2022; Khattab et al., 2016; Xu et al., 2023).

In short, the integration of IoT and cloud provides the following benefits:

1. The IoT devices can access hardware and software services from cloud from any remote location.
2. Cloud enables centralized device registration, configuration, and management.
3. The scalability of cloud-based IoT applications is very high.
4. Cloud provides secure storage facility and life cycle management for IoT data.
5. Cloud can serve as a platform for developing complex applications with better use of online data.
6. Cloud facilitates large scale data analysis using machine learning algorithms.
7. Could ensures regular updates of software, platforms, and firmware which protect the IoT applications against known vulnerabilities.
8. Cloud provides scalable, reliable, and adaptable services and solutions which certainly lead to enhanced performance of the real-life applications.

Despite the above benefits, the integration of IoT and cloud is implicitly associated with two limitations, namely latency and the need for high network bandwidth for the transfer of data from IoT to cloud. Due to the network latency, real-time analysis of IoT data is not possible with faraway cloud environments. Real-time analytics are performed using edge computing at the point of data acquisition itself. But irrespective of the situations in which real-time analysis is required, for any application, the relevant and necessary data must be archived for deeper analysis, decision making, data warehousing, business continuity, and business intelligence purposes. Since data is one of the primary assets of corporations it cannot be ignored without extracting hidden knowledge from it. This illustrates the frequent need for cloud computing resources by IoT applications.

Apart from the above benefits, the amalgamation of IoT and cloud is associated with increased security issues (Almolhis et al., 2020). Security becomes the major concern when an IoT system is integrated with cloud due to reasons like improper device updates, lack of robust protocols, lack of device monitoring, not updating the default passwords and unconscious use (Tawalbeh et al., 2020). Also, the built-in authentication mechanism of IoT devices is not reliable due to weak, guessable, and hardcoded passwords (Sivaselvan et al., 2022). Conventional security solutions are not directly applicable to cloud-based systems, and deep learning-based methods can address industrial security issues in the cloud (Ahmad et al., 2022). In Chen et al. (2021), the authors have elaborated the insecurity aspects of IoT-cloud integration with ten case studies, and they suggested potential security risk mitigation methods to protect IoT cloud systems. Shakya's (2022) review has investigated different security issues that occur in the integration of IoT and cloud and has provided potential solutions, with special emphasis being placed on light-weight cryptography for improved data security.

In the context of IoT and cloud integration, the primary benefit of cloud must be perceived clearly. Cloud is available as a well-matured platform that can readily establish a centralized device management facility, which is the very first need of any IoT system. If device registration, control, and management can be performed effectively, then the device integrity would be automatically satisfied. Thus like any other use, an IoT system can get all other monitoring, security, and management services along with device connectivity. Another important aspect regarding the integration of IoT and cloud is that there are various commercially available IoT cloud platforms provided by different service providers for consumption by IoT systems. An IoT cloud platform serves as a gateway between the IoT system and cloud. Here, an IoT system, as a cloud user can connect via the IoT cloud platform and avail the services of cloud easily. These platforms are built on the top of cloud and have features including centralized device connectivity, device configuration, device management, network management, data acquisition, data analysis, visualization, application enablement, integration, and storage. These platforms help in securely and efficiently leveraging the services and resources of cloud to IoT systems.

As far as IoT-cloud platforms are concerned, developing one's own platform for integration is time consuming. Technical challenges are involved. Building an integration platform is associated with more cost and human effort. Beyond all, any business requires a proof of validation before its full set of implementations. The commercially available IoT-cloud platforms are serving as proven solutions for building cloud-based IoT systems. As discussed in Ray (2016), the IoT-cloud integration platforms help in resolving various issues, namely device management, system management, heterogeneity management, data management, data analytics, deployment, monitoring, visualization, and research. Further, these platforms facilitate the speedy and simplified development of IoT ecosystems (Fortino et al., 2022).

In this work, a review has been done with the following two research questions:

1. How can the security challenges that arise during the integration of an IoT system and cloud be addressed by cloud?
2. How can IoT-cloud integration platforms facilitate IoT-cloud integration?

Through the findings, the review illustrates how cloud can extend its device connectivity, management, and other services via the integration platforms and ultimately achieve the basic security requirements, namely integrity, availability, confidentiality, and privacy, across different layers of any cloud-based IoT system.

The contributions of the review include:

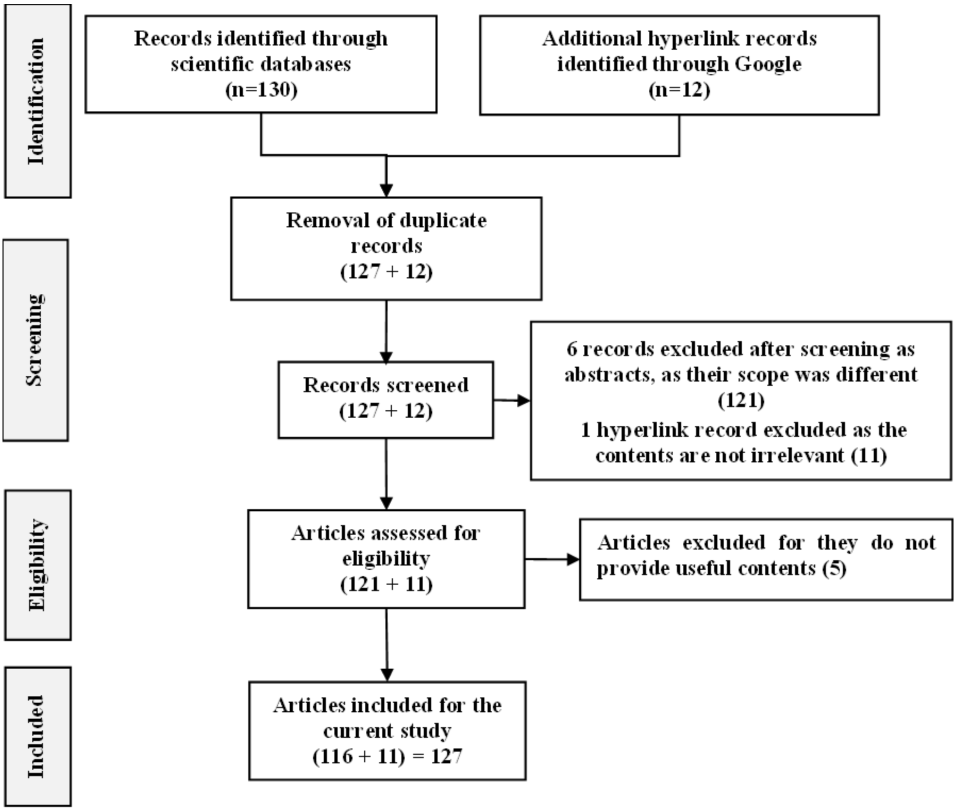
- A brief overview of security challenges in cloud and their resolving methods.
- A short description of security aspects of IoT.
- A brief account of security issues that arise during the integration of IoT and cloud and their solutions.
- A description of the layered model of cloud-based IoT application.
- An overview of top commercial IoT-cloud platforms, namely Amazon Web Services (AWS) IoT, Microsoft Azure IoT, Cisco IoT Cloud Connect, IBM Watson IoT, and Google Cloud IoT Platform.

- An illustration of the way these platforms can ensure the fulfillment of basic security requirements (namely authentication, authorization, confidentiality, integrity, availability, and privacy) in an IoT system.
- A description of the review method and findings of the review along with a note on limitations and future research directions.

REVIEW METHOD

Publications related to the objective of the review have been collected from different data sources, namely Web of Science, Scopus, Springer, and IEEE, and as well as from Google using keyword searching. Different keywords, like "security issues in IoT", "security issues in cloud", "security challenges cloud based IoT", and "security issues in the integration of IoT and cloud", have been used. The title and abstract of the retrieved publications have been carefully analyzed for additional keywords such as "security challenges in SaaS", "security issues in PaaS", "security challenges in IaaS", "IoT Cloud platforms", and "security challenges in the cloud based IoT". The search resulted in 130 records from scientific databases and 12 hyperlink records from Google. At first duplicate scientific records (3) have been eliminated. The remaining records have been manually scanned for abstracts. Publications which are not useful (11 scientific records and 1 hyperlink record) for the current objective were eliminated. Ultimately a collection of 127 representative records (116 scientific records and 11 hyperlink records) has been included for the study. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) flow diagram of the review method is shown in Figure 1.

Figure 1. PRISMA flow diagram of the proposed review


Identification
Records identified through scientific databases (n=130)
Additional hyperlink records identified through Google (n=12)
Screening
Removal of duplicate records (127 + 12)
Records screened (127 + 12)
6 records excluded after screening as abstracts, as their scope was different (121)
1 hyperlink record excluded as the contents are not irrelevant (11)
Eligibility
Articles assessed for eligibility (121 + 11)
Articles excluded for they do not provide useful contents (5)
Included
Articles included for the current study (116 + 11) = 127

The representative publications have been categorized according to the research questions and are given in Table 1.

FINDINGS OF THE REVIEW

The representative publications have been carefully analyzed towards answering the proposed research questions. The following are the findings of the review, and they are discussed in a hierarchical manner in the subsequent sections:

- A brief overview of cloud security issues and their solution approaches.
- A description of IoT security issues and their solving methods.
- A narration on the security challenges in the integration of IoT and cloud along with mitigation strategies provided by cloud.
- A highlight about the need for IoT-cloud platforms for easy and secure integration.
- An overview of popular IoT-cloud platforms.
- An illustration of the fulfillment of the basic security requirements in a cloud-based IoT application.
- A discussion of limitations and future research directions.

OVERVIEW OF CLOUD SECURITY

With unique characteristics, namely on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell & Grance, 2011), cloud computing offers a wide range of computing resources to its consumers. The resources are provided through different service classes, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), over different deployment models, namely public, private, and hybrid (Quilachamin et al., 2018). Here, the control that a consumer could get over different computing resources that s/he avails is based on the concerned service class. In the case of IaaS, though the service providers have more control over the infrastructure (computing, storage, and network resources), the consumers are also being given more control with respect to the operating systems and applications that they deploy in the infrastructure. In the case of PaaS, only service providers have maximum control over both the infrastructure as well as the platforms and other software offered by them. With SaaS, the

Table 1. Categorization of representative publications for the current study

S.No	Specific focus	Number of publications
1	The critical need for cloud for IoT applications	25
2	Overview of cloud security	13
3	Security issues and solution approaches in IaaS cloud	15
4	Security issues and solving methods in PaaS cloud	6
5	Security issues and solutions in SaaS cloud	6
6	IoT security	30
7	Security issues at the integration of IoT and cloud and their solutions	26
8	IoT-cloud platforms	5
9	Security requirements of IoT applications	1
	Total	127

consumers have almost no control over the software applications they consume. Also, cloud security follows a shared responsibility model where both service provider and consumer are responsible for implementing security mechanisms based on the service class (Al-Anzi et al., 2014; Saini et al., 2022).

