Hybrid Cloud Network Security Issues and Challenges for Sensor as a Service in Virtual Sensor Networks

Nishant Tripathi[1], Charanjeet Singh[2] and Kamal Kumar Sharma[3]
[1]Department of Electronics and Communication Engineering, School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara, Punjab (India)
Department of Electronics and Communication Engineering, Pranveer Singh Institute of Technology, Kanpur
phd.nishant17@gmail.com
[2]Department of Electronics and Communication Engineering, School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara, Punjab (India)
rcharanjeet@gmail.com
[3]Ambala College of Engineering and Applied Research Devsthali, Ambala Cantt – Jagadhari Road, P.O. Sambhalkha Ambala, Haryana, India
kamalsharma111@gmail.com

Abstract

In recent years, the desire to have a large amount of storage capacity combined with well-organized scalability created a pushing and engaging driving force behind the migration of various enterprises, organizations, and small businesses from standalone execution to different types of Cloud like private, public and hybrid along with Fog, edge, and containers. The Wireless based sensor network and their data storage Security in different types of Cloud, Computing systems are the primary focus of this work, with users' privacy being protected from attackers as a secondary objective. As sensor networks are now coming to a new era of virtual sensor networks (VSN) with Cloud services getting added to Sensor networks, the online database is growing exponentially. With the emergence of Sensor as a Service (SaS) in cloud applications the focus of each storage and computing model is on protecting sensor-based data belonging to users and their privacy from thwarting cyber-attacks. It is also critical to ensure data integrity for cloud-based storage which has to be maintained. This research article provides takes a systematic approach to review comparative analysis provided by various authors and the security threat at different layers of open system interconnections for service providing and privacy aspects on hybrid Cloud storages and service applications in Sensor as a Service for Virtual Sensor Networks based on Wireless sensor networks.

Index Terms: Cloud Computing, Network Security, Data Security, Hybrid Cloud

DOI:10.48047/ecb/2023.12.si6.673

1. INTRODUCTION

Historically, Cloud service-based customers have had rightful admission to their personal information and data. Several important security and privacy concerns are raised, and they can be addressed on a random basis and order: The preservation of privacy, as well as the integrity, accountability, confidentiality, and availability of the cloud-based storage and network application, has always been targeted by the researchers [1].

The sensor cloud is a cloud platform that can be used to get, store, and analyze a lot of different types of information. The major cause for introducing the idea of a sensor cloud is to let a user- organization not know where the sensor nodes are in real life through virtualization. Virtualization creates a complete abstraction of the primary physical Member sensor nodes [2]. It doesn't matter what the physical topology looks like, it looks like the same topology of sensor nodes, but this one is built on the cloud. Thus, the architecture for a sensor cloud doesn't matter how the resources are arranged or where they are. The most important thing that makes applications work in a sensor-cloud environment is that everyone who has an application can use sensor nodes, even if they don't own any sensor nodes. The use of a sensor cloud also cuts down on the extra work that a user of a Wireless Sensor Network (WSN) has to do because of maintenance,

replacement, redeployment, and other hardware-management costs. As a result, unlike the WSN, every user organization thinks of sensors as a service, not as a piece of hardware.

Sensor-as-a-Service (SaS) is also a lot cheaper than traditional WSNs. Thus, a user organization doesn't have to pay a lot of money at the start to set up and manage the system. From a billing perspective, Se-as is broken down into units that can be measured. Users are charged only for the units that they use. This pay-as-you-go model is good for the sensor cloud as a whole. The current article presents a theoretical model to counter the threat and network security in the Hybrid cloud. In any wireless sensor network, virtualization with common features at the end user has provided the Virtual sensor network concept. The virtual sensor network concept works on the principle of Sensor as a service, in the cloud domain post-virtualization of the physical abstraction of any wireless sensor network. So, in the current article, see how the threats and network issues looming around hybrid cloud w.r.t Sensor as a service, then types of network characteristics, followed by hybrid cloud model for the sensor as a service in Virtual Sensor Network. The mid part of the article illustrates the types of security issues in different layers of networking, and then a comparative analysis of threats and their prominent solution for different types of cloud models for Sensor as a service. The last part will be having a conclusion and discussion. Table 1 describes the abbreviations used in this paper.

Table 1 Abbreviations and Key Terms used

WSN	Wireless Sensor Network
AES	Advanced Encryption Standard [3]
NAP	Network Access Point [3]
CSA	Security Auditor for Cloud [3]
DDoS	cloud-based Distributed Denial of Service request [3]
DoS	cloud-based Denial of Service Request [3]
HTTP	Hypertext Transfer Protocol [3]
IaaS	Infrastructure as a service in cloud computing [3]
IBC	Identity-Based Cryptography in data security [3]
IBE	Identity-Based Encryption for data transmission [3]
IDS	Intrusion Detection System for data reception [3], [4]
IoWT	Internet of Wearable Things for 6 G-based communications in different networks [2], [3], [4]
MAC	Medium Access Control for Layers in OSI Model [3]
MITM	Man-in-the-Middle Attack for