Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks

Anupam Chaudhary, Ankur, Kartikaya Dwivedi, Omkar Hedge, Saurabh Singh, *Student, IIT BHU*

[1]

***Abstract*—The orchestration of cloud computing with wireless sensor network (WSN), termed as sensor-cloud, has recently gained remarkable attention. It enhances the processing and storage capabilities of the resources-constrained sensor networks in various applications such as healthcare, habitat monitoring, battlefield surveillance etc. The diverse nature of sensor network applications processing and storage limitations on the sensor networks, which can be overcome by integrating them with the cloud paradigm. Sensor-cloud offers numerous benefits such as flexibility, scalability, collaboration, automation, and virtualization with enhanced processing and storage capabilities. However, these networks suffer from limited bandwidth, resource optimization, reliability, load balancing, latency, and security threats. Therefore, it is essential to secure the sensor-cloud architecture from various security attacks to preserve its integrity. The main components of the sensor-cloud architecture which can be attacked are: (i) the sensor nodes; (ii) the communication medium; and (iii) the remote cloud architecture. Although security issues of these components are extensively studied in the existing literature; however, a detailed analysis of various security attacks on the sensor-cloud architecture is still required. The main objective of this research to present state-of-the-art literature in the context of security issues of the sensor-cloud architecture along with their preventive measures. Moreover, several taxonomies of the security attacks from the sensor cloud's architectural perspective and their innovative solutions are also provided.**

***Index Terms*—Sensor-cloud architecture, security, wireless sensor networks, Internet of Things.**

I. INTRODUCTION

A wireless sensor network is made up of many tiny sensor nodes that are spread out over the sensing environment and collect a lot of data. They are exposed to a wide range of difficulties when sending such a massive volume of raw data through the network, including low quality of service (QoS), which includes latency, congestion, throughput, and security in these resource-constrained networks. They have restricted memory, processing, communication, and, most crucially, a restricted supply of unreplaceable energy. A new computing paradigm known as sensor-cloud is created by combining the wireless network with cloud computing to solve the aforementioned restrictions.

An architecture that enables completely ubiquitous computation employing sensors as an interface between the physical and digital worlds and the Internet as the communication medium is known as a sensor cloud. Most resource-intensive functions, such as processing, storing, and data aggregation, are moved from resource-constrained sensor networks to the cloud architecture in the sensor cloud. This improves QoS, increases network lifespan, and allows users to gather quickly, store, access, process, display, and analyse massive amounts of sensory data utilising enhanced cloud computing resources.

However, sensor-cloud offers several benefits such as flexibility, scalability, collaboration, automation virtualization with better processing and storage capacities, and so forth. However, they suffer from a number of restrictions, including resource scheduling, Quality of Service, load balancing, and, most significantly, security and privacy. As a result, 49% of firms are postponing sensor-cloud implementation owing to security concerns. As a result, security remains a major barrier to widespread sensor-cloud use.

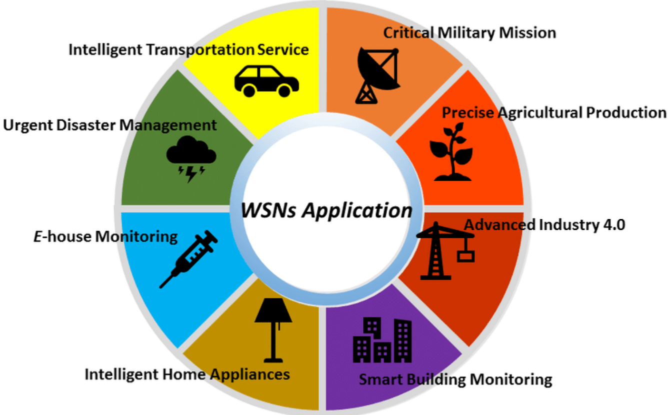

WSNs Application
Critical Military Mission
Precise Agricultural Production
Advanced Industry 4.0
Smart Building Monitoring
Intelligent Home Appliances
E-house Monitoring
Urgent Disaster Management
Intelligent Transportation Service

Fig. 1 Application of Wireless Sensor Networks(WSN)

Sensors, communication mediums, and cloud architecture are the major components of the sensor cloud, with each component accountable for a certain duty. Despite their importance, these components are vulnerable to various security vulnerabilities.