In Hashizume et al. (2013), the authors have related various vulnerabilities in cloud to their corresponding threats. Also, the authors have given some countermeasures for different threats. In the study of Vurukonda and Thirumala Rao (2016), the authors have identified security issues, such as data breach, data theft, and unavailability of data, related to cloud data storage. In Khan et al. (2021), the authors have identified 15 security challenges, namely data secrecy issues, geographical data location issues, unauthorized data access issues, lack of control, lack of data management, network-level issues, data integrity issues, data recovery issues, lack of trust, data sharing issues, data availability, asset issues, legal amenabilities, lack of quality issues, and lack of consistency. These issues are related to big data in cloud computing. Using the fuzzy-Technique for Order Preference by Similarities to Ideal Solution (TOPSIS) method, the authors found the data secrecy issue to be the most prominent security challenge. In Dong et al. (2019), the authors presented the state-of-the-art Distributed Denial of Service (DDoS) attacks in Software Defined Cloud (SDN). In Rajasekaran and Ranganathan (2021), the authors discussed various security issues from a federated cloud perspective. In Sabir (2018), the authors reviewed various security aspects and key factors which affect cloud security and provided solution approaches. In Butt et al. (2023), security threats, difficulties, strategies, and solutions related to the cloud computing environment were discussed. The article by Alhijawi et al. (2022) reviews and classifies the research efforts on SDN and DoS. In Hassan and Thayananthan (2021), the applications of machine learning for securing SDN were discussed.

Security Issues in IaaS and Their Solving Methods

In the IaaS model, cloud consumers have more responsibility in implementing security measures as the service providers have control over only the physical infrastructure. The available physical resources are virtualized and shared by many consumers. Security issues related to virtualization and multi-tenancy become important. Here, Virtual Machine (VM) needs to be protected against attacks due to virtualization. In addition, the vulnerabilities in the underlying hypervisor must be given more importance. An attacker who gains access to hypervisor can even access the underlying hardware easily. Similarly, DoS attacks against any VM are likely to affect the other VMs that share the same physical machine as the targeted VM. Software used to implement virtualization may contain bugs. VM escape is a serious attack where an attacker intentionally runs code to break a VM and interacts with the host operating system. The VM escape gives an attacker unlimited control over the host system because the attacker can access all the VMs in the host. Also, if VMs are not monitored and managed properly, they may be left simply idle or without the required security patch or update. Such VMs become vulnerable to more attacks. VMs are affected by malware attacks also. An attacker who gains access to the VM management console can copy sensitive data from the VM to outside. Network virtualization allows multiple cloud users to have their virtual networks on a shared physical network infrastructure. When the virtual networks are not isolated completely, an attacker can exploit the vulnerability and access the other virtual networks as well (Alharbi & Portmann, 2019; Duan et al., 2016; Li & Chen, 2015). Misconfiguration of computing instances by cloud consumers creates security vulnerabilities, and it is one of the major security concerns in cloud (Alghofaili et al., 2021; Nobles, 2022). Virtualization and hypervisor related security attacks in IaaS along with their solution approaches are given in Table 2.

Security Issues in PaaS and Their Solving Methods

In the PaaS service class, the service providers provide infrastructure (i.e., servers, storage, and networking resources) as well as the programming and execution environment required for design, development, testing, and deployment of applications. The PaaS service class is expected to provide high scalability, on-demand provisioning, automatic deployment of applications, high availability,

Table 2. Virtualization and hypervisor related attacks in IaaS and their solution approaches

Security attack	Solution approaches
VM theft – this refers to the stealing of a VM (essentially a file) over a network in order to use it elsewhere	Strong access control Secure hypervisor configuration Encryption of VM An access control model developed by D. Bell and J. LaPadula (Wu et al., 2017)
VM sprawl – VM remains out of date for security updates	Regularly monitoring VMs to check whether any VM is left idle or remains without a software update Optimizing the resources of VM VM management tool Encryption of VM image
VM escape – an attacker gains unauthorized access to a VM and thereby to other VMs running on the same physical hardware (Abusaimeh, 2020)	An access control model developed by D. Bell and J. LaPadula (Wu et al., 2017) Penetration test for virtualization environment (Tank et al., 2019) Hypervisor hardening (Rakotondravony et al., 2017) Interposing the interactions in-between the guest VMs and hypervisor through clearly defined entry and exit points by using CloudVisor (Szefer & Lee, 2012)
Hyperjacking – an attacker takes control over the hypervisor and thereby creates attacks	Protecting hypervisor integrity and reducing attack surface (Vasudevan et al., 2013) (Szefer et al., 2011) Maintaining the integrity of control flow in hypervisors using HyperSafe (Wang, 2010) Protection of code of hypervisor from malicious activity
Hypercall attack – an attacker exploits the weakness of hypercall interface and requests specific services like memory allocation, device access, or process scheduling from the hypervisor	Up to date software update for hypervisor and continuous monitoring
Hypervisor failure – hypervisor undergoes failure or is not functioning properly	Regular update of hypervisor software and monitoring using tools
Guest hopping attack/VM hopping attack – an attacker on one VM hops to another VM on the same host	VM hopping defense is mainly solved by building healthier hypervisors (lightweight hypervisors) and designing more robust access control policies (Dong & Lei, 2019)
Cross VM side channel attack – if VMs are co-resident on the same hardware, the malicious VM can observe the hardware behavior of the target VM with an intention to steal passwords (Narayana & Jayashree, 2021)	Implementation of different mechanisms at CPU level, like indirect branch prediction barriers and flushing the L1 data cache Implementation separate cache memory for CPUs

high reliability, multi-OS, multi-language support, etc. (Yasrab, 2018). In PaaS multiple tenants deploy their applications on virtual environments which share the same physical resources. So, it becomes crucial to ensure that an application is getting executed in an isolated environment (Hussain et al., 2017). In the PaaS cloud, the consumers are given permission to access several platforms, tools, and software along with their concerned application and data. Attackers can exploit the vulnerabilities of applications and software tools and gain access to various resources. The major security issues in the PaaS cloud along with their solving methods are given in Table 3.

Applications should be equipped with real-time automatic monitoring for detecting and blocking unauthorized access. User accounts should be properly managed. Only authorized users should be given permission to access their concerned resources up to the level of privileges they have. Also, the administrators should ensure that the users are given only the necessary privileges. Since PaaS supports a wide range of software including proprietary, open-source, and third-party tools, flaws that exist in any of these components lead to security vulnerabilities. Attack simulation and threat

Table 3. Major security issues in PaaS cloud and their solution approaches

Security attacks	Solution approaches
As discussed in Tank et al. (2019), there are three major causes for security issues in PaaS Heterogeneity in hardware and software cause flaws as the security setting for different resources would be different Host in a multi-tenant environment becomes vulnerable to security attack (vulnerable host) The resource of objects in a host also tends to be vulnerable (vulnerable object)	Trusted Computing Base (TCB) is a promising method to address security flaws that may arise due to heterogeneity issues and a vulnerable host (Hussain et al., 2017) Sensitive data associated with different resources can be kept safe using encryption
Lack of monitoring ability on a heterogeneous workload system and difficulty in maintaining consistent security across multiple platforms or tools is a major issue in PaaS (Finsliq Blog, n.d.). In the case of a multi-cloud environment, the monitoring becomes still more complex (Raj Chelliah & Surianarayanan, 2021). It means that the host or VM or container on which the workload would be deployed will be varying with respect to time. This makes the monitoring with fixed/constant network intrusion detection more complex (TechTarget, n.d.)	By using cloud workload protection platforms (CWPPs), unified management can be brought in which the security related controls would be packed along with workloads themselves
If an attacker gains access to resources of PaaS with administrative privileges due to poor access control, the attacker can access not only the instances of the application but also the servers in the instances have been deployed (FutureLearn, n.d.).	By using robust access control mechanisms

monitoring must be done as a routine activity. Logging of user activities helps in analyzing whether the users are working only according to their granted privileges. Data must be communicated via secure protocols. Also, the data must be validated thoroughly to ensure that clean data is being communicated. Multi-factor authentication needs to be implemented along with strong security policy. Privacy-aware authentication using proxy certificates, indicating access control policies agreed upon by service providers and users, must be used. As mentioned earlier, implementing security is a shared responsibility of cloud service providers and cloud consumers; the consumers may use their own security mechanisms to protect their applications. The PaaS cloud offers various security related services such as the following:

1. **Security broker for cloud access (CASB):** These security brokers are cloud security gateways used to establish various countermeasures, like monitoring unauthorized access, implementing security policies, controlling access to resources according to users' privileges, and auditing cloud configurations.
2. **Platforms for securing cloud workloads:** Cloud workload security platforms continuously monitor the workload instances and defend against malware. Also, the platforms help in security management across different PaaS providers.
3. **Control of cloud protection posture:** A security posture manager audits the cloud environment on a regular basis for security and offers manual or automated remediation strategies to handle enforcement related issues.

Security Issues in SaaS and Their Solution Approaches

In the SaaS model, the consumers must ensure security for their data. It is the primary responsibility of the user to implement strong authentication and authorization mechanisms to ensure the data security. The data is at greater risk for its leakage or deletion due to unauthorized access. Accessing SaaS services without explicit security is the main driver for shadow IT (ISACA, 2022). In addition, consumers of SaaS are not or less aware of the security posture of the provider. Also, the providers may include third-party vendors in their services and operations. So, it becomes crucial to assess and evaluate the security aspects of third-party vendors. There are situations where users may not be informed about the infrastructure and application-level security event logs to the SaaS customers (for example, password-replay attack of a customer may not be informed to the customer at right time which may lead to data breach). Also, the consumers may be unaware of the shared security model as the SaaS providers may not reveal the shared responsibility matrix or Complementary User Entity Controls (CUEC). In addition to the above, SaaS providers have the risks while disclosing security program details to consumers as disclosing too much details (about security policies, procedures, standards, business continuity plans, controls, and risks) help attackers in compromising SaaS environment. Disclosing too little information makes the legitimate users unaware of the security posture of the provider. Further, customization of SaaS services is really challenging, as the flaws in configuration may create security vulnerabilities. Security issues in SaaS along with their solution approaches are given in Table 4.

IoT SECURITY

IoT devices typically have limited computing resources which prohibit the implementation of strong security solutions. The following research works have handled security aspects of IoT. In Abdur Razzaq et al. (2017), the authors emphasized that the usage of IoT devices keeps on increasing, whereas the majority of the IoT devices and applications are not being designed to handle security and privacy issues. Also, the authors have given an overview about the security requirements in IoT along with a description about various security attacks in a categorized manner. In Yang et al. (2017), the authors performed a survey with four segments; the first segment deals with the limitations of IoT

