International Journal of Advanced Engineering and Management Research

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Sensor-cloud Architecture: a Security Taxonomy in Cloud-assisted Sensor Networks

Zemenu Ketema[1], Baba Ahmad Mala[2], Gradwell Dzikanyanga[3], Romário Tomo[2], Jamilu Ibrahim Argungu[3]

[1]Huazhong university of science and technology,
Wuhan, Hubei 430074, China

[2]Huazhong university of science and technology,
Wuhan, Hubei 430074, China

[3]Huazhong university of science and technology,
Wuhan, Hubei 430074, China

[4]Huazhong university of science and technology,
Wuhan, Hubei 430074, China

[5]Adamu Augie College of Education,
Argungu, Kebbi State, Nigeria

doi: 10.51505/ijaemr.2023.9204 URL: http://dx.doi.org/10.51505/ijaemr.2023.9204

Received: Dec 15, 2023 Accepted: Dec 21, 2023 Online Published: March 19, 2024

Abstract

The integration of cloud computing with wireless sensor networks (WSN), known as Sensor-Cloud, has garnered significant attention for its application in fields such as healthcare, habitat monitoring, military surveillance, and disaster management. This fusion aims to overcome the inherent processing and storage limitations of sensor networks by leveraging the cloud's flexibility, scalability, and enhanced capacities. Despite these advantages, Sensor-Cloud systems face challenges including latency, dependability, load balancing, bandwidth constraints, resource optimization, and security vulnerabilities. Security concerns are paramount, as the architecture's integrity is threatened by potential attacks on sensor nodes, communication channels, and the cloud infrastructure. Although existing literature extensively explores these issues, a comprehensive analysis of security threats specific to Sensor-Cloud remains essential. This paper presents an in-depth examination of security challenges within Sensor-Cloud environments, proposing innovative solutions and developing taxonomies of security attacks from an architectural perspective. Through this analysis, the paper aims to fortify Sensor-Cloud architecture against diverse security threats, ensuring its robustness and reliability across various applications.

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Keywords: Sensor-cloud architecture, security, wireless sensor networks, Internet of Things

1. Introduction

1.1 Security Challenges in Sensor-Cloud Integration

The rapid proliferation of Internet of Things (IoT) technologies and sensor networks has ushered in an era of unprecedented data generation, presenting both opportunities and significant challenges. As sensors become increasingly ubiquitous, generating vast volumes of data, traditional centralized data collection and processing approaches struggle to keep pace. This has catalyzed the emergence of the sensor-cloud architecture, an innovative paradigm that marries cloud computing's scalability and storage capabilities with IoT's extensive data collection network. This architecture is pivotal in sectors like healthcare, environmental monitoring, and defense, offering enhanced data management, processing, and analysis.

However, this integration is not without its challenges. The primary concern lies in maintaining quality of service (QoS) amidst issues such as latency, congestion, and security within these inherently resource-constrained networks. The sensor-cloud paradigm aims to mitigate these limitations by offloading resource-intensive tasks to the cloud, thereby extending network lifespans and improving QoS. Yet, security, privacy, and trust within sensor-cloud architectures remain underexplored in literature, with existing studies focusing more on component-specific vulnerabilities than on a holistic security framework.

This study builds upon previous work by delving into the security challenges specific to sensor-cloud environments. Unlike earlier reports, which might have separately addressed cloud computing or IoT security, this paper offers a comprehensive analysis of the sensor-cloud architecture, highlighting critical security, privacy, and trust issues. Most resource-intensive tasks are transferred from the resource-constrainedsensornet works to the cloud architecture(Jan, Khan, et al., 2019).

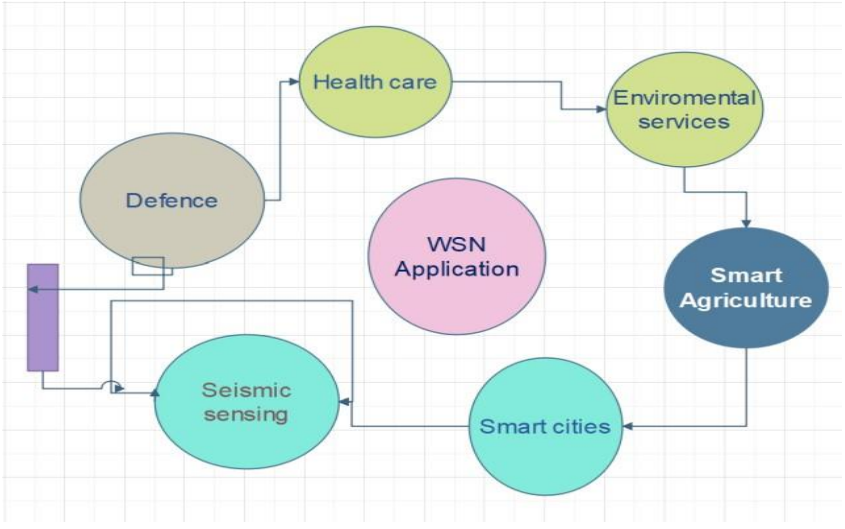

Figure 1. Applications of wireless sensor networks

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Asseenin Figure 1, WSNs are currently usedin several sectors, suc has healthcare, defence (such as military target tracking and surveillance (Yu et al., 2021), government, and environmental services like natural disasterre life (Jan, Zhang, et al., 2019), hazardous environment exploration (Erdelj et al., 2017), and seismic sensing (Khedo et al., 2020). Through this research, we aim to:

1) Establish the importance of security analysis within sensor-cloud architectures, acknowledging the gap in comprehensive security studies.
2) Relate our study to existing research by identifying the unique security challenges of integrating sensor networks with cloud computing, thus extending the theoretical and practical understanding of sensor-cloud security.
3) Propose a modern taxonomy of security and privacy measures, detailing security attacks and countermeasures from an architectural standpoint, to enhance the resilience of sensor-cloud systems.

By addressing these objectives, the research underscores the criticality of robust security frameworks to facilitate the safe, effective deployment of sensor-cloud technologies across various industries.