The purpose of this article is to provide a complete assessment of potential security attacks on these separate components as well as their countermeasures.

II. SECURITY AND PRIVACY ISSUES IN THE SENSOR-CLOUD

Sharing resources is simpler by the sensor cloud. Multiple users can develop their sensing applications simultaneously in these networks. By allowing the sharing of computational,

[1]

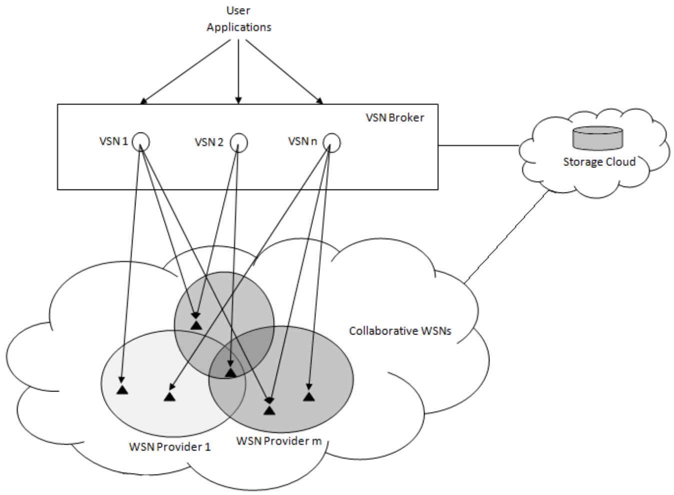


Fig.2 Sensor Cloud Architecture

sensing, and network resources across several users and applications, it provides a multi-user, on-demand sensory system. Despite the advantages of sensor clouds, the security problem still exists, primarily because the general public can utilize this infrastructure for various purposes. As a result, it is hampered by inherent security and privacy concerns in the sensor-cloud infrastructure.

Multiple WSNs make up a sensor cloud, which is a service offered to consumers by the sensor cloud middleware platform. The WSNs are made up of inexpensive nodes that are ad hoc distributed over a huge region to gather qualities like temperature, humidity, and other delicate environmental data as required by a user's application. These deployments may take place in danger zones where they are not continuously observed physically. The possibility of attacks also grows with the integration of WSNs with various ownership entities under a sensor cloud platform that runs a range of user apps. This is due to the reason that well-known conventional security techniques like robust encryption and privacy-preserving measures cannot be adopted and put into practise due to the resource-constrained nature of sensor nodes (in terms of memory, computing power, and energy).

We give a taxonomy of cybersecurity threats on the three elements of the sensor-cloud architecture—**sensors, the communication channel**, and the **cloud framework**. Individual subsections for these three elements go into further depth.

III. SECURE THE SENSOR NODE

Physical security measures or approaches for authorisation and authentication can both be used to protect a sensor node. Restriction of remote access to physical location of deployed sensor nodes falls in the category of physical security measures. Giving permission only to appropriate users or nodes falls in the category of logical security techniques.

IV. SECURE THE COMMUNICATION CHANNEL

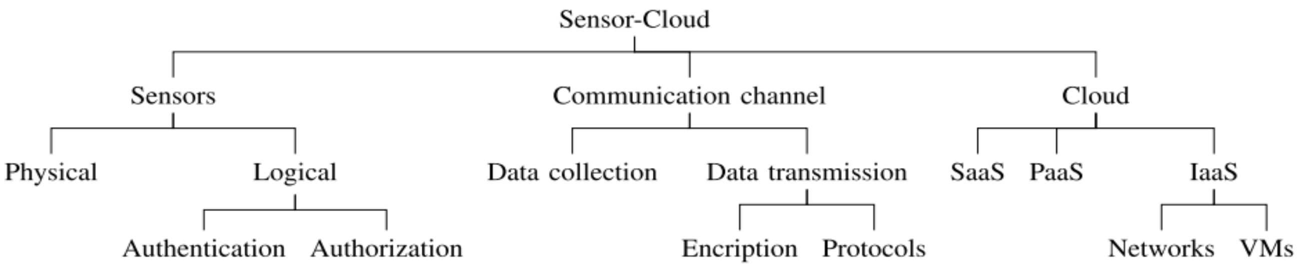
Measures to secure the communication channel broadly classified in two categories : (i) attacks and countermeasures during data collection at the sensor node; (ii) attacks and countermeasures during secure data transmission