Table 4. Security issues in SaaS and their solution approaches

Security attacks	Solution approaches
Poor IAM and lack of user control are major two security issues in SaaS (Humayun et al., 2022). Due to lack of control, users are likely to misconfigure the application and security related settings. This may result in the exposure of data to various cyber-attacks such as malware, ransomware, etc.	Multifactor authentication robust access control mechanisms Protection against malicious software Solutions such as given in Subba Rao et al. (2023)
Insecure APIs may lack proper role-based access control, and this leads to vulnerabilities. Most of the SaaS providers are likely to simply permit users having Internet (without explicit approval from information security and legal teams) to access and consume their SaaS applications (Asghar & Amjad, 2018; Islam et al., 2016); and this may put the organization at security risk.	Strong authentication and authorization for access APIs Testing APIs for their security Logging and auditing of API activities such as API access, API actions, and authentication failures etc. API traffic monitoring
Service Level Agreement (SLA) issues (Bernsmed et al., 2011) – Similar to other non-functional attributes, SLA should include security related parameters such as data encryption, access controls, vulnerability management, etc. Issues are likely to occur if the providers do not deliver the service up to expected level of security.	Service users should be aware of the expected level of security from the providers Enforcing SLA compliance makes the service providers implement the agreed upon security related mechanisms
Data security issues like incomplete data-deletion (data remanence), data breach, data loss, data backup, and recovery related issues	Using encryption for data-in-transit Secure storage Life cycle management of data Strong authentication and robust access control
Logical data storage segregation due to multi-tenancy – users are unaware of their data location. This can raise concerns about compliance with data protection regulations	Data protection regulations must be transparently stated in SLA

devices, the second segment presents the classification of IoT attacks, the third segment describes architectures for authentication and access control, and the fourth segment analyzes security issues in different layers. In Imran et al. (2021), the authors have examined the past, present, and future of the IoT security issues by analyzing existing IoT security vulnerabilities. With their review, the authors have found that in the past, data security, privacy, integrity, and confidentiality were the most discussed issues. Also, they found that, in the present and future, along with the four mentioned issues, authenticity has also been included. In Hassija et al. (2019), a detailed review of the security related challenges, sources of threats along with the role of different technologies like blockchain, edge computing, fog computing and machine learning, in enhancing the security of IoT applications, have been discussed. The integration of a wide range of smart devices into the standard Internet introduces several security challenges as the internet technologies and protocols were not designed for IoT (Krishna & Gnanasekaran, 2017). Also, in the above paper, the authors have discussed IoT-layered architecture, security attacks in different layers, solution approaches, and their limitations. In the review paper by Azrour et al. (2021), the authors have identified the key security issues that arise in the IoT environment and have described various IoT authentication techniques towards enhancing IoT security. In Mohanty et al. (2021), the authors have handled IoT security with two perspectives; one is with respect to different layers of IoT architecture, and the other is with respect to protocols. Further, the authors have developed security mechanisms for various protocols. In another study by Leloglu (2017), the author has discussed security requirements and challenges that are common to IoT implementations and has provided solutions for each layer of IoT architecture. In contrast to the above survey works, in the review by Abed and Anupam (2022), the authors have described major attributes related to IoT security along with potential solutions based on AI.

The most important security issues in the IoT, as described in (Peerbits. 2023):

1. An IoT device may trust the other devices in the local network and share the data to other devices in the same network, as a single device may not be able to provide extensive functionality (Trnka & Cerny, 2017).
2. In the IoT environment, devices of the same model or design are delivered with the same default passwords. Frequently, those passwords are not being updated by users. The use of default passwords is dangerous and creates vulnerabilities (Knapp, 2011).
3. IoT devices like smart TV, phones, cameras, etc. are basically powered by processors that run on either Android or Unix operating systems. These operating systems use Android Debug Bridge (ADB) for managing communication between devices. However, there are several smart TV manufactures that sell these TVs with an uncertified version of Android along with the ADB ports left open (QuickHeal, 2019). This results in security vulnerabilities.
4. In general, the software released for IoT devices will undergo vulnerability research, and if any vulnerability is found, then the vendors of the software will be notified. They release countermeasures as patches. When a device is not updated for the patch, it becomes vulnerable to security attacks (Prakash et al., 2022).
5. When an IoT device communicates data in the plain text form, it creates security issues such as eavesdropping.
6. A wormhole attack is an internal attack which is hard to identify as attackers simply listen to the activities of the network without altering it (Nitiynandan & Kamalakkannan, 2022).
7. The use of general-purpose computers as devices in an IoT environment also creates security issues as they permit the installation of any software and an attacker may misuse this feature. By limiting the functionality of the device, the possibilities to abuse the device can be reduced. A trusted execution environment can be created as in Apple iPhone to totally restrict the code that runs on the IoT devices.

8. Consumer devices typically store sensitive information which can be accessed by attackers, and this creates data privacy issues. Insufficient physical security of IoT devices also brings security vulnerabilities.

Security issues in different layers of an IoT application along with their solution approaches are given in Table 5.

SECURITY CHALLENGES IN THE INTEGRATION OF IOT AND CLOUD

Security becomes a major concern in the integration of IoT and cloud due to the following reasons:

1. **Increased attack surface due to large scale deployment of IoT sensors:** Very often, an IoT system consists of numerous sensors and gateways which make the system more vulnerable to security breaches. As discussed in Al-Garadi et al. (2020) intruders also may try to get unauthorized access as mostly the devices are operating in an unattended environment and the attack surface has been increased due to interdependent and interconnected environments.
2. **Complex security management due to device heterogeneity:** In general, IoT systems contain devices manufactured by different vendors. The hardware, software, protocols, and operating systems of different devices are heterogeneous. New security issues arise due to the heterogeneity of IoT applications and devices (Choudhary, 2018). Each type of device has its own security vulnerabilities. When there is a diversity, ensuring a security patch update for each type of device itself becomes difficult.
3. **Difficulty in the implementation of consistent security:** In addition, each type of device has its own security features. So, implementing consistent security across the heterogeneous devices also becomes tedious.
4. **Increased security vulnerabilities due to lack of interoperability:** The communication protocols and standards are different among devices, which leads to interoperability issues. The incompatibility and interoperability issues increase the attack surface of the system (Sadhu et al., 2022).
5. **Lack of control and visibility:** In general, organizations depend on third-party vendors for devices and tools. Those vendors provide only limited control over the security configurations. In addition, users of devices may not have the full visibility due to their ignorance about the internal behavior of the devices. Insufficient access control, flaw of default user credentials, and elevated permissions to users help hackers to gain unauthorized access, and close to 48% of IoT users are unaware that their devices could be used to conduct attacks (Neshenko et al., 2019).
6. **Need for strong authentication and authorization control:** When an IoT system is integrated with cloud, authenticating, and authorizing the devices as well as users. Authentication and authorization are the first lines of defense against unwanted actions (Putra et al., 2020).
7. **Privacy issues:** When data is stored in cloud, data privacy cannot be ensured as data is stored in different geographical locations where the privacy laws are different, and it is very likely that the data may be exposed to foreign entities. So, data storage must be carefully planned in sectors like healthcare where sensitive data is bulk and fragmented across insurance, pharmacy, clinical labs, etc. (Wassan et al., 2022).
8. **Security and privacy issues:** Associated with Medical IoT systems and the need for implementing suitable countermeasures to enhance the resiliency of these systems to cyber attacks have been discussed in Gaurav et al. (2022).
9. **Identity-based privacy protection algorithm:** For cloud computing is proposed in Li et al. (2023).
10. **Data security issues:** Data breach and data loss are likely to happen in cloud due to security vulnerabilities and insider threats. In addition, data remanence also leads to security attacks.

Table 5. Security issues and solution approaches in IoT environment

Layer	Security attack	Solution approaches
Perception Layer	Node capture attack – A hacker may tamper with an IoT device physically or electronically to extract secret key information and data and to impersonate a legitimate node, inject messages, or attempt passive attacks	Lightweight Extensible Authentication Protocol (LEAP) protocol enhances the authentication and access control mechanisms. This can reduce the occurrences of node capture (Keerthika & Shanmugapriya, 2021).
	Compromised node attack – A legitimate node would be controlled by an attacker for an adversary action	A behavior-based algorithm compares the behavior of neighboring nodes with one another and identifies the node with misbehavior (Xie et al., 2019)
	Replication node attack – In this attack a malicious node can use the ID and keys of a legitimate node	This can be resolved using a unique pair key method. In this method, for every pair of nodes in a network, a unique pair of keys would be generated using cryptographic methods. So, whenever a new node is joining the network, it must establish communication with other nodes of the network using a unique pair of keys. Here, every pair of nodes would have its own unique pair of keys, and this thus eliminates the replication node attack (Xie et al., 2019)
	RF jamming attack – In this attack, an attacker sends radio signals to disrupt the communication between the RFID reader and legitimate tags (Akhtar & Feng, 2022)	The use of frequency hopping or direct sequence spread spectrum makes the transmission to spread over a wider frequency band which makes it hard for the attacker to create jamming signal for interference Antijamming algorithms can be used to identify jam signals and to remove them for a reliable communication
	Tag cloning attack – In this attack, the identity related information from a legitimate tag are captured and used for a cloned tag	Floyd-Warshall Algorithm creates a graph representation of nodes in the IoT network which detects nodes that have the same identity information and detects the cloned tag from the differences in the short path distances (Huang et al., 2020)
	Spoofing attack – In this attack, a legitimate node is impersonated by using its Media Access Control (MAC) address, IP address, or Global Positioning System (GPS) data	Implementing software defined wireless networking (Mohammadnia & Ben Slimane, 2020)
Network layer	Replay attack – An attacker fraudulently delays or resends valid data or commands to a receiver to misdirect the receiver	Implementation of time synchronization-based methods and nonce value-based methods is difficult. So, an efficient mutual user authentication and secure-session-key-agreement-based method would be more useful to eliminate the replay attack (Feng et al., 2017)
	Sybil attack – In this attack a malicious node called Sybil node having multiple identities (which are obtained either by stealing or by creating fake IDs) attacks the integrity of an IoT network	Implementing unique and verifiable identities for each device prevents the creation of fake IDs By analyzing the behavior and resource usage patterns, Sybil attack can be detected and eliminated (Rajan et al., 2017)
	Sinkhole attack – In sinkhole attack, the entire traffic from a specific area is diverted by a compromised node to a sink. Here hoping that there exists some best route, the other nodes send the packets to sinkhole where the data will be compromised	Sinkhole Attacks can be handled by using secure routing protocols that authenticate the nodes and verify the path before forwarding the traffic The network traffic would be analyzed by calculating the number of Destination Oriented Directed Acyclic Graph Information Object (DIO) messages. The nodes for which the DIO exceeds the Upper Control Limit would be detected as sinkholes (Hachemi et al., 2020)
	Blackhole attack – Node compromised by a blackhole attack attracts the incoming traffic by advertising that the wrong path that it has, as the small route to destination and drops the data without forwarding (Ali et al., 2018)	Enhanced authentication to ensure only legitimate nodes can participate in the communication Intruder detection and monitoring
	Wormhole attack – Wormhole attack is an internal attack which listens to the network activities without changing them (Goyal & Dutta, 2018)	Ad hoc On-Demand Distance Vector typically results in shorter routes whereas in wormhole attack a tunnel is created between two distant nodes. Based on this difference, wormhole attack can be detected and eliminated (Goyal & Dutta, 2018)
	Man-in-the-middle attack – In this attack a malicious node is inserted between two legitimate nodes for different attacks	Mutual authentication between the nodes helps to ensure the verification of the nodes
	DoS attack – Requested service is not available to legitimate users	Regression modeling analyzes historical data and detects DoS from network traffic and resource utilization patterns (Nitiynandan & Kamalakkannan, 2022)
	Sniffing attack – This attack intercepts the traffic and tries to grab plain data	Encryption, secure protocols, and traffic monitoring prevent sniffing attacks (Ingham et al., 2020)

continued on following page

Table 5. Continued

Layer	Security attack	Solution approaches
Application layer	Code injection attack – Attacker inserts a malicious code in the application	Validation of inputs, secure code practices, regular security updates, testing the applications for vulnerabilities related to code injection
	Buffer overflow – An attacker can overwrite the memory of an IoT application	Input validation and bound checking Hardware assisted buffer overflow detection and elimination (Xu et al., 2018)
	Phishing attack – Email or message of higher-level authority would be used for attack	Strong authentication mechanism helps in eliminating phishing attack Email filtering and anti-phishing solutions can prevent phishing Phishing attacks can be addressed in a proactive manner by aggregating signatures of legitimate websites at the source (Nirmal et al., 2020)
	DoS attack – an attacker, as though a legitimate user, logs into the application and creates DoS	Message Queuing Telemetry Transport protocol, Advanced Message Queuing Protocol, and Constrained Application Protocol can be implemented with a rate limiting mechanism to limit the number of messages from a single source (Swamy et al., 2017)

Moreover, the following research explores different security issues in cloud-based IoT applications. The work of Deore et al. (2022) primarily focuses on the analysis of possible security threats for cloud-based IoT systems along with techniques of cryptographic solutions to address the identified challenges. In Stergiou et al. (2023), the authors have described security and management challenges of cloud computing while handling the big data exported from IoT. The authors discussed how cloud computing contributes to security and privacy related concepts during the integration of IoT-based big data. In Ahmad et al. (2022), a comprehensive survey on cloud-based IoT architectures, services, configurations, and security models has been done with a classification of cloud security concerns in IoT. The authors have classified the security concerns into four major categories: data, network and service, application, and people-related security issues. The research work by Bonkra and Dhiman (2021) explores various IoT cloud security challenges and how data on the cloud-IoT platform might be protected. In Mohiuddin and Almogren (2020) the authors performed a study to investigate the challenges and strategies adopted by cloud computing to facilitate a safe transition of IoT applications to the cloud. In Zhou et al. (2017), the authors introduced an architecture, unique security, and privacy requirements for the next generation mobile technologies on cloud-based IoT along with efficient privacy preserving authentication method.