1.2 Motivation

The concept of combining sensors with cloud computing, known as sensor-cloud, has gained a lot of attention for its ability to function virtually. This setup is celebrated for its efficient exchange of information in real time and its flexible management of resources, leading to better use of resources. It also improves upon traditional sensor networks by offering better processing and storage options. Thanks to these qualities, it's a great fit for systems that need to make quick decisions based on real-time data, serving multiple users and applications simultaneously. However, the spread-out and virtual nature of sensor-cloud, along with its wide variety of users, introduces several challenges. To address these issues, a vast amount of research has been conducted, looking at sensor-cloud from different angles. But when it comes to security, many of these studies fall short because they only focus on the security of individual components. The study by(F. Khan et al., 2020) breaks down the various parts and connections within a unique sensor-cloud setup. It organizes the architecture of sensor-cloud into three main layers: one focused on the client, one on the middleware, and one on the sensors themselves, each layer stacked vertically. Yet, this broad overview doesn't tackle security concerns directly. This research steps in to cover new ground by examining security and privacy challenges that span from the bottom layer (sensors) through the communication channels up to the cloud infrastructure itself, offering a comprehensive look from the architectural standpoint. This approach not only adds to the existing body of knowledge but also expands on previous research by highlighting security and privacy concerns across all levels of the sensor-cloud architecture.

1.3 Significance of Addressing Sensor-Cloud Security

The integration of sensor networks with cloud computing, forming the sensor-cloud architecture, represents a cornerstone in advancing IoT applications across various sectors. This architecture's capacity to process and manage large volumes of data in real-time is vital for critical applications in healthcare, environmental monitoring, and national security. However, the evolving landscape

Vol. 9, No. 02; 2024

ISSN: 2456-3676

of cyber threats poses significant risks, threatening the integrity, privacy, and functionality of these systems. The urgency to address these security challenges is not merely technical but a requisite for societal trust and the sustainable adoption of sensor-cloud technologies. Past research has often treated the security considerations of cloud computing and sensor networks in isolation, leading to a fragmented understanding of the threats and vulnerabilities unique to their integration. The sensor-cloud environment, characterized by its distributed nature and the sensitivity of the data it handles, necessitates a novel approach to security. This research aims to bridge this gap, providing a comprehensive analysis of security challenges and proposing targeted countermeasures that are critical for the resilience of sensor-cloud architectures. The importance of this research extends beyond theoretical contributions, offering practical solutions to a pressing global challenge. By systematizing security threats and their countermeasures within the sensor-cloud context, the study supports the development of more robust and secure infrastructures. This, in turn, facilitates the broader deployment and acceptance of sensor-cloud systems, ensuring their potential benefits can be fully realized without compromising security or privacy.

1.4Review of Pertinent Literature

The integration of sensor networks with cloud computing, known as sensor-cloud, has emerged as a significant area of interest due to its transformative potential in data management across various fields. This combination enhances data processing, storage, and analysis capabilities but introduces substantial security challenges, extensively explored in recent literature. Security within sensor networks, cloud computing, and their communication channels has been the focus of numerous studies. Research addressing secure data communication includes works cited in (Bhushan & Sahoo, 2018), (Olakanmi & Dada, 2020), which discuss vulnerabilities and countermeasures to secure data transmission. Specifically, the findings in (W. Li et al., 2021) spotlight security gaps at the sensor network level, proposing solutions ranging from energy-efficient protocols to sophisticated security mechanisms. The security of cloud architectures has been analyzed in depth, with studies like (Liu et al., 2015) categorizing attacks into application-based, storage-based, virtual machine-based, and network-based, offering innovative security measures through system adjustments. This discussion is furthered by(Parast et al., 2022), and (El Kafhali et al., 2022) (Tabrizchi & Kuchaki Rafsanjani, 2020), which assess risks, explore intrusion detection systems, and provide a comprehensive taxonomy of security threats to cloud platforms, suggesting directions for future research. Additionally, the convergence of sensor and cloud technologies has prompted investigations into architecture and concept (Alturki et al., 2021), service virtualization (Bordel et al., 2018), and service-oriented frameworks (Chatterjee et al., 2015), contributing to a comprehensive understanding of the sensor-cloud ecosystem. Analytically validated theoretical models(Ali et al., 2022), protocol analyses(Zhang et al., 2020), and application-specific studies, such as those focusing on healthcare privacy and security (Masood et al., 2018), smart data collection(Ali et al., 2020), secure communication (Yao et al., 2019), and secure data collection in sensor-cloud architectures (Tian et al., 2022), further the discourse, providing insights into practical applications and security considerations.This extensive body of literature underscores the criticality of security within the sensor-cloud

Vol. 9, No. 02; 2024

ISSN: 2456-3676

paradigm and sets a foundation for this study. Despite significant advancements, the unique combination of sensor networks and cloud computing in this integrated architecture presents new challenges and opportunities for innovation, directing the focus of our research.

2. Security and Privacy Challenges in the Sensor-Cloud

The sensor cloud is a type of computer system that lets different sensor networks share resources and work together. It lets many people build sensing apps at the same time without the usual limits. This setup allows for a system where many users and apps can use the same processing, sensing, and network resources together. Even though sensor clouds offer a lot of benefits, there's a big problem with security. Since anyone can use this system for different reasons, it's not very secure or private. This means there's a big risk that private information could get stolen or misused. Traditional security methods that work for single sensor networks or regular cloud systems don't work well for sensor clouds, so we need new ways to keep them safe. Based on these security issues, we suggest a way to understand and deal with cyber-attacks on sensor clouds, focusing on three main parts shown in Figure 3.We talk more about these parts and other details in the sections that follow.

2.1 Protection of the Sensor Node

This involves the implementation of robust security measures to safeguard the sensor nodes against unauthorized access and tampering. These measures can be classified into physical and logical categories. Physical protection strategies restrict unauthorized physical access to the sensor nodes' location, thereby safeguarding the hardware components. Logical protection strategies encompass a range of authentication mechanisms designed to verify the identities of users or nodes requesting access, ensuring that only authorized entities can interact with the sensor nodes. Moreover, the communication among sensor nodes is secured through the adoption of advanced security protocols.