(i). ATTACKS AND COUNTERMEASURES DURING DATA COLLECTION AT THE SENSOR NODE

a. Device tampering attack : The actual node is changed into a fraudulent node in device tampering attacks so that hackers can access sensitive information flowing through it or being saved in the node's buffer.
b. Jamming attacks : In jamming cyberattacks, the attacker uses a powerful jamming source to try to stop the network's and the sensor nodes' regular operation. The source of the jamming uses the same radio frequency as the sensor network to broadcast radio signals. Frequency hopping strategies can be used to prevent jamming attacks.
c. Denial of Service (DoS) attacks: The attacker node (acting as a normal node) uses all the resources during these assaults. All resources were monopolised by the attacker, preventing authorised users from using the network's resources, applications, and services.

(ii). ATTACKS AND COUNTERMEASURES DURING SECURE DATA TRANSMISSION ON THE WIRELESS CHANNEL

a. False routing : This kind of attack involves inserting fake routing information in order to attack the routing table. It gets overloaded with erroneous data, resulting in routing table overflow.
b. Packet replication : Attackers replicate the packets they receive and then send them on to other nodes during packet replication assaults which slow down performance of network.
c. Black hole attacks : The infected node serves as a black hole in these attacks. It receives all incoming network traffic and refuses to further forward it to the other nodes. This causes network traffic to be rerouted towards the malicious node.
d. Sink hole attacks : In sinkhole attacks, a single corrupted node is used to divert all network traffic to the hacked node.
e. Worm hole attacks : A packet is acquired at one site and sent via a tunnelling mechanism from the other site in a wormhole attack. The identical packet then begins transmission from its new site back into the network.



f. Selective packet forwarding : During these assaults, the malicious nodes retain a few chosen messages while the others are sent over the network. This hinders the accuracy and trustworthiness of the overall system.

g. Spoofing Attacks : In spoofing exploits, the perpetrator launched many attacks while acting as an authorised user. By exploiting the login information of legitimate users, they create a false profile. By changing the routing information, introducing routing loops, producing misleading alerts, these attacks severely affect network traffic flow.

h. Node replication attacks : Attackers install a malicious node by using the Identity of the actual nodes in node replication attacks. By delivering incorrect routing information, these attacks interfere with the functioning of the network.

i. Passive information gathering : Phishers track out the sensor node, identify it in the network, and comprehend the signals being sent there. They can initiate many assaults after finding the node, such as harming the sensor node.

j. Sybil attacks : A hostile node impersonates a number of legitimate nodes concurrently in a Sybil attack, which has an impact on entire network performance.

k. Smurf attack : A significant quantity of the ICMP queries in these assaults are sent to the target node. The victim node responds to these requests by sending an infinite number of ICMP answers, which chokes and shuts down the entire network.

V. SECURING DATA AT THE CLOUD PLATFORM

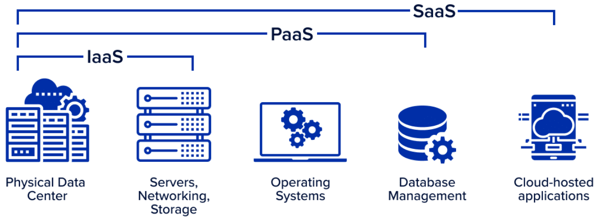


Fig.3 Cloud Service Models

1) **SOFTWARE AS A SERVICE (SaaS)** : In this model, the complete application package is hosted at the cloud server. It is offered to an unlimited number of individual clients as a service on demand.A brief account of various security attacks on the SaaS platform is provided below:

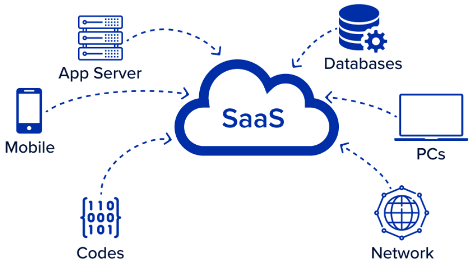


Fig.4 SaaS Model

a) **denial of service (DoS) attacks** : A massive amount of demands are made of the targeted system and resources during a denial-of-service attack, negatively affecting their ability to function normally. The attackers transmitted a huge number of unnecessary packets that are more than the network and server can handle. DoS attacks can result in buffer overflow, packet loss, congestion, and the waste of the network's usable resources.

b) **distributed denial of service (DDoS) attacks** : An excessive number of Internet bots are used in DDoS assaults to bombard a particular application, server, or network with requests. These networks are unable to provide services to authorised users as a result. A denial-of-service response plan, a secure network architecture, and a threat detection strategy are all included in the all-encompassing defence approach. The sharp decline in network performance or an increase in spam are two indicators that these assaults may have occurred.

c) **sql injection attack** : Attackers introduce malicious malware onto SQL servers to execute and alter SQL instructions. These operations can even remove individual rows, whole tables, or even the entire database in some cases.

d) **authentication attacks** : Attackers attempt to steal the identities of the authorised users who are used for authentication in these attacks. Such information is used by the attackers to get access to users' private information and confidential data. Other security threats including bypass attacks, brute force assaults, session eavesdropping, replay attacks, and keylogger attacks can result from authentication attacks.

e) **cross site scripting attacks**: These assaults typically target software designed for the web. The offender often adds certain client-side scripts into online programmes that seek to discover the credentials of authorised users. They then conduct different security attacks using this information.

2) **PLATFORM AS A SERVICE (PaaS) :** In this arrangement, cloud service providers give consumers access to some software and development environments. The consumers benefit from increased scalability and management as a result. Below is a list of a few typical PaaS security threats.

PaaS
Platform as a Service

Fig.5 PaaS Model

a) **phishing attacks** - In phishing attacks, the attackers typically attempt to get access to and steal sensitive data from authorised individuals through emails. It is a significant source of identity theft and a preferred method of assault. Opening such an email might result in the installation of malware, which would harm files, the system as a whole, and give access to private data.

b) **man in the middle attack**- In this assault, the attacker tries to listen in on the two parties' conversations—which may be virtual machines—to see what information they are exchanging. This has caused the private information they shared to leak, which may then be used as a springboard for subsequent security assaults.

c) **cloud malware** - By impairing the server's functionality, this assault changes data and a number of features. SQL Injection and Cross-Site Scripting are two of the most prevalent malware injection attacks (XSS).

d) **password reset** -In order to deceive the victim into requesting a password reset, the perpetrator attempts to persuade her to register for a service that the attacker controls. These services range from format conversion to free downloads, among others. The attacker then makes use of this registration information to get access to the victim's numerous accounts across several platforms before changing their passwords.

e) **programming flaws** - A software programme can have a fault if it has a problem, a weakness, or even an error. When this happens, the Software may perform strangely or even crash, posing a serious security risk. These holes might serve as the starting point for a number of security assaults. Attackers can therefore conduct a variety of assaults that have unexpected time and financial consequences.

f) **application security** -Mission-critical applications employ WSNs. Periodically, the sink node receives the collected data for processing. The sink node serves as a gateway to enable the transfer of gathered data to the cloud. The attackers often attempt a variety of security assaults against different apps, including overwhelm, repudiation, data corruption, and malicious code. Attacks like this have a negative impact on the network's performance and use up its meagre energy and bandwidth

3) **INFRASTRUCTURE AS A SERVICE (IaaS) :** These services transform the capital cost into operational cost for any organisation. Different IaaS service types are offered in terms of storage, compute

and other resources. Instead of being centralised, these services are delivered to each user individually. Below is a list of a few typical security threats on IaaS/HaaS.