Solution Approaches to the Security Issues in the Integration of the IoT and Cloud

As cloud has been serving as an infrastructure-backbone for various organizations over a decade, it has gone through a set of known security vulnerabilities which can be handled via the existing cloud security services. When an IoT system is integrated, the security mechanisms at device layer must be tightened with rigorous authentication and authorization measures. In Alizai et al. (2018), a light-weight, multi-factor authentication scheme has been described. In Zhou et al. (2019), one-hashing and XOR-based two-factor authentication has been presented. In Ahmed et al. (2021), special focus has been given to machine learning-based authentication and authorization.

Like any other user, an IoT system interacts with the cloud via gateway. Very often, the IoT system contains their devices scattered across different geographical locations, utmost care must be taken in maintaining the device integrity. Software-defined networks (SDNs) offer unique and attractive solutions to manage large scale IoT networks. SDN-IoT network collaboration can be established with enhanced security by transforming heterogeneous controllers into a homogeneous group of controllers as presented in Sood et al. (2020). In addition to the efficient device management, the availability of the IoT ecosystem must be ensured. Distributed DoS attacks can be addressed by obtaining probabilistic knowledge about whether a user is malicious or not by observing the network for a long time with Bayesian game theory-based solution as described in Dahiya and Gupta (2021).

Further, an intrusion prediction system which can predict botnet in Automated Guided Vehicles (AGV) has been presented in Shaikh et al. (2022).

The IoT devices must be continuously monitored for their proper behavior. There are solutions such as the one discussed in Cvitić et al. (2021), which classifies the IoT devices into different classes according to the network traffic generated by them and helps in the monitoring and management of large heterogeneous IoT environments. Different kinds of Intruder Detection Systems (IDS), like host-based IDS for monitoring devices and network-based IDS for monitoring the IoT network, should be included for the detection of potential intrusions and anomalies. Ensemble learning Catboost model with Bayesian optimization approach has been described for efficient detection of malicious activities and anomalies has been described in Nayak et al. (2022). Document Object Based cross-site scripting vulnerabilities in mobile cloud-based online social network can be alleviated by runtime Document Object Model (DOM) tree generator and nested context-aware sanitization-based framework (Gupta et al., 2017). Chaotic whale crow (CWC) optimization framework for secure data communication and routing based on selected trusted nodes which are identified through various direct, indirect, forwarding rate, integrity, and availability factors has been descried to resolve the security issues associated with IoT networks (Raj & Pani, 2022). In Li et al. (2019), a framework to enhance the security of the cloud-based IoT context through trustworthy cloud services has been presented. Also, an identity-based privacy protection algorithm for cloud computing is proposed in Li et al. (2023).

IoT devices are shipped with default password settings. These passwords should be updated (Russell et al., 2015). Firmware and software updates must be done securely (Bettayeb et al., 2019). Implementing new industry-wide standards and best practices help to resolve security in IoT (Karie et al., 2021). Further, implementation of security must be considered in the design stage itself. Security features such as secure firmware, strong authentication mechanism, and secure coding must be thought over during the design stage itself. Each device type must be configured correctly for its application and security setting. Any misconfiguration may lead to potential threats. The debugging ports which are used for testing the IoT devices and applications should be closed once the debugging is completed. Vendors of IoT tools and devices must explore the possibility of explicitly providing more control and visibility without compromising the security. Security penetration testing and vulnerability scanning should be done regularly to detect weaknesses in the IoT network and to take appropriate countermeasures. Logging all activities in an IoT network stores information about various activities, events, and interactions within the system, including user actions, device operations, network traffic, and security events. Log records help to identify security threats and malicious activity in an IoT environment. Security auditing evaluates the security practices and processes in order to assess their compliance with security standards and regulations. It also helps to detect weaknesses in security implementations. Security compliance testing must be performed as a routine task. It ensures that appropriate security measures have been taken to safeguard the assets

IOT CLOUD INTEGRATION PLATFORMS

The integration of IoT and cloud is preferred to meet the needs of many real-life applications, such as smart city, smart home, healthcare, agriculture, etc. The integration is simplified with the help of commercially available IoT-cloud integration platforms. The commercially available integration platforms are preferred to one's own platform to cloud due to the following reasons:

1. At first, one must validate the business case under study with the proposed integration platform to check whether the all the requirements of the problem in hand would be fulfilled by the platform.
2. Various technical challenges are associated with the development of an integration platform.
3. A large development team is required.
4. The process of developing one's own platform is time consuming.
5. Implementing security would be one of the major concerns.

In contrast to these difficulties, the commercially available IoT-cloud platforms are available as already proven solutions. Such platforms can immediately cater to the needs of large scale IoT applications. IoT-cloud platforms provide a seamless connectivity between the IoT system and cloud. So, the IoT application can securely avail different services offered by the cloud. These platforms facilitate the development of a cloud-based IoT ecosystem in short time. The IoT-cloud platform sits as an intermediate layer between the IoT system and cloud, as seen in Figure 2.

As in Figure 2, the IoT system consists of sensors and protocols that transmit the data to IoT cloud platforms. As mentioned earlier, the platform is the gateway to access various capabilities including device connectivity and management, data storage, data processing, visualization, and security. To provide an insight about IoT-cloud platforms, a brief overview about the most popular IoT-cloud platforms, namely AWS IoT platform, Microsoft Azure IoT platform, Cisco IoT Cloud connect, IBM Watson IoT, and Google Cloud IoT, has been described in the subsequent subsections.

AWS IoT Platform

Different services of AWS IoT platform include:

1. **AWS core service:** This service establishes a secure connection and interaction between IoT devices and cloud application. It can access billions of devices, process the messages from all devices, and keep track of devices.
2. **AWS IoT device service:** This service monitors IoT devices for their functionality at a large scale and troubleshoots the malfunctioning of the devices.
3. **AWS IoT device defender:** This service provides security. It creates and manages device identity, device authentication, and device authorization and provides data encryption.
4. **AWS IoT analytics:** This service facilitates analysis of huge data collected from IoT devices using machine learning algorithms.
5. **freeRTOS:** This is an operating system for microcontroller, and it can be used in edge computing for performing real-time tasks.
6. **AWS IoT Greengrass:** This service is used to build and manage IoT application at the edge.

In AWS IoT platform, AWS IoT device defender performs the security related functions as shown in Figure 3 (Amazon Web Services, n.d.).

Figure 2. Layers of a cloud-based IoT application assisted by IoT cloud platform

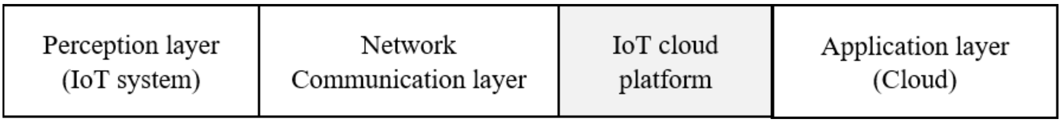
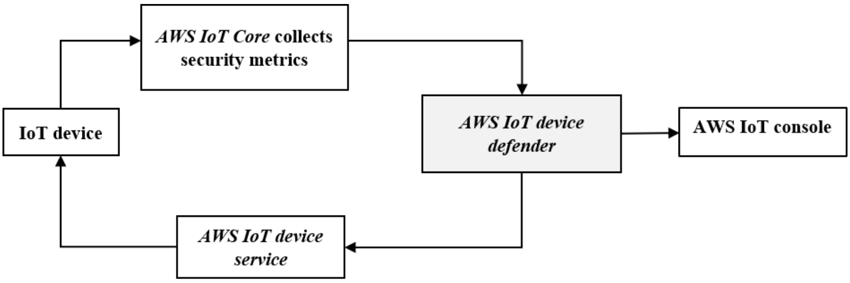

Perception layer (IoT system)
Network Communication layer
IoT cloud platform
Application layer (Cloud)

Figure 3. AWS IoT device defender in implementing security related functions


AWS IoT Core collects security metrics
IoT device
AWS IoT device defender
AWS IoT console
AWS IoT device service

Security related use cases of AWS IoT device defender include:

- Authentication and authorization with X.509 device certificate.
- Continuous monitoring of security metrics collected from an IoT device with the help of AWS IoT core.
- Update device for firmware and software updates with the help of AWS IoT device management.
- Establishment of device connection, identity creation, control, and management using AWS IoT management.
- Analysis of security related metrics using machine learning algorithm for detecting anomalies.
- Continuous monitoring and detection of attack vectors and initiation of the mitigation process.

Microsoft Azure IoT Platform

The core services of Microsoft Azure-IoT platform are categorized into devices, insights, and actions.

The following are the devices:

1. **Azure IoT Hub Device provisioning service:** This service facilitates the registration of IoT devices in a large scale in a secure manner.
2. **Azure-IoT Hub:** This service is the cloud gateway service used to connect and manage IoT devices.

The following are the insights related services:

1. **Azure Stream Analytics/Azure HDInsight:** It performs near real-time analytics.
2. **Azure Data Explorer:** It is used for storing and analyzing large volumes of data.
3. **Azure Data Lake Storage:** It stores large volumes of data.
4. **Azure Machine Learning/Azure Databricks:** It analyzes stored data.

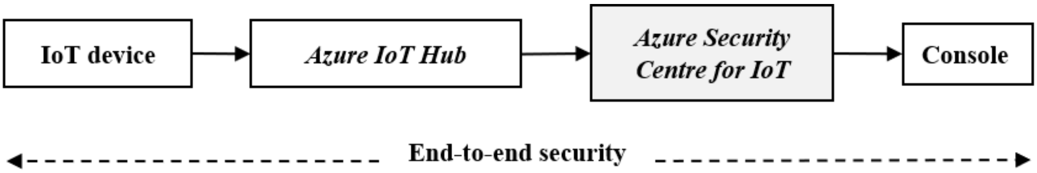
The following are the actions (management and business integration) and related services such as:

1. **Power BI:** It connects to AI-based models and enables data-driven decisions.
2. **Azure Map:** It helps to create location-aware applications.
3. **Azure Cognitive Search:** It provides a cognitive-based search facility.
4. **Azure API Management:** It provides a single place to manage all APIs.
5. **Azure App Service:** It deploys web applications at scale.
6. **Azure Mobile Apps:** It builds cross platform and native mobile apps.