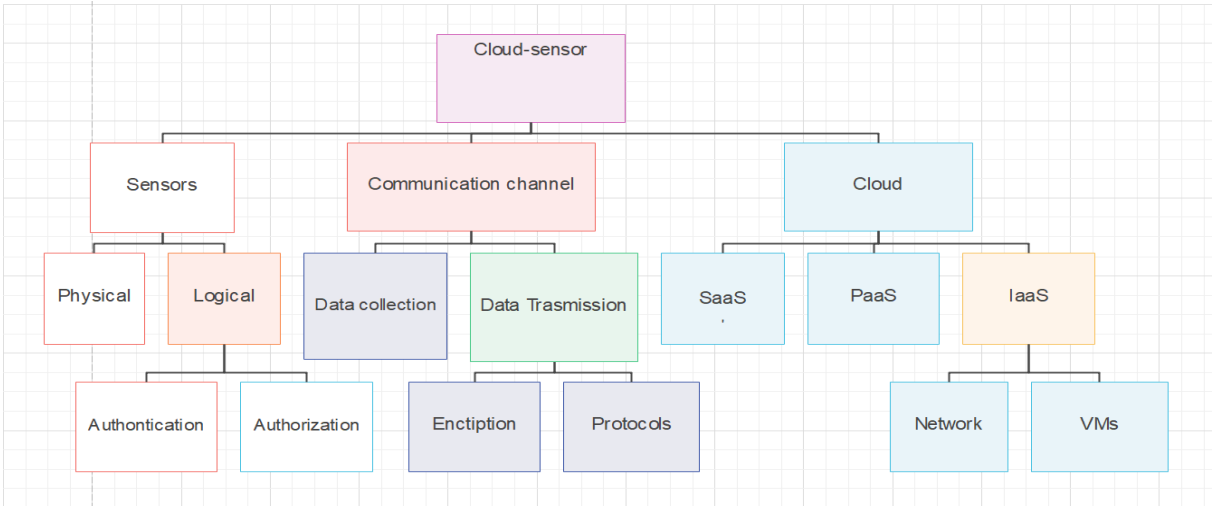

Figure 2:Cybersecurity Attack Taxonomy in Sensor-Cloud Architecture.

2.2 Securing the Communication Pathway

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Security in the context of communication channels is twofold: addressing attacks and countermeasures during the data collection phase at the sensor node, and mitigating risks and implementing defenses for secure data transmission over the wireless channel.

2.2.1 Attacks and defenses at the sensor node when gathering data

a) Tampering and Eavesdropping: These attacks involve unauthorized modifications to the sensor nodes, converting legitimate nodes into malicious ones to facilitate unauthorized access to sensitive data or to intercept communications. Such breaches can lay the groundwork for more severe security threats, including wormhole and black-hole attacks. Countermeasures against device tampering require the deployment of tamper-proof technologies, albeit with potential increases in energy consumption and processing overhead.
b) Jamming and Denial of Service (DoS) Attacks: These attacks disrupt the standard operational protocols of sensor nodes and networks by overwhelming them with interference from a powerful jamming source operating on the same frequency. The impact of jamming attacks varies based on the strength of the jamming source, from localized disruptions to widespread network incapacitation. Frequency-hopping techniques can be used to prevent jamming assaults. However, these approaches are inappropriate for resource-constrained sensor nodes due to high processing and memory needs. Transmission strategies using Ultra Wide Band (UWB) provide a potential solution for defending these resource-constrained networks from jamming attempts. However, they are not as efficient against jamming attempts as the frequency hopping strategy(Al-Shaihk & Hassanpour, 2019). One of the strategies for mitigating this type of attack is frequency hopping.
c) Denial of Service (DoS) Attacks: In these attacks, an attacker node exhausts all available resources, denying access to legitimate users. The attackers, masquerading as normal nodes, disrupt the network's operation and diminish its service capacity.

2.2.2 Attacks and Responses during Secure Wireless Data Transmission

a) False Routing: In this scenario, an attacker introduces incorrect routing data into the system, causing the routing table to be overwhelmed with inaccurate information and to exceed its capacity. Additionally, the attacker might reroute the data packets along an unintended path before they are sent through the network(Ray & Kumar, 2021), (J. Li et al., 2020).
b) Packet Replication: In environments with limited resources like Wireless Sensor Networks (WSN), attackers target the scarcity of power, processing capacity, and bandwidth by duplicating received packets and distributing them to other nodes. This action triggers network overload, leading to congestion and diminished performance, while also prematurely draining the network's energy and shortening its lifespan (Dabbagh & Rayes, 2019).
c) Black Hole Attacks: Here, a malicious node acts as a data void or "black hole" by accepting all incoming data but failing to forward it. This disrupts data flow within the network and degrades its functionality.
d) Sinkhole Attacks: Attackers manipulate traffic by using compromised nodes to falsely advertise routing information, tricking other nodes into sending their data towards a malicious target. This misdirection can lead to data being intercepted or misrouted, affecting

Vol. 9, No. 02; 2024

ISSN: 2456-3676

network reliability.

e) Wormhole Attacks: Through this method, data packets are captured at one location and tunneled to another, re-entering the network at this new point. It involves collaboration between attackers to distort routing information, alter the network's structure, and cause packet loss.

f) Selective Message Forwarding: Attackers selectively block certain data packets while allowing others to pass, resulting in partial data loss. This undermines the network's reliability and the integrity of its applications, especially when the attacker is situated along the data's path.

g) Spoofing Attacks: In spoofing attacks, an attacker disguises as a legitimate user to launch various disruptions. By forging credentials, they alter routing data, create loops, send false errors, and delay transmissions, severely impacting network traffic. Techniques like acknowledgment and IP spoofing are used to either fake node statuses or hijack IP addresses, leading to network congestion or even paralysis, while also gaining unauthorized access to sensitive data.

h) Acknowledgment Spoofing: This involves replicating nodes using legitimate IDs to introduce unauthorized nodes into the network, misleading routing information and affecting decision-making processes. It raises concerns over network security and privacy, suggesting the need for verification methods to detect such duplications

i) Node Replication Attacks: Passive information collecting involves attackers using powerful antennas and receivers to capture information and data streams from both the node and the network. Along with other information, the attackers intercept the sensor node's location, locate the node in the network, and comprehend the messages conveyed. After discovering the node, the attacker can launch various attacks, including sensor node damage and deeper network knowledge.

j) Passive Information Gathering: A sensor network comprises sensor nodes that work together to complete a task. In a Sybil attack, malicious node masquerades as a group of nodes while assuming the identities of the real nodes, disrupting network operations. Among the problems caused by Sybil's assaults are distributed storage, approximation of node location, and erroneous routing information. By confirming the identity of the nodes, the WSN can be safeguarded from the Sybil attack. The difficult issue is that nodes are resource-constrained. Hence classic techniques are inapplicable in these networks. As a result, lightweight security solutions should be built to protect nodes from future security attacks.

k) Sybil Attacks: Many ICMP requests are routed to the victim node in these attacks. In response to these requests, the victim node sends out infinite ICMP answers, clogging and paralyzing the entire network. One approach for protecting the network from such assaults is to configure network devices such as routers and individual computers to ignore continuous ICMP requests.