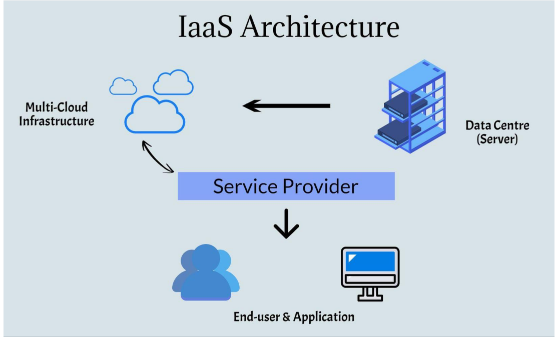


Fig.6 IaaS Model

a) **stepping stone** : In this kind of attack, the perpetrator typically conceals their identity using a number of methods. Discovering the suspect's identification is exceedingly challenging.

b) **virtual machine escape** : This type of attack specially focus on virtual machines. As a result, all virtual machines and the operating system that hosts them are completely accessible to the attackers.

c) **Side channel attacks** : The attacker obtains data from the system's implementation at the level of design. They take advantage of the network flaw and get the system's information and use it to attack again.

d) **malicious insiders** : When an insider uses up all of the system's data storage and compute power, a malicious insider attack happens. These attacks have the potential to seriously harm the performance of system.

e) **VM rollback attacks** : These attacks include the perpetrator disabling a few security updates or ignoring some security checks. Like, an attacker may use a brute-force method to try to guess the Virtual Machine login credntials. The reply attacks, in contrast to the roll-back attacks, involve the attacker sending the VM the same earlier data repeatedly. Whereas Roll-back assaults result in a response from the VM.

f) **cross VM attacks** : In this type of attack the perpetrators focus on multi-tenant virtual systems. By rerouting network traffic, the attackers exploit a single virtual machine to attack additional virtual machines on the same hypervisor. The cache memory is the major area of attack. Along with the network, they also want to compromise the processor, main memory, and input-output devices.

g) **session hijacking** : During these assaults, the attacker obtains unauthorised access to data contained in cookies that is necessary for session setup. Once the perpetrator has access to this data, it gives them the authority to use the network in any way that an actual user might, endangering its security.

h) **Distributed denial of service(DDoS) attacks** : An intruder's goal in a DDoS assault is to confuse the system to prevent regular functioning through preventing the network's access to its resources. To conduct DDoS assaults, the intruders often use a huge number of bots. To initiate such assaults, these intruders typically use a defect, weakness, or well-known insecurity in software.

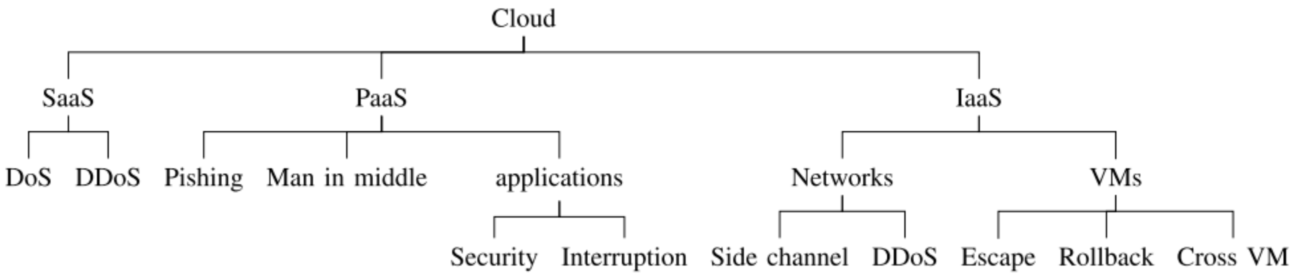
i) **Theft-of-service attacks** : In Theft of service attack a VM which is malicious misbehaves to hack the hypervisor, which assigns more capabilities in term of resources than VM is authorised to get. It results in reduction in system performance and increment in price.