When a new device is created, *Azure-IoT Hub* provides two authentication methods for establishing communication between the device and the hub. They are Shared Access Signature (SAS) token-based with symmetric key authentication and X.509 certificate-based authentication. Also, in the Azure IoT platform, *Azure security centre for IoT* (InfoQ, 2019) service provides end-to-end security for IoT deployment, as shown in Figure 4.

It helps in identifying security threats and responding to emerging threats and handles issues in configurations. *Azure Security Center for IoT* also creates ranked lists of possible misconfigurations and insecure settings, allowing IoT administrators and security professionals to fix the most important issues in their IoT security posture. It creates a list of potential threats, ranked by importance, so that the security operators can remediate problems.

Figure 4. Security related functions using azure security centre for IoT



Cisco IoT-Cloud Connect

Cisco IoT-cloud connect is a mobility cloud-based software suite. It fully optimizes and utilizes the network. Cisco provides IoT solutions for networking, security, and data management. The following are services provided by Cisco IoT-cloud connect:

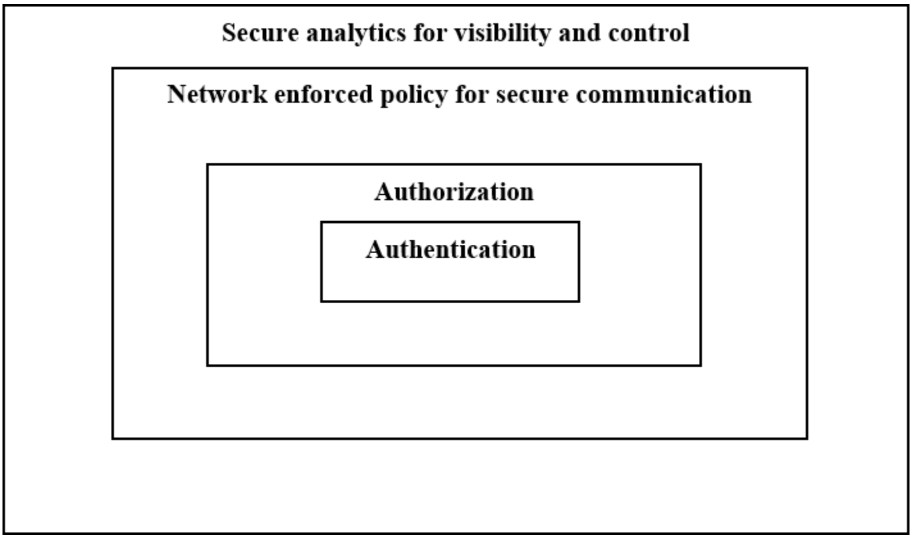
1. It provides granular and real-time visibility over every level of network.
2. It provides updates for every level of the network.
3. It protects the control system from human errors and attacks.
4. It provides increased visibility and control by defending malware and intrusion and offers centralized security controls.

As a secure network-as-a-service, it can optimize the performance and security of every connection, providing end-to-end protection for users and devices across multiple clouds and networks.

It protects the entire IoT systems against every aspect of the unpredictable by securing each device, user, and point of attack to stop more threats.

The key point in Cisco IoT-Cloud Connection with respect to security is the implementation of security foundation using trust relationship between the entities of the IoT system, as shown in Figure 5 (LearnIoT, n.d.).

Figure 5. Cisco IoT-cloud connect: trust relationship-based security framework


Secure analytics for visibility and control
Network enforced policy for secure communication
Authorization
Authentication

Trust is built across different layers and entities of IoT using the following aspects:

1. Only authorized and trusted devices can connect to the network.
2. Trust is established among the entities using strong authentication with certificates and robust access control mechanisms.
3. Trust across layers is brought by secure communication by using encryption protocols like IPsec, TLS (Transport Layer Security), etc.
4. Cisco builds trust by implementing continuous threat monitoring.
5. More importantly with security analytics and visibility services, Cisco gains deeper insights about the IoT environment.

IBM Watson IoT

IBM Watson IoT Platform - Message Gateway (IBM, n.d.) is the core service of *IBM Watson IoT platform*. It connects users and devices on the Internet to the platform through Message Queuing Telemetry Transport (MQTT) protocol with two kinds of publishing, namely point-to-point messaging and topic-based publish-subscribe messaging. The platform investigates the data from devices and extracts the meaningful information for better decisions. It optimizes the operations and resources. It provides AI-based real-time analytics, domain expertise, flexible solutions, and security. Also, *analytics as a service* is an add-on of the platform.

The *IBM Watson IoT Platform* offering integrity for IoT solutions with security by design, certified under the International Organization for Standardization (ISO) 27001 standard, which defines the best practices for information security management processes. Basically, it implements security using authentication, authorization, and encryption.

The platform supports connectivity over TLS v1.2. Certificates and security policies can be used to enhance device connection security. Blacklists can be used to specify devices that are not allowed to connect. Whitelists can be used to allow specific devices to connect. Also, *IBM Watson IoT Platform Advanced Security* visualizes critical risks and enables the creation of policy-driven mitigation actions.

Google Cloud IoT Platform

The main components of Google Cloud IoT platforms (Google Cloud, n.d.) are as follows:

1. **Device manager:** It is used to register the devices.
2. **Protocol bridges:** The registered devices connect to the IoT platform using MQTT or HTTP.
3. **Cloud Pub/Sub:** This component receives the forwarded data and triggers cloud functions.

Google IoT-cloud provides a multi-layered secure infrastructure for building an IoT ecosystem with improved operational efficiency and predictive maintenance of equipment. It analyzes the data using machine learning algorithms and provides immediate business insights.

Google IoT-cloud platforms provide end-to-end security using asymmetric key authentication. Each device is authenticated individually with a pair of keys. Google IoT-cloud provides the following cryptographic algorithms for signing and verifying digital signatures:

1. **RS256:** This algorithm uses an RSA asymmetric encryption scheme with the SHA-256 hashing algorithm for signing and verifying digital signatures.
2. **RSA256_X509:** This combination refers to RSA with X.509 digital certificate which contains identity, public key information, and other details.
3. **ES256:** This algorithm refers to the Elliptic Curve Digital Signature Algorithm which provides smaller key size with the SHA-256 hashing algorithm for signing and verifying digital signatures.

4. **ES256_X509:** This combination refers to the combination of the Elliptic Curve Digital Signature Algorithm with the X.509 certificate format.
5. **The communication between a device and cloud is taking place using TLS v1.2:** Which provides strong encryption and protection against eavesdropping, tampering, and data forgery during data transmission. It uses symmetric and asymmetric encryption algorithms to establish secure connections.
6. **Cloud-IoT Core API access:** Is controlled by Identity and Access Management (IAM) roles and permissions.

How IoT-Cloud Platforms Make the Integration Simple and Secure

The IoT-cloud integration platform can resolve the security challenges effectively and enables a seamless integration. At first, loud computing has been a well-established and mature technology for over a decade, the security aspects have been thoroughly developed and reinforced through various tools and platforms. Several industries use the cloud as their primary infrastructure to support long-term data storage and data backup for recovery during disaster and to perform deeper analytics using historical data. Secondly, cloud is employing several AI-based techniques to monitor and detect security related issues. In addition, predictive algorithms assist in taking appropriate countermeasures against the anticipated issues. Cloud proactively implements various security mechanisms against both known and predicted vulnerabilities. Ultimately, the security attacks in IoT devices and networks can be addressed efficiently through the specialized security services of IoT-cloud platforms:

1. **Centralized security management:** At first the IoT-cloud platform permits for implementation of centralized security management. The devices of IoT networks would be monitored in a unified manner and help in enhanced security governance across the large deployment of IoT devices.
2. **Centralized device registration:** Each device must be registered in the IoT-cloud platform which prevents the inclusion of any unwanted or malicious device into the network.
3. **Centralized device integrity:** No new device can enter the cloud-based IoT network without device registration. Only registered devices can connect to the cloud after proving their authentication. Further, according to ACL and RBAC, the device will be given permission to access the resources according to the previously defined privileges. This ensures device integrity. The key point to be noted here is that the integrity is achieved in a centralized manner.
4. **Enhanced authentication and authorization:** IoT cloud platforms, by implementing stringent authentication protocols and robust access control policies, prevent unauthorized access and device impersonation.
5. **Secure data transmission:** IoT-cloud platforms help in ensuring the communication of data in its encrypted form with the help of encryption protocols like TLS.
6. **Secure data storage:** Cloud provides secure storage of data along with proper storage-access controls. This helps to maintain the integrity and confidentiality of data.
7. **Continuous security monitoring:** The IoT-cloud platforms provide services for continuously monitoring devices, behavior of devices, networks, workloads, applications, etc. in an end-to-end fashion and collect data related to security metrics. These metrics are analyzed to identify the security related threats and to raise alerts for suitable countermeasures.
8. **Regular software update:** The IoT-cloud platform makes the update of firmware, software, and configuration settings easier.
9. **Regular security audit and compliance:** Security audit and compliance becomes a part of the regular tasks of the IoT-cloud platforms, which helps to ensure that proper security processes are in place to safeguard the assets.
10. **Data life cycle management:** The platform helps to enhance data security and data privacy through data life cycle management.

11. **Intruder detection:** With efficient monitoring tools, the platform performs routine intruder detection across IoT networks and across different layers of cloud.
12. **Predictive analytics for detection of potential threats:** The entire IoT ecosystem is monitored for threats using AI-based algorithms. The prediction helps in taking proactive countermeasures in case a weakness is predicted.

FULFILLMENT OF BASIC SECURITY REQUIREMENTS IN AN IOT ECOSYSTEM

Basic security requirements of any IoT system should include confidentiality, integrity, availability, and privacy. How these requirements are fulfilled across different layers of a cloud-based IoT system is discussed in this section:

1. **Confidentiality:** Confidentiality refers to the prevention of data from being accessed by unauthorized persons. This requirement is built based on authentication and authorization. With respect to the perception layer, the data and programs should be protected from disclosure and tampering. In the communication network layer, it should be confidentially transferred. Also, confidentiality should be maintained during storage and processing. In the application layer, the data should be accessed by the specific user for whom it is intended. Authentication and authorization play a vital role in implementing confidentiality. Authentication verifies one's identity. Authorization grants or denies access to resources based on access privileges, permissions, and roles. With these mechanisms, unauthorized access to data is prevented, and thus confidentiality is maintained.
2. **Integrity:** Integrity refers to the protection of data and programs from being altered by unauthorized users. In the perception layer, in addition to data and programs, the integrity of a device is very important. During communication, storage, and processing the integrity of data should be preserved. In the application layer, integrity of data and application programs should be preserved. Here also, by authentication and authorization, access of resources by unauthorized persons can be prevented. Data integrity will be maintained.
3. **Availability:** Availability ensures that all IoT services and devices are accessible only to legitimate users. By authentication and authorization, IoT platforms can prevent DoS attacks and can ensure that system resources are available only to legitimate users.
4. **Privacy:** Privacy protects the personal or sensitive information of a user from other individuals. It is more relevant to the application layer. Through implementation of strong authentication and strict access control, exposure of sensitive information may be prevented.

Thus, authorization and authentication are the very basic mechanisms to realize confidentiality, integrity, availability, and privacy. The fulfillment of basic security requirements across the different layers of a cloud-based IoT ecosystem is given in Table 6.