2.2.3Securing data at the cloud platform

The NIST developed the three sensor-cloud delivery models and subsequently adopted them by the industry. This section presents various security threats that target each component and their

Vol. 9, No. 02; 2024

ISSN: 2456-3676

responses. Figure 4 depicts a taxonomy of possible assaults on three different cloud services: SaaS, PaaS, and IaaS(A. A. Khan et al., 2020)(Zakarya & Gillam, 2019). VM security is also considered because the cloud is typically virtualized regarding resource provisioning(Muhammad et al., 2019),(Sharma et al., 2019).

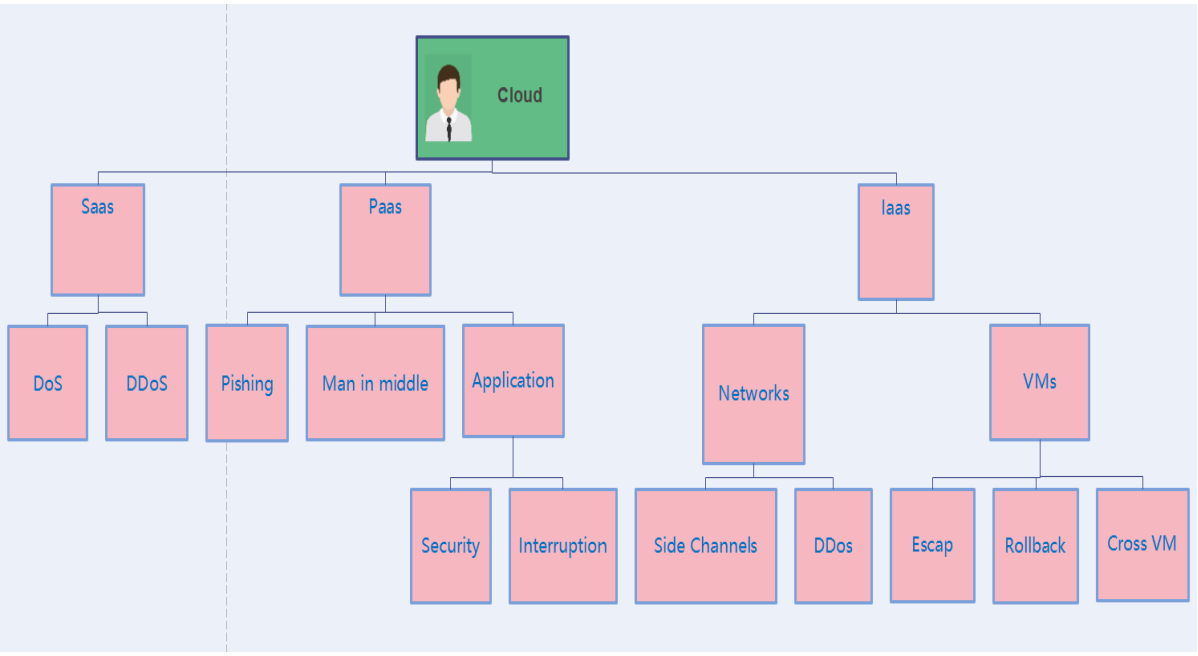

Figure 3. Security Threats in Cloud Computing Service Models

a) Software as a Service (SaaS)

The entire application package is hosted on the cloud server in this architecture. It is provided as a service on demand to an unlimited number of clients.

Some well-known on-demand software services include email platforms like Gmail and development environments like Google App Engine. The online system also solves issues for its users around things like managing software permissions, offering a wide variety of software options, and providing as much memory as needed. This is because on-demand software merges information and processes to deliver services over the internet or through software-based methods, as shown in Figure 4.

Vol. 9, No. 02; 2024

ISSN: 2456-3676

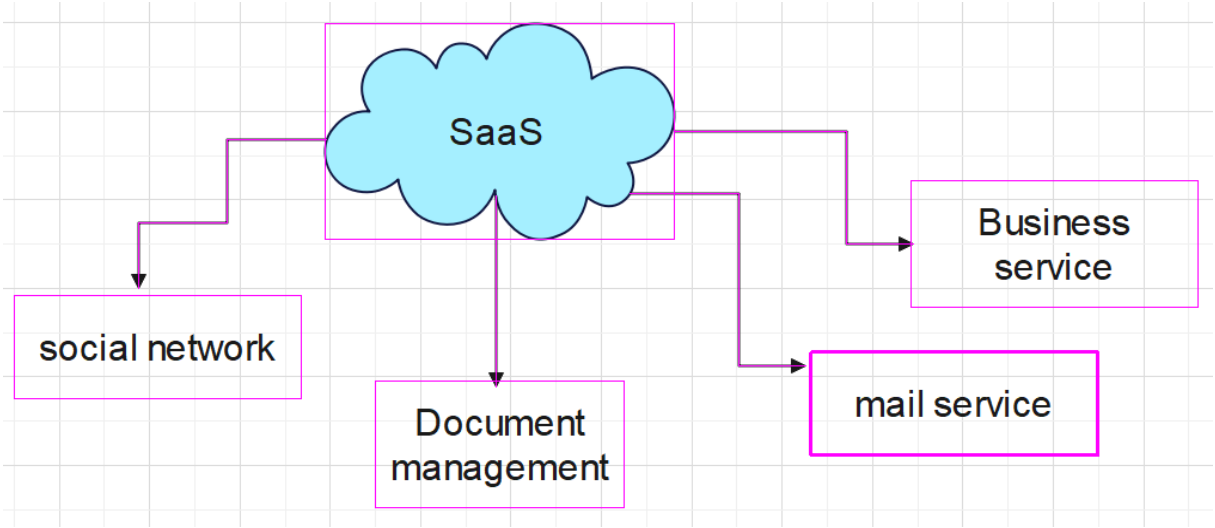

Figure 4. Examples of Software as a Service (SaaS) Applications

Below is a list of common security problems that on-demand software faces.