VI. COUNTERMEASURES AND CONTROL

It is a difficult challenge to secure the sensor-cloud architecture. Because a safe system is a holistic blend of rules, technology, and people, it must be controlled as a whole. The following are a few alternative strategies for securing this architecture against various security risks and assaults.

a) The main advantage of the sensor-cloud is that it moves resource-intensive tasks like processing and storage from centralised to distributed architecture. Although this change in tasks has many advantages on the one hand, it also introduces several security risks on the other. Due to the transfer of such data from numerous geographical regions and servers to servers, end-to-end encryption is particularly desirable.

b) Despite this, end-to-end encryption is extremely successful at protecting data from hostile actions. It does, however, bring additional hazards. The fact that encrypted data is unreadable by the firewall and intrusion detection system is one such danger.Thus,



novel countermeasures and preventive measures, such as intrusion detection systems (IDS) and firewalls, should be developed to distinguish real encrypted data from malicious data once it reaches these points.

c) The cloud helps users by moving a few resource-intensive activities from a platform with limited resources to one with abundant resources (sensor to fog, sensor to distant cloud, fog to cloud). The verification of true and legitimate users from intruders and hackers, however, is one of the difficult problems in these systems.

d) Interfaces and APIs are crucial elements of cloud architecture. They provide administration, orchestration, and automation. By monitoring malicious interfaces and APIs, security issues must be identified, managed, and mitigated.

e) The majority of assaults on the sensor-cloud architecture are security attacks carried out by insiders. Due to their extensive understanding of the business process and different network components, former workers of the organisation also offer a severe security danger. They could have a detrimental impact on the information system's privacy and security features. Because of their dual function, insiders are challenging to identify. For monetary advantage, these attackers serve as agents for the competing groups. To protect their business from such threats, cloud companies must take preventative steps including user authentication and bolstering internal security systems.

f) Due to the multi-tenancy approach, 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.

g) It is essential to maintain track of any security assaults and lapses that have occurred in the past and document how that organisation has responded to such instances. This is crucial since these records serve as a reference for the company should any future security breaches like this one. Once future security risks and assaults are predicted, machine learning-based approaches may be used to analyse the tracked and recorded data to activate the proper avoidance mechanisms.

VII. CONCLUSION

In this paper, we focus our discussion on one of the important and challenging issues of security in the sensor-cloud architecture. A state-of-the-art taxonomy of security attacks on the sensors-cloud is also presented. These security attacks are categorized based on the sensor-cloud's architectural perspective targeting various components of this architecture and securing them from security attacks.

We expect that security and privacy shall be accounted for at the preliminary design stage of the IoT systems to evade the common drawback of seeing security as an afterthought. Though pursuing the position of intelligent objects is considered a concealment violation; however, it may also have some beneficial cases, i.e., security agencies depend on chasing the smart objects carried by a missing person to identify the location of the missing person. Such kinds of digital forensics in the IoT era will play an important role and is expected to receive further attention in the future.

VIII. REFERENCES

1. *R. Alturki et al., "Sensor-Cloud Architecture: A Taxonomy of Security Issues in Cloud-Assisted Sensor Networks," in IEEE Access, vol. 9, pp. 89344-893
59, 2021, doi: 10.1109/ACCESS.2021.3088225.*

2. R. M. A. Haseeb-Ur-Rehman et al., "Sensor Cloud Frameworks: State-of-the-Art, Taxonomy, and Research Issues," in IEEE Sensors Journal, vol. 21, no. 20, pp. 22347-22370, 15 Oct.15, 2021, doi: 10.1109/JSEN.2021.3090967.

3.Zhang, Zeyu & Mehmood, Amjad & Shu, Lei & Huo, Zhiqiang & Zhang, Yu & Mukherjee, Mithun. (2018). A Survey on Fault Diagnosis in Wireless Sensor Networks. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2794519.

4.A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, "A survey on sensor-cloud: Architecture, applications, and approaches," Int. J. Distrib. Sensor Netw., vol. 9, no. 2, Feb. 2013, Art. no. 917923

5. S. Madria, V. Kumar, and R. Dalvi, "Sensor cloud: A cloud of virtual sensors," IEEE Softw., vol. 31, no. 2, pp. 70–77, Mar. 2014.

6.S. K. Dash, J. P. Sahoo, S. Mohapatra, and S. P. Pati, "Sensorcloud: Assimilation of wireless sensor network and the cloud," in Proc. Int. Conf. Comput. Sci. Inf. Technol. Berlin, Germany: Springer, 2012, pp. 455–464.

7.M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," Future Gener. Comput. Syst., vol. 92, pp. 1028–1039, Mar. 2019.