As defined in Pal et al. (2020), there a many other security requirements like key management, trust, non-repudiation, accountability, usability, reliability, data-freshness, load balancing, mobility, fault-tolerance, location-privacy, etc. So, the security administrator and operators must analyze the security requirements for a particular IoT application in hand. In addition to the basic security requirements, the consumers must necessarily implement the additional security requirements according to the application requirements. The consumers should keep in mind the shared responsibility model of cloud security and implement the required security services from the cloud to meet the specific security needs of the application. Further, the consumers should be conscious of the inclusion of various security related attributes into the Service Level Agreement (SLA). The security solutions should be provided by the providers according to the level mentioned in the SLA.

Table 6. Fulfillment of basic requirements across different layers of a cloud-based iot ecosystem

Security requirement	Perception Layer	Network communication layer	IoT-cloud platform	Application layer (Cloud)
Authentication	Authentication is implemented by mechanisms like X.509 certificates, shared keys or secure tokens	Message-signing and protocol level authentication are implemented during TLS handshake	IoT-cloud platform verifies identities of the devices and users with certificates, shared keys, and secure tokens	Authentication is performed at cloud infrastructure level by verifying the identity of the IoT cloud platform itself using certificates, shared keys, or secure tokens
Authorization	Within an IoT system, authorization is enforced to specify which devices or roles have permission to interact with a particular device using ACL and RBAC	Authorization is to control the access to communication channels, protocols, and message exchanges. It is implemented using ACL and RBAC	Authorization is done to manage access to platform services, data, and resources by defining roles and access control policies with RBAC or ABAC and for accessing different services within the platform	Authorization is done by defining and enforcing user access to cloud services with ACL, RBAC, and ABAC
Confidentiality	Within an IoT system, confidentiality can be implemented using light-weight encryption protocols and secure storage	Confidentiality is implemented through encryption using the TLS protocol	Confidentiality is implemented through encryption using the TLS protocol	Here, confidentiality is done through secure storage
Integrity	Integrity is implemented using checksum and hashing	TLS can employ Message Authentication Code (MAC) algorithms to ensure the integrity of transmitted data	Within the platform, integrity is implemented by data monitoring	Within the cloud, integrity is done through storage integrity checks and security monitoring
Availability	Availability is achieved by the continuous monitoring of the IoT network for detecting failures and anomalies	Availability is achieved by using reliable communication protocols	Availability is obtained by using threat detection and continuous monitoring	Availability is attained by using redundancy and geographic distribution
Privacy	Privacy is implemented using access control. Light-weight encryption is also being used	Privacy is implemented using TLS	Within the IoT-cloud platform, privacy is implemented using access control, data anonymization, and pseudonymization Data lifecycle management	Within cloud, privacy is implemented using encryption storage access controls Security auditing Compliance testing

LIMITATIONS

Apart from the benefit of cloud in providing the resources for storage, processing, analytics, and visualization for IoT applications, the integration of IoT with cloud has brought in increased security challenges on the both sides. This means that the vulnerabilities in the cloud may influence the IoT system and vice versa. So, robust security mechanisms must be implemented and security monitoring should be done to proactively look for security weaknesses and perform timely countermeasures.

IoT-cloud platforms facilitate the secure integration through the readily available proven best security practices. The following are major limitations in the cloud-based IoT environment:

1. Ensuring privacy in a cloud-based environment is very difficult due to variations in the laws and regulations of privacy among countries, while cloud inherently deals with data storage across different geographical locations.
2. Despite the best security implementation, human errors may occur in the configuration of infrastructure related settings, platform related settings, application related settings, and security related settings.
3. Lack of visibility into devices and their internal operations (as vendors do not reveal much information to users) makes the user configure the devices with flaws, which again poses serious issues.
4. Implementing access control is really challenging in a large scale computing environment where numerous devices, users, and gateways are interacting with one another. As access control is implemented through various forms like ACL, RBAC, ABAC, and other policies while dealing with several platforms, applications and hardware, it is more likely for the error to occur.
5. Despite the implementation of security tools, insider, or intruder threats in both the IoT environment as well as cloud environment post still a big issue as both the industries are involved with a wide range of stakeholders, like device manufacturers, third-party hardware and software vendors, service providers, certificate providers, etc.

CONCLUSION

The IoT world is growing with an exponential increase in the number of devices connected to the Internet. Cloud computing becomes an inevitable element of an IoT ecosystem to provide resources for storing IoT data, to assist in the analysis of data, and to support visualization and actions. Obviously, the integration of cloud and IoT increase the security threats on either technology. The IoT system may get exposed due to the security vulnerabilities and vice versa. This paper comprehensively reviews the security issues that are likely to occur while both get merged. For an industry, developing its own connectivity solution to cloud involves more effort, a high cost, and a long time. Despite these, the business case needs a proof-of-validation before its development. Here, commercially available IoT-cloud platforms readily enable industries to simplify the integration. Moreover, it is packed with several security mechanisms to address the evolving security issues. Machine learning algorithms are extensively used for predicting potential threats and so people can take appropriate security measures in time to protect the resources. Cloud extends its centralized security monitoring and management services to cover a wide range of tasks to maintain device integrity, data protection, system availability, and privacy protection. Despite all these security measures, one cannot ensure that an IoT ecosystem is completely safe and secure due to manual errors, insider threats, intruders, physical threats, and threats associated with third-party vendors and service providers themselves. Apart from these, in the future IoT is moving forward to its next generation with more and more devices, 5G and improved connectivity, edge AI, etc. which will obviously require robust security measures. Future research needs to address the security needs of next-generation IoT networks.

REFERENCES

Abdur Razzaq, M., Habib, S., Ali, M., & Ullah, S. (2017). Security issues in the Internet of Things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, *8*(6). doi:10.14569/IJACSA.2017.080650

Abed, A. K., & Anupam, A. (2022). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(4), e285. doi:10.1002/spy2.285

Abusaimeh, H. (2020). Virtual machine escape in cloud computing services. *International Journal of Advanced Computer Science and Applications*, *11*(7). doi:10.14569/IJACSA.2020.0110743

Adi, E., Anwar, A., Baig, Z., & Zeadally, S. (2020). Machine learning and data analytics for the IoT. *Neural Computing & Applications*, *32*(20), 16205–16233. doi:10.1007/s00521-020-04874-y

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics (Basel)*, *11*(1), 16. doi:10.3390/electronics11010016

Ahmed, K. I., Tahir, M., Habaebi, M., Lau, S. L., Ahad, A., Zhao, J., Li, F., Kaleem, Z., Pham, V., Han, H., & Yang, H. (2021). Machine learning for authentication and authorization in IoT: Taxonomy, challenges and future research direction. *Sensors (Basel)*, *21*(15), 1–34. doi:10.3390/s21155122 PMID:34372351

Akhtar, M. S., & Feng, T. (2022). A systemic security and privacy review: Attacks and prevention mechanisms over IoT layers. *EAI Endorsed Transactions on Security and Safety*, *8*(30), e5. doi:10.4108/eetss.v8i30.590

Al-Anzi, F. S., Yadav, S. K., & Soni, J. (2014). Cloud computing: Security model comprising governance, risk management and compliance. In *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, 1-6. doi:10.1109/ICDMIC.2014.6954232

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys and Tutorials*, *22*(3), 1646–1685. doi:10.1109/COMST.2020.2988293

AlamT. (2018). A reliable communication framework and its use in Internet of Things (IoT). *CSEIT1835111, 3*(5), 450-456. https://ssrn.com/abstract=3619450

Alam, T. (2021). Cloud-based IoT applications and their roles in smart cities. *Smart Cities*, *4*(3), 1196–1219. doi:10.3390/smartcities4030064

Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Al-Rimy, B. A. S. (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. *Applied Sciences (Basel, Switzerland)*, *11*(19), 9005. doi:10.3390/app11199005

Alharbi, T., & Portmann, M. (2019). The (in)security of virtualization in software defined networks. *IEEE Access : Practical Innovations, Open Solutions*, *1*, 66584–66594. Advance online publication. doi:10.1109/ACCESS.2019.2918101

Alhijawi, B., Almajali, S., Elgala, H., Bany Salameh, H., & Ayyash, M. (2022). A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers & Electrical Engineering*, *99*, 99. doi:10.1016/j.compeleceng.2022.107706

Ali, S., Khan, M. A., Ahmad, J., & Malik, A. W., & ur Rehman, A. (2018). Detection and prevention of Black Hole Attacks in IOT & WSN. In *Proceedings of the 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC)*, (pp. 217-226). IEEE. doi:10.1109/FMEC.2018.8364068

Alizai, Z. A., Tareen, N. F., & Jadoon, I. (2018). Improved IoT device authentication scheme using device capability and digital signatures. In *Proceedings of the 2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, (pp. 115–119). IEEE. doi:10.1109/ICAEM.2018.8536261

Almolhis, N., Alashjaee, A. M., Duraibi, S., Alqahtani, F. A., & Moussa, A. N. (2020). The security issues in IoT - cloud: A review. *16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, (pp. 191-196). IEEE.

Amazon Web Services. (n.d.). *AWS IoT device defender*. Amazon web services. https://aws.amazon.com/iot-device-defender/

Asghar, M., & Amjad, A. (2018). Securing insecure web API's in cloud computing. *Mitteilungen Klosterneuburg, 68.*

Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J., & Wills, G. B. (2017). Integration of cloud computing with Internet of Things: Challenges and open issues. In *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, (pp. 670-675). IEEE. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105

Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of Things security: Challenges and key issues. *Security and Communication Networks*, *2021*, 1–11. doi:10.1155/2021/5533843

Bernsmed, K., Jaatun, M. G., & Undheim, A. (2011). Security in service level agreements for cloud computing. In *CLOSER 2011 - Proceedings of the 1st International Conference on Cloud Computing and Services Science*, (pp. 555-560). IEEE.

Bettayeb, M., Nasir, Q., & Abu Talib, M. (2019). Firmware update attacks and security for IoT devices: Survey. In *Annual International Conference on Arab Women in Computing.* ACM. doi:10.1145/3333165.3333169

Bonkra, A., & Dhiman, P. (2021). IoT security challenges in cloud environment. In *2021 2nd International Conference on Computational Methods in Science & Technology (ICCMST)*, (pp. 30-34). IEEE. doi:10.1109/ICCMST54943.2021.00018

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684–700. doi:10.1016/j.future.2015.09.021

Butt, U. A., Amin, R., Mehmood, M., Ahmad, F., & Hassan, S. (2023). Cloud security threats and solutions: A survey. *Wireless Personal Communications*, *128*(1), 387–413. doi:10.1007/s11277-022-09960-z

Chen, F., Luo, D., Xiang, T., Chen, P., Fan, J., & Truong, H. (2021). IoT cloud security review: A case study approach using emerging consumer-oriented applications. [TIOT]. *ACM Computing Surveys*, *54*(4), 1–36. doi:10.1145/3447625

Choudhary, D. (2018). Security challenges and countermeasures for the heterogeneity of IoT applications. *Journal of Autonomous Intelligence*, *1*(2), 16. doi:10.32629/jai.v1i2.25

Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, *12*(11), 3179–3202. doi:10.1007/s13042-020-01241-0

Dahiya, A., & Gupta, B. B. (2021). A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. *Future Generation Computer Systems*, *117*(12), 193–204. doi:10.1016/j.future.2020.11.027

Dahiya, A., Gupta, B. B., Alhalabi, W., & Ulrichd, K. (2022). A comprehensive analysis of blockchain and its applications in intelligent systems based on IoT, cloud and social media. *International Journal of Intelligent Systems*, *37*(12), 11037–11077. doi:10.1002/int.23032

Deore, M., Mane, D., Upadhye, G., & Kittad, N. (2022). The security concerns and solutions for cloud-based IoT system. *Journal of Theoretical and Applied Information Technology*, *100*, 5159–5178.