- Denial Of Service (dos)attacks: During a DoS attack, the system and its resources are bombarded with excessive requests, disrupting their standard functions. The assailants flood the network and servers with a barrage of superfluous data packets, overwhelming their operational thresholds. Such assaults can render the network or system inoperable, denying legitimate users access to services. DoS attacks may cause network bottlenecks, data loss, and system crashes. To defend against these, a combination of response planning, robust network design, and early threat identification is crucial. DDoS attacks, a variant of DoS, are complex and can be challenging to detect, often signaled by a noticeable decrease in network speed. Quick action is essential upon recognizing these signs to address the compromised elements.
- Sql Injection Attack: SQL injection attacks involve introducing malicious code that executes and modifies SQL commands. These operations can even delete rows, tables, or entire tables, as well as the entire database in some cases.
- Cross-Site Scripting: The attackers seek to steal the identity information of legitimate users who use these services for authentication in these attacks. The attackers use this information to access their private information and confidential data being communicated or stored on the network. Authentication attacks can also result in bypass attacks, brute force attacks, session eavesdropping, replay attacks, and key logger attacks (Aladwan et al., 2020).
- Website Application Attacks: Attackers often target online applications, inserting harmful client-side scripts to get login information from legitimate users. They use this information to launch various attacks. When users visit these web applications, the harmful script runs without them knowing.

b) Platform as a Service (PaaS)

In this model, cloud providers offer their users both software and tools to create their own

Vol. 9, No. 02; 2024

ISSN: 2456-3676

applications. Users benefit from greater flexibility and control, allowing them to either use available applications or craft customized ones that fit their specific requirements. Examples of the software environments provided include combinations like Linux, Apache, MySQL, PHP, as well as limited versions of Java EE, Ruby, etc., as depicted in Figure 5. Users pay for these services based on their usage.

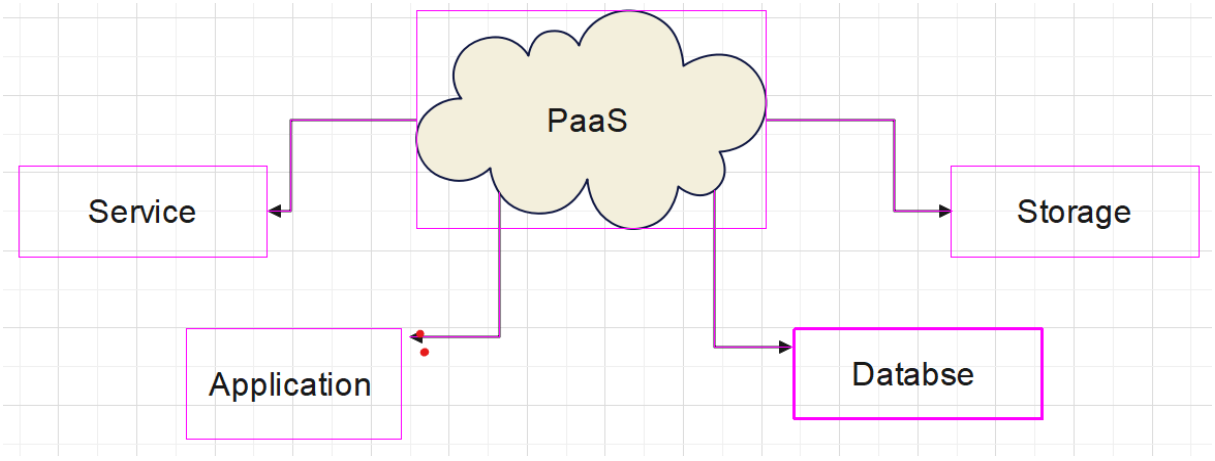

Figure 5: Platform as a service (PaaS)

When it comes to security breaches associated with this service model, the following are noted:

- Phishing attacks: During phishing scams, perpetrators commonly aim to illicitly acquire confidential data from unsuspecting individuals. This form of deception is preferred by cybercriminals for committing identity theft. They often send deceptive emails to legitimate users requesting private and sensitive details. When users are fooled into responding to these emails, their responses, which include private information, are rerouted to the cybercriminals. Additionally, merely opening these fraudulent emails may result in the installation of malware or other malicious files that compromise the system and allow unauthorized access to confidential data. The information most at risk includes private financial details and personal identification data.
- Man-in-the-middle attack: In these attacks, an unauthorized party positions themselves between two communicating entities, such as virtual machines, to eavesdrop and potentially steal confidential information. This breach can serve as a stepping stone for further attacks.
- Cloud malware-injection attacks: This attack modifies data and various functionalities of the server by deteriorating its performance. Some of the most common malware injection attacks are SQL injection and cross-site scripting (XSS).
- Password reset: Attackers may trick users into resetting their passwords through deceptive means, such as offering bogus services that require registration. Once the attacker has the registration details, they can reset passwords for various user accounts across multiple platforms.
- Programming flaws: Refer to defects or errors in software that can result in abnormal

Vol. 9, No. 02; 2024

ISSN: 2456-3676

behavior or crashes. These vulnerabilities may be exploited by attackers to gain control over systems and access confidential data, potentially leading to unexpected downtime and financial losses. It is essential for software developers to correct these vulnerabilities and for providers to update them on users' machines.