Dong, S., Abbas, K., & Jain, R. (2019). A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 80813–80828. doi:10.1109/ACCESS.2019.2922196

Dong, Y., & Lei, Z. (2019). An access control model for preventing virtual machine hopping attack. *Future Internet*, *11*(3), 82. doi:10.3390/fi11030082

Duan, Q., Ansari, N., & Toy, M. (2016). Software-defined network virtualization: An architectural framework for integrating SDN and NFV for service provisioning in future networks. *IEEE Network*, *30*(5), 10–16. doi:10.1109/MNET.2016.7579021

Feng, Y., Wang, W., Weng, Y., & Zhang, H. (2017). A replay-attack resistant authentication scheme for the Internet of Things. In *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, (pp. 541-547). IEEE. doi:10.1109/CSE-EUC.2017.101

Finsliq Blog. (n.d.). PaaS security issues in cloud computing. *Finsliq Blog*. https://www.finsliqblog.com/paas-security-issues-in-cloud-computing/

Fortino, G., Guerrieri, A., Pace, P., Savaglio, C., & Spezzano, G. (2022). IoT platforms and security: An analysis of the leading industrial/commercial solutions. *Sensors (Basel)*, *22*(6), 2196. doi:10.3390/s22062196 PMID:35336368

FutureLearn. (n.d.). *Steps - Key topics in digital transformation*. FutureLearn. https://www.futurelearn.com/info/courses/key-topics-in-digital-transformation/0/steps/257345

Gaurav, A., Psannis, K., & Peraković, D. (2022). Security of cloud-based medical Internet of Things (miots): A survey. [IJSSCI]. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–16. doi:10.4018/IJSSCI.285593

Google Cloud. (n.d.). *Overview of Google Cloud IoT Core*. Google Cloud. https://cloud.google.com/iot/docs/concepts/overview

Goyal, M., & Dutta, M. (2018). Intrusion detection of wormhole attack in IoT: A review. In *2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET)*, (pp. 1-5). IEEE. doi:10.1109/ICCSDET.2018.8821160

Guida, C. G., Gupta, B. B., Lorusso, A., Marongiu, F., Santaniello, D., & Troiano, A. (2021). An integrated BIM-IoT approach to support energy monitoring. In *International Conference on Smart Systems and Advanced Computing (Syscom-2021)*, (pp. 1-6). IEEE.

Gupta, S., Gupta, B. B., & Chaudhary, P. (2017). Hunting for DOM-based XSS vulnerabilities in mobile cloud-based online social network. *Future Generation Computer Systems*, *79*, 307–318. doi:10.1016/j.future.2017.05.038

Hachemi, F. E., Mana, M., & Bensaber, B. A. (2020). Study of the impact of sinkhole attack in IoT using Shewhart control charts. In *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, (pp. 1-5). IEEE. doi:10.1109/GLOBECOM42002.2020.9322603

Haghnegahdar, L., Joshi, S. S., & Dahotre, N. (2022). From IoT-based cloud manufacturing approach to intelligent additive manufacturing: Industrial Internet of Things—An overview. *International Journal of Advanced Manufacturing Technology*, *119*(3-4), 1461–1478. doi:10.1007/s00170-021-08436-x

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(5), 5. doi:10.1186/1869-0238-4-5

Hassan, A. A., & Thayananthan, V. (2021). Analysis of machine learning for securing software-defined networking. *Procedia Computer Science*, *194*, 229–236. doi:10.1016/j.procs.2021.10.078

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 82721–82743. doi:10.1109/ACCESS.2019.2924045

Huang, W., Zhang, Y., & Feng, Y. (2020). ACD: An adaptable approach for RFID cloning attack detection. *Sensors (Basel)*, *20*(8), 2378. doi:10.3390/s20082378 PMID:32331407

Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. *Applied Sciences (Basel, Switzerland)*, *12*(8), 3953. doi:10.3390/app12083953

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics*, *13*(1), 57–65. doi:10.1016/j.aci.2016.03.001

IBM. (2021). *Overview of the architecture*. IBM Knowledge Center. https://www.ibm.com/docs/en/wip-mg/5.0.0.1?topic=overview-architecture

Imran, S. M. A., Alam, M. M., & Su'ud, M. M. (2021). A survey of IoT security issues - From past to future trends. *Journal of Computational Science*, *17*(11), 1031–1045. doi:10.3844/jcssp.2021.1031.1045

Info Q. (2019, August 16). *Azure security center for IoT reaches general availability*. InfoQ. https://www.infoq.com/news/2019/08/azure-security-center-iot-ga/

Ingham, M., Marchang, J., & Bhowmik, D. (2020). IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN. *IET Information Security*, *14*(4), 329–339. doi:10.1049/iet-ifs.2019.0447

ISACA. (2022). *SaaS security risk and challenges*. ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2022/saas-security-risk-and-challenges

Islam, T., Manivannan, D., & Zeadally, S. (2016). A classification and characterization of security threats in cloud computing. *International Journal of Next-Generation Computing, 7*.

Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A review of security standards and frameworks for IoT-based smart environments. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 121975–121995. doi:10.1109/ACCESS.2021.3109886

Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks - Vulnerabilities and countermeasures. *Global Transitions Proceedings*, *2*(2), 362–367. doi:10.1016/j.gltp.2021.08.045

Khan, A. W., Khan, M. U., Khan, J. A., Khan, J., & Gul, W. (2021). Identification and prioritization of security challenges of big data on cloud computing based on SLR: A fuzzy-TOPSIS analysis approach. *Software, Practice & Experience*, *33*(12).

Khanam, S., Tanweer, S., & Khalid, S. S. (2022). Future of Internet of Things: Enhancing cloud-based IoT using artificial intelligence. [IJCAC]. *International Journal of Cloud Applications and Computing*, *12*(1), 23. doi:10.4018/IJCAC.297094

Khattab, A., Abdelgawad, A., & Yelmarthi, K. (2016). Design and implementation of a cloud-based IoT scheme for precision agriculture. In *2016 28th International Conference on Microelectronics (ICM)*, (pp. 201-204). IEEE. doi:10.1109/ICM.2016.7847850

Knapp, E. (2011). Common pitfalls and mistakes. *Industrial Network Security*, 303-312. DOI: .10.1016/B978-1-59749-645-2.00011-2

Krishna, B. V. S., & Gnanasekaran, T. (2017). A systematic study of security issues in Internet-of-Things (IoT). In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, (pp. 107-111). IEEE. doi:10.1109/I-SMAC.2017.8058318

LearnIoT. (n.d.). *Cisco IoT security framework*. LearnIoT. https://www.learniot.com/cisco-iot-security-framework/

Leloglu, E. (2017). A review of security concerns in Internet of Things. *Journal of Computer and Communications*, *5*(1), 121–136. doi:10.4236/jcc.2017.51010

Li, F., Wang, J., & Song, Z. (2023). Privacy protection of cloud computing based on strong forward security. *International Journal of Cloud Applications and Computing*, *13*(1), 1–9. doi:10.4018/IJCAC.323804

Li, X., Wang, Q., Lan, X., Chen, X., Zhang, N., & Chen, D. (2019). Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach. *IEEE Access : Practical Innovations, Open Solutions*, *1*, 9368–9383. Advance online publication. doi:10.1109/ACCESS.2018.2890432

Li, Y., & Chen, M. (2015). Software-defined network function virtualization: A survey. *IEEE Access : Practical Innovations, Open Solutions*, *3*, 2542–2553. doi:10.1109/ACCESS.2015.2499271

Lineswala, H., & Swali, P. (2020). Remote monitoring of IoT device: Cloud computing & IoT. [IJERT]. *International Journal of Engineering Research & Technology (Ahmedabad)*, *8*(5).

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology., doi:10.6028/NIST.SP.800-145

Mercado Herrera, A., Ling Lopez, J. C., Tong Delgado, M. A., Rivas Lopez, M., Morales Carbajal, C., Romero Parra, R., Bravo Zanoguera, M. E., Cuevas Gonzalez, D., Amezquita Garcia, J. A., Cota Rivera, E. I., Limon-Molina, G. M., & Murrieta-Rico, F. N. (2023). Effective use of embedded platforms in the development of experiments for enhancing the interests of STEAM students in Mexico. In C. Martin, B. T. Miller, & D. Polly (Eds.), *Technology integration and transformation in STEM classrooms*.

Mohammadnia, H., & Ben Slimane, S. (2020). IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network. *2020 Seventh International Conference on Software Defined Systems (SDS)*, (pp. 5-13). IEEE. doi:10.1109/SDS49854.2020.9143903

Mohanty, J., Mishra, S., Patra, S., Pati, B., & Panigrahi, C. R. (2021). IoT security, challenges, and solutions: A review. In C. R. Panigrahi, B. Pati, P. Mohapatra, R. Buyya, & K. C. Li (Eds.), Progress in advanced computing and intelligent engineering (pp. 525-536). Springer. doi:10.1007/978-981-15-6353-9_46

Mohiuddin, I., & Almogren, A. (2020). Security challenges and strategies for the IoT in cloud computing. In *2020 11th International Conference on Information and Communication Systems (ICICS)*. ICICS. doi:10.1109/ICICS49469.2020.239563

Narayana, K. E., & Jayashree, K. (2021). Survey on cross virtual machine side channel attack detection and properties of cloud computing as sustainable material. *Materials Today: Proceedings*, *45*(7), 6465–6470. doi:10.1016/j.matpr.2020.11.283

Nayak, J., Naik, B., Dash, P. B., Vimal, S., & Kadry, S. (2022). Hybrid Bayesian optimization hypertuned catboost approach for malicious access and anomaly detection in IoT nomalyframework. *Sustainable Computing: Informatics and Systems, 36*. ISSN 2210-5379. 10.1016/j.suscom.2022.100805

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys and Tutorials*, *21*(3), 2702–2733. doi:10.1109/COMST.2019.2910750

Nirmal, K., Janet, B., & Kumar, R. (2020). Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection. *Peer-to-Peer Networking and Applications*, 1–13.

Nitiynandan, S., & Kamalakkannan, S. (2022). Detection and prevention of man-in-the-middle attack in IoT network using regression modeling. *Advances in Engineering Software*, 169.