- Application security: These are often used in critical applications for extra processing, are also targeted by attackers. The sink node, which relays collected data to the cloud, becomes a prime target. Various attacks on these networks can degrade performance and consume the limited energy and bandwidth, which underscores the importance of securing these networks to safeguard sensitive information.

c) Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) aims to boost system efficiency by offering a variety of computing resources such as server farms, data storage grids, and shared computing environments. In the realm of IaaS, services like Amazon Web Services (AWS) EC2, virtual machines, containers, and Google Cloud are well-known offerings, as depicted in an illustrative figure 6. These services provide resources related to computing power and data storage in a distributed manner to individuals, rather than from a single, centralized location. This distribution not only saves on the expenses associated with acquiring high-end, expensive infrastructure but also tends to be more dependable. Users typically incur costs based on how much they use these services, paying the provider accordingly.

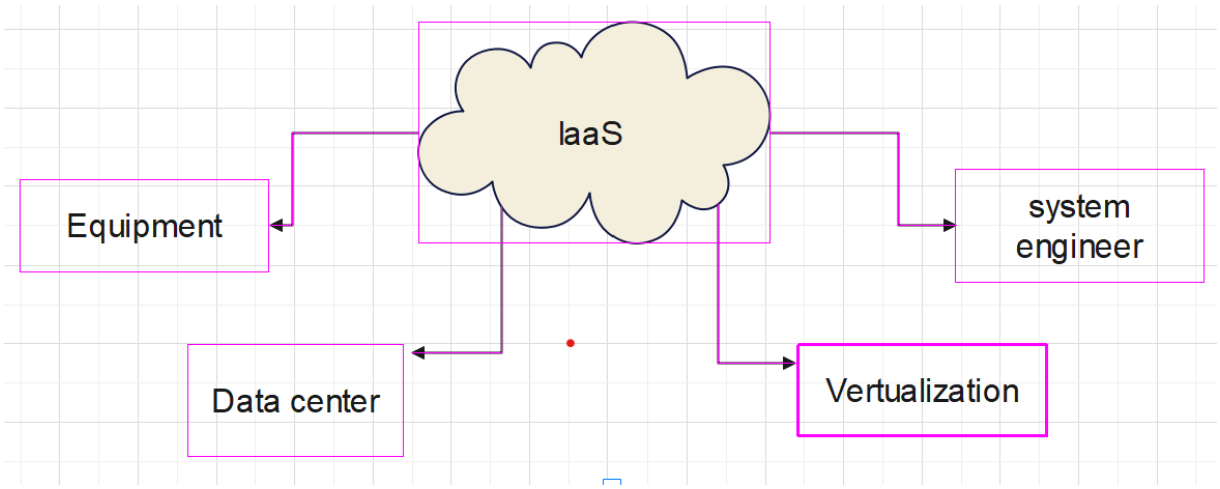

Figure 6: Platform as a service (IaaS)

There are several common security threats that target IaaS platforms, which users and providers must be vigilant against. Some of them are explained below.

a) Stepping Stone Attacks: This attack involves an aggressor concealing their trail by using multiple intermediate points, making it tough to trace their real identity due to the deployment of deceptive tactics.

b) Virtual Machine Escape: An attacker exploits this weakness to make a virtual system

Vol. 9, No. 02; 2024

ISSN: 2456-3676

improperly interact with its managing software, gaining unauthorized control and compromising all virtual systems overseen by that software.

c) Side Channel Attacks: The attacker obtains knowledge from the system's implementation at the design level in these types of attacks. They exploit the network flaw and gain access to information such as power usage, electromagnetic leaks, and sound leaks, which give the attackers further information to launch subsequent assaults.

d) Insider Threats: An individual within an organization pushes the system's limits of storage and processing, potentially leading to minor disruptions or a total system collapse.

e) Virtual Machine (VM) rollback attacks: In a Virtual Machine (VM) rollback attack, an intruder covertly uses a compromised system manager to reactivate a VM to an earlier state without the legitimate user's awareness. Users who manage one or more VMs through cloud services are typically the targets. The attacker in these scenarios ignores or undoes essential security measures, such as recent updates that protect the system. For example, they might launch a brute force attack to guess a VM's login credentials. Operating systems often have defenses to prevent such attacks, like temporarily locking access after multiple incorrect password entries or deleting data after a set number of failed attempts. However, attackers can bypass these security measures by resetting the VM to its original state repeatedly. They can also revert changes to user permissions, potentially exposing sensitive information to unauthorized individuals. This type of attack is unique in that the VM is set back to a previous state, as opposed to replay attacks, where old communications are sent repeatedly to the VM. Moreover, these attacks can be related to the process of moving VMs from one location to another.

f) Cross Virtual Machine Attacks: The cloud architecture makes it easier for businesses to extend their resources on demand by delivering virtual machines (VM). It also provides logical isolation between the VMs that isolate one from the other. It suggests that these are logically separate VMs that share a physical server and resources. Cross-VM attacks are commonly used to target such a multi-tenant virtual environment. By redirecting network traffic and manipulating or accessing other VMs on the same hypervisor, the attackers exploit a single VM to target other VMs on the same hypervisor. Furthermore, the attackers mostly target cache memory. They also attack the CPU, memory, I/O devices, and cloud network.

g) Session Hijacking: A session is all of the information associated with an ongoing transaction. The session information and a unique ID are often saved on a server. The unique ID is often a random number combined with the session's start time and date. Customers receive the session ID with their initial request and present it to the server with each subsequent request. It enables the server to retrieve the stored data relevant to that particular session, establishing a logical link between the current and prior operations. Session hijacking is a prevalent security concern in cloud computing. During these assaults, the adversary acquires unauthorized access to session-related information contained in cookies. Once the attacker obtains such access, It allows them to perform everything a legitimate user can do on the network, jeopardizing its security, privacy, and integrity.

h) Distributed Denial of Service (DDoS) Attacks: The attackers' goal in a DDoS assault is to disrupt regular network operations by restricting access to available resources and the

Vol. 9, No. 02; 2024

ISSN: 2456-3676

network. These resources include web servers, CPU, bandwidth, and memory. Cloud architecture can harm the numerous cloud services provided by virtual servers. It reduces its quality or, in certain cases, completely disrupts network connectivity and consumes its bandwidth. To launch DDoS assaults, attackers typically use many agents or bots. To initiate such attacks, these attackers typically target a bug/flaw or known vulnerabilities in software. They typically monitor the network for vulnerable machines that operate as agents for attackers, also known as zombies(Agrawal & Tapaswi, 2019). The attacker's primary goal is to interrupt the network's normal operation.

i) Theft-of-Service Attacks: A hostile virtual machine misbehaves in a Theft-of-Service attack, so the VM hacks the hypervisor and assigns more resources than it can receive. The other VMs co-located on the same server suffer due to this increased resource allocation for the malicious virtual machine. As a result, other co-located VMs receive fewer resources than they have paid for, which lowers their performance and raises their expenses.

3. Countermeasures and controls

Ensuring the safety of the sensor-cloud architecture involves intricate efforts. To achieve a secure environment, it's essential to coordinate policies, technology, and personnel effectively. Here are several proposed strategies to safeguard this architecture from a range of security challenges and attacks.

3.1End-to-end encryption

The main advantage of the sensor cloud is the transition from centralized to distributed architecture of various resource-intensive tasks, like processing and storage. Even though this change in work distribution has many benefits, it also creates several security risks. End-to-end encryption is highly desirable because this data is transferred from server to server and between numerous geographic areas.

3.2Scanning for malicious activities

Although end-to-end encryption significantly enhances data protection against malicious threats, it introduces certain challenges. One notable issue is that firewalls and intrusion detection systems are unable to inspect encrypted data. This limitation necessitates the development of innovative strategies and preventive actions to effectively differentiate between benign and malicious encrypted data once it arrives at these security checkpoints, such as IDS and firewalls.

3.3Consumer validation for the cloud

The cloud helps users by moving a few resource-intensive operations (from the sensor to fog, sensor to remote cloud, and fog to the cloud) from the resource-constrained Platform to the resource-rich Platform. However, verifying true and legitimate users from intruders and hackers is one of the difficult problems in these systems. It safeguards the cloud infrastructure.

3.4Insider attacks

The most common threats to the security of sensor-cloud systems come from insiders, such as current or former employees. These individuals, whether working full-time, part-time, or previously employed by the organization, pose a significant risk due to their comprehensive

Vol. 9, No. 02; 2024

ISSN: 2456-3676

knowledge of the company's operations and network infrastructure. Their potential to compromise the confidentiality and integrity of the information system stems from various motives, including revenge, pressure, ideological reasons, personal pride, or the desire for financial gain by stealing intellectual property or engaging in espionage. Identifying these insider threats is difficult because they often have legitimate access and may even work for rival companies to gain a financial edge. To protect against such risks, cloud services must adopt security measures like user verification and strengthen internal safeguards. Strategies such as implementing strict organizational policies, rotating job roles, educating staff, and promptly removing access for departing employees are critical in mitigating these threats.

3.5Secure leveraged resources

Due to the multi-tenancy concept, all cloud resources are shared by numerous users. In such a setting, user authentication is required before the shared resources, such as the hypervisor, orchestration, and monitoring tools, are secured presents a thorough analysis of similar attacks and their defenses.

3.6Business continuity plans

Maintaining records of previous security incidents and breaches is crucial for an organization's ability to react effectively. These records serve as a guide for handling future security issues. Utilizing machine learning techniques to analyze historical data can help predict potential security threats or attacks, enabling the implementation of preemptive measures.

4. Open research challenges

Cloud computing has changed the way we use, manage, and control various resources, but it also brings many challenges, especially in security. Although experts have made significant progress in securing cloud and sensor networks, there are still many questions that need answers. One issue is that attackers can easily overwhelm the limited resources of sensor nodes with harmful data, draining their energy and resources. One way to prevent this is by adding special packets that check and control data flow, along with strong ways to verify the identity of devices to prevent attacks.

However, creating these security measures is difficult for two main reasons. First, the basic components of these devices can't support complex encryption methods that are commonly used because they're too advanced or heavy for the devices' capabilities. Second, adding extra security information to messages increases costs because it requires more data, computation, and storage.

Future solutions should aim for security methods that are efficient, requiring minimal extra data and less computational power. Another challenge is the inherent weaknesses in the communication protocols of cloud architecture, which are crucial for automating and managing services but can be exploited by attackers to launch attacks and steal data. For example, specific ways of communicating, like SOAP, can be vulnerable to attacks.

Furthermore, since data in sensor-cloud networks is spread out over wide areas, it must be securely encrypted as it moves. While there are studies focusing on symmetric encryption (where the same key is used for both encrypting and decrypting data), these often overlook the risks of

Vol. 9, No. 02; 2024

ISSN: 2456-3676

node capture attacks, where an attacker takes control of a node in the network. Developing new encryption methods that are both strong and efficient for this setup would be very interesting.

Finally, our review shows there's a lack of a unified approach in IoT security that enables communication across different domains (like cloud, fog, and sensor devices) to address specific types of threats. Future research could also explore areas like lightweight encryption, network security protocols, and digital forensics to enhance security in sensor-cloud architectures.

4. Conclusion and future work

In summary, the approach of combining sensor technology with cloud computing offers an innovative solution to manage the vast data generated by Internet-connected devices. This method is flexible, can grow as needed, and is cost-effective for managing and processing data from sensors over the cloud. It enables immediate analysis and processing of this data, supporting applications in urban development, healthcare, and environmental observation. The paper also outlines a detailed classification of potential security threats to this setup, grouping them by the parts they target and suggesting protective measures based on the structure's design, including the communication paths between the cloud and the sensors. The paper points out the gaps in previous research and highlights its contributions to understanding these security challenges. It suggests areas for future investigation to make the sensor-cloud framework more robust, reliable, and safeguarded against new threats. Looking ahead, there could be developments in the design of sensor-cloud systems to overcome current technical hurdles. Future research could explore ways to bolster data security and confidentiality in the cloud. Emerging technologies like edge computing and block chain could be integrated into the sensor-cloud setup to boost its efficiency and dependability. Further studies might also look into how sensor-cloud setups affect devices that rely on batteries. There's an anticipation that considerations for the security and privacy of IoT systems will be integrated early in their design process to prevent treating security as a secondary concern. While tracking the location of smart devices raises privacy issues, there are scenarios where it could be beneficial, such as aiding authorities in locating a missing person through their devices. Interest in this area of digital investigation is expected to grow, alongside efforts to push computing capabilities closer to the data source, in what's known as the fog computing domain. The architecture of the sensor cloud has the potential to revolutionize how we manage and utilize data from sensors, enabling us to build smarter and more efficient urban spaces, industries, and societies by continually seeking ways to refine and enhance this technology.