Nobles, C. (2022). Investigating cloud computing misconfiguration errors using the human factors analysis and classification system. *Science Bulletin*, *27*(1), 59–66. doi:10.2478/bsaft-2022-0007

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2020). Security requirements for the Internet of Things: A systematic approach. *Sensors (Basel)*, *20*(20), 5897. doi:10.3390/s20205897 PMID:33086542

Peerbits. (2023). *Biggest IoT Security Challenges*. Peerbits. https://www.peerbits.com/blog/biggest-iot-security-challenges.html

Prakash, V., Xie, S., & Huang, D. Y. (2022). *Software update practices on smart home IoT devices*. https://arxiv.org/pdf/2208.14367.pdf

Putra, G. D., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2020). Trust management in decentralized IoT access control system. In *Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, (pp. 1–9). IEEE. doi:10.1109/ICBC48266.2020.9169481

Qabil, S., Waheed, U., Awan, S. M., Mansoor, Y., & Khan, M. A. (2019). A survey on emerging integration of cloud computing and Internet of Things. In *2019 International Conference on Information Science and Communication Technology (ICISCT)*. IEEE. doi:10.1109/CISCT.2019.8777438

QuickHeal. (2019). *Android-based IoT devices open ADB port, inviting easy attacks, crypto-miners*. Quick Heal Blogs. https://blogs.quickheal.com/android-based-iot-devices-open-adb-port-inviting-easy-attacks-crypto-miners/

Quilachamin, W. G., Alonso, I. A., & Herrera-Tapia, J. (2018). Overview of service and deployment models offered by cloud computing, based on International Standard ISO/IEC 17788. *International Journal of Advanced Computer Science and Applications*, *9*(11), 218–228. doi:10.14569/IJACSA.2018.091131

Raj, M. G., & Pani, S. K. (2022). Chaotic whale crow optimization algorithm for secure routing in the IoT environment. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–25. doi:10.4018/IJSWIS.300824

Raj Chelliah, P., & Surianarayanan, C. (2021). Multi-cloud adoption challenges for the cloud-native era: Best practices and solution approaches. [IJCAC]. *International Journal of Cloud Applications and Computing*, *11*(2), 67–96. doi:10.4018/IJCAC.2021040105

Rajan, A., Jithish, J., & Sankaran, S. (2017). Sybil attack in IoT: Modelling and defenses. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, (pp. 2323-2327). IEEE. doi:10.1109/ICACCI.2017.8126193

Rajasekaran, P., & Ranganathan, M. (2021). A study of security challenges from a federated cloud perspective. In *Advances in Security and Privacy in Communication Systems* (pp. 182–193). IGI Global. doi:10.4018/978-1-7998-5040-3.ch011

Rakotondravony, N., Taubmann, B., Mandarawi, W., Weishäupl, E., Xu, P., Kolosnjaji, B., Protsenko, M., de Meer, H., & Reiser, H. P. (2017). Classifying malware attacks in IaaS cloud environments. *Journal of Cloud Computing: Advances. Journal of Cloud Computing (Heidelberg, Germany)*, *6*(1), 1–12. doi:10.1186/s13677-017-0098-8

Ray, P. P. (2016). A survey of IoT cloud platforms. *Future Computing and Informatics Journal*, *1*(1–2), 35–46. doi:10.1016/j.fcij.2017.02.001

Righi, R. da R., Correa, E., Gomes, M. M., & Costa, C. A. (2020). Enhancing performance of IoT applications with load prediction and cloud elasticity. *Future Generation Computer Systems*, *109*, 689–701. doi:10.1016/j.future.2018.06.026

Russell, B., Garlati, C., & Lingenfelter, D. (2015). *Security guidance for early adopters of the Internet of Things (IoT); Mobile working group peer reviewed document*. Cloud Security Alliance Publishing.

Sabir, S. (2018). Security issues in cloud computing and their solutions: A review. *International Journal of Advanced Computer Science and Applications*, *9*(11), 343–346. doi:10.14569/IJACSA.2018.091147

Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and solutions survey. *Sensors (Basel)*, *22*(19), 7433. doi:10.3390/s22197433 PMID:36236531

Saini, D. K., Kumar, K., & Gupta, P. (2022). Security issues in IoT and cloud computing service models with suggested solutions. *Security and Communication Networks*, *2022*, 1–9. doi:10.1155/2022/4943225

Shaikh, S., Rupa, C., Srivastava, G., & Reddy Gadekallu, T. (2022). Botnet attack intrusion detection in IoT enabled automated guided vehicles. In *2022 IEEE International Conference on Big Data (Big Data)*, (pp. 6332-6336). IEEE. doi:10.1109/BigData55660.2022.10020355

Shakya, S. (2022). A perspective review of security issues in IoT with cloud environment. *Journal of IoT in Social, Mobile, Analytics, and Cloud*, *4*(2), 84–93. doi:10.36548/jismac.2022.2.002

Sivaselvan, N., Bhat, K. V., Rajarajan, M., Das, A. K., & Rodrigues, J. J. P. C. (2022). SUACC-IoT: Secure unified authentication and access control system based on capability for IoT. *Cluster Computing*. doi:10.1007/s10586-022-03733-w

Sood, K., Karmakar, K. K., Yu, S., Varadharajan, V., Pokhrel, S. R., & Xiang, Y. (2020). Alleviating heterogeneity in SDN-IoT networks to maintain QoS and enhance security. *IEEE Internet of Things Journal*, *7*(7), 5964–5975. doi:10.1109/JIOT.2019.2959025

Stergiou, C. L., Bompoli, E., & Psannis, K. E. (2023). Security and privacy issues in IoT-based big data cloud systems in a digital twin scenario. *Applied Sciences (Basel, Switzerland)*, *13*(758), 758. doi:10.3390/app13020758

Subba Rao, B. V., Sharma, V., Rathore, N., Prasad, D., Anandaram, H., & Soni, G. (2023). A secure framework to prevent three-tier cloud architecture from malicious malware injection attacks. [IJCAC]. *International Journal of Cloud Applications and Computing*, *13*(1), 1–22. doi:10.4018/IJCAC.317220

Swamy, S. N., Jadhav, D., & Kulkarni, N. J. (2017). Security threats in the application layer in IoT applications. *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, (pp. 477-480). IEEE. doi:10.1109/I-SMAC.2017.8058395

Szefer, J., Keller, E., Lee, R. B., & Rexford, J. (2011). Eliminating the hypervisor attack surface for a more secure cloud. In *Proceedings of the 6th ACM International Systems and Storage Conference*, (pp. 13-24). Association for Computing Machinery. doi:10.1145/2046707.2046754

Szefer, J., & Lee, R. B. (2012). Architectural support for hypervisor-secure virtualization. In *Proceedings of the 49th Annual Design Automation Conference*, (pp. 723-728). Association for Computing Machinery. doi:10.1145/2150976.2151022

Tank, D., Aggarwal, A., & Chaubey, N. (2019). Virtualization vulnerabilities, security issues, and solutions: A critical study and comparison. *International Journal of Information Technology : an Official Journal of Bharati Vidyapeeth's Institute of Computer Applications and Management*, *14*(2), 847–862. doi:10.1007/s41870-019-00294-x

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences (Basel, Switzerland)*, *10*(12), 4102. doi:10.3390/app10124102

TechTarget. (n.d.). Cloud workload protection platform security benefits and features. *Tech Target.*. https://www.techtarget.com/searchsecurity/tip/Cloud-workload-protection-platform-security-benefits-features

Tiwari, A., & Garg, R. (2022). Adaptive ontology-based IoT resource provisioning in computing systems. [IJSWIS]. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–18. doi:10.4018/IJSWIS.306260

Trnka, M., & Cerny, T. (2017). Authentication and authorization rules sharing for Internet of Things. *Software Networking*, *2017*(1), 35–52. doi:10.13052/jsn2445-9739.2017.003

Truong, H.-L., & Dustdar, S. (2015). Principles for engineering IoT cloud systems. *IEEE Cloud Computing*, *2*(3), 68–76. doi:10.1109/MCC.2015.23

Vasudevan, A., Chaki, S., Jia, L., McCune, J., Newsome, J., & Datta, A. (2013). Design, implementation and verification of an extensible and modular hypervisor framework. In *Proceedings of the IEEE Symposium on Security and Privacy*, (pp. 430-444). IEEE. doi:10.1109/SP.2013.36

Vurukonda, N., & Thirumala Rao, B. (2016). A study on data storage security issues in cloud computing. *Procedia Computer Science*, *92*, 128–135. doi:10.1016/j.procs.2016.07.335

Wang, Z. (2010). HyperSafe: A lightweight approach to provide lifetime hypervisor control-flow integrity. In *IEEE Symposium on Security and Privacy*, (pp. 380–395). IEEE. doi:10.1109/SP.2010.30

Wassan, S., Suhail, B., Mubeen, R., Raj, B., Agarwal, U., Khatri, E., Gopinathan, S., & Dhiman, G. (2022). Gradient boosting for health IoT federated learning. *Sustainability (Basel)*, *14*(24), 16842. doi:10.3390/su142416842

Wu, J., Lei, Z., Chen, S., & Shen, W. (2017). An access control model for preventing virtual machine escape attack. *Future Internet*, *9*(2), 20. doi:10.3390/fi9020020

Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2019). Data collection for security measurement in wireless sensor networks: A survey. [8543865]. *IEEE Internet of Things Journal*, *6*(2), 2205–2224. doi:10.1109/JIOT.2018.2883403

Xu, B., Ma, M., Wu, J., Li, L., Liu, Y., & Shen, H. (2018). A security design for the detecting of buffer overflow attacks in IoT device. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 72862–72869. doi:10.1109/ACCESS.2018.2881447

Xu, Z., He, D., Vijayakumar, P., Gupta, B. B., & Shen, J. (2023). Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical WSNs. *IEEE Journal of Biomedical and Health Informatics*, *27*(5), 2334–2344. doi:10.1109/JBHI.2021.3128775 PMID:34788225

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. doi:10.1109/JIOT.2017.2694844

Yasrab, R. (2018). *MPSM: Multi-prospective PaaS security model*. arXiv preprint arXiv:1804.04731 [cs.CR].

Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. *IEEE Communications Magazine*, *55*(1), 26–33. doi:10.1109/MCOM.2017.1600363CM

Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, *91*, 244–251. doi:10.1016/j.future.2018.08.038

Chellammal Surianarayanan currently holds the position of Assistant Professor of Computer Science in the Centre for Distance and Online Education, Bharathidasan University, Tiruchirappalli, Tamilnadu, India. Prior to her current role, she worked as a Scientific Officer at the Indira Gandhi Centre for Atomic Research, Department of Atomic Energy, Kalpakkam, India. In total she gained 25 years of research and academic experience. Completed Ph.D., degree at Bharathidasan University, India. Published more than 25 research papers in esteemed peer-reviewed journals such as IEEE Transactions, Springer-Verlag, Inderscience, IGI Global, ICTACT, MDPI, and others. She has authored three books and contributed ten book chapters. She has also served as an editor for three books.

Pethuru Raj has been the chief architect and vice president of the Site Reliability Engineering (SRE) Center of Excellence (CoE) division, Reliance Jio Infocomm Ltd. (RJIL), Bangalore. His previous stints are in IBM Cloud center of Excellence (CoE), Wipro consulting services (WCS), and Robert Bosch Corporate Research (CR). In total, he has gained more than 17 years of IT industry experience and 8 years of research experience.Finished the CSIR-sponsored PhD degree at Anna University, Chennai and continued with the UGC-sponsored postdoctoral research in the Department of Computer Science and Automation, Indian Institute of Science, Bangalore. Thereafter, he was granted a couple of international research fellowships (JSPS and JST) to work as a research scientist for 3.5 years in two leading Japanese universities. Published more than 30 research papers in peer-reviewed journals such as IEEE, ACM, Springer-Verlag, Inderscience, etc. He has authored 10 books thus far and focus on some of the emerging technologies such as IoT, Cognitive Analytics, Blockchain, Digital Twin, Docker Containerization, Dvata Science, Microservices Architecture, fog/edge computing, etc. He has contributed 30 book chapters thus far for various technology books edited by highly acclaimed and accomplished professors and professionals.