References

Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769–3795.

Aladwan, M. N., Awaysheh, F. M., Alawadi, S., Alazab, M., Pena, T. F., & Cabaleiro, J. C. (2020). TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud. *IEEE Transactions on Industrial Informatics*, *16*(9), 6203–6213.

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Ali, I., Ahmedy, I., Gani, A., Munir, M. U., & Anisi, M. H. (2022). Data collection in studies on Internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): Similarities and differences. *IEEE Access, 10*, 33909–33931.

Ali, I., Ahmedy, I., Gani, A., Talha, M., Raza, M. A., & Anisi, M. H. (2020). Data collection in sensor-cloud: A systematic literature review. *IEEE Access, 8*, 184664–184687.

Al-Shaihk, N. F. A., & Hassanpour, R. (2019). Active defense strategy against jamming attack in wireless sensor networks. *International Journal of Computer Network and Information Security, 10*(11), 1.

Alturki, R., Alyamani, H. J., Ikram, M. A., Rahman, M. A., Alshehri, M. D., Khan, F., & Haleem, M. (2021). Sensor-cloud architecture: A taxonomy of security issues in cloud-assisted sensor networks. *IEEE Access, 9*, 89344–89359.

Bhushan, B., & Sahoo, G. (2018). Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks. *Wireless Personal Communications, 98*, 2037–2077.

Bordel, B., Alcarria, R., Sanchez de Rivera, D., Martín, D., & Robles, T. (2018). Fast self-configuration in service-oriented Smart Environments for real-time applications. *Journal of Ambient Intelligence and Smart Environments, 10*(2), 143–167.

Chatterjee, S., Ladia, R., & Misra, S. (2015). Dynamic optimal pricing for heterogeneous service-oriented architecture of sensor-cloud infrastructure. *IEEE Transactions on Services Computing, 10*(2), 203–216.

Dabbagh, M., & Rayes, A. (2019). Internet of things security and privacy. *Internet of Things from Hype to Reality, 621*, 211–238.

El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering, 29*(1), 223–246.

Erdelj, M., Król, M., & Natalizio, E. (2017). Wireless sensor networks and multi-UAV systems for natural disaster management. *Computer Networks, 124*, 72–86.

Jan, M. A., Khan, F., Alam, M., & Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems, 92*, 1028–1039.

Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. *Journal of Network and Computer Applications, 137*, 1–10.

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Khan, A. A., Zakarya, M., Khan, R., Rahman, I. U., & Khan, M. (2020). An energy, performance efficient resource consolidation scheme for heterogeneous cloud datacenters. *Journal of Network and Computer Applications*, *150*, 102497.

Khan, F., ur Rehman, A., & Jan, M. A. (2020). A secured and reliable communication scheme in cognitive hybrid ARQ-aided smart city. *Computers & Electrical Engineering*, *81*, 106502.

Khedo, K. K., Bissessur, Y., & Goolaub, D. S. (2020). An inland Wireless Sensor Network system for monitoring seismic activity. *Future Generation Computer Systems*, *105*, 520–532.

Li, J., Cai, J., Khan, F., Rehman, A. U., Balasubramaniam, V., Sun, J., & Venu, P. (2020). A secured framework for sdn-based edge computing in IOT-enabled healthcare system. *IEEE Access*, *8*, 135479–135490.

Li, W., Chai, Y., Khan, F., Jan, S. R. U., Verma, S., Menon, V. G., Kavita, fnm, & Li, X. (2021). A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *Mobile Networks and Applications*, *26*, 234–252.

Liu, Y., Sun, Y. L., Ryoo, J., & Vasilakos, A. V. (2015). *A survey of security and privacy challenges in cloud computing: Solutions and future directions*.

Masood, I., Wang, Y., Daud, A., Aljohani, N. R., & Dawood, H. (2018). Towards smart healthcare: Patient data privacy and security in sensor-cloud infrastructure. *Wireless Communications and Mobile Computing*, *2018*, 1–23.

Muhammad, K., Lloret, J., & Baik, S. W. (2019). Intelligent and energy-efficient data prioritization in green smart cities: Current challenges and future directions. *IEEE Communications Magazine*, *57*(2), 60–65.

Olakanmi, O. O., & Dada, A. (2020). Wireless sensor networks (WSNs): Security and privacy issues and solutions. *Wireless Mesh Networks-Security, Architectures and Protocols*, *13*, 1–16.

Parast, F. K., Sindhav, C., Nikam, S., Yekta, H. I., Kent, K. B., & Hakak, S. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*, *114*, 102580.

Ray, P. P., & Kumar, N. (2021). SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. *Computer Communications*, *169*, 129–153.

Sharma, S., Chang, V., Tim, U. S., Wong, J., & Gadia, S. (2019). Cloud and IoT-based emerging services systems. *Cluster Computing*, *22*, 71–91.

Vol. 9, No. 02; 2024

ISSN: 2456-3676

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: Issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532.

Tian, W., Yang, L., & Weiwei, F. (2022). A comprehensive trustworthy data collection approach in sensor-cloud systems. *IEEE Transactions on Big Data*, *8*(1), 140–151.

Yao, W., Yahya, A., Khan, F., Tan, Z., Rehman, A. U., Chuma, J. M., Jan, M. A., & Babar, M. (2019). A secured and efficient communication scheme for decentralized cognitive radio-based Internet of vehicles. *IEEE Access*, *7*, 160889–160900.

Yu, X., Zhan, D., Liu, L., Lv, H., Xu, L., & Du, J. (2021). A privacy-preserving cross-domain healthcare wearables recommendation algorithm based on domain-dependent and domain-independent feature fusion. *IEEE Journal of Biomedical and Health Informatics*, *26*(5), 1928–1936.

Zakarya, M., & Gillam, L. (2019). Managing energy, performance and cost in large scale heterogeneous datacenters using migrations. *Future Generation Computer Systems*, *93*, 529–547.

Zhang, M.-Z., Wang, L.-M., & Xiong, S.-M. (2020). Using machine learning methods to provision virtual sensors in sensor-cloud. *Sensors*, *20*(7), 1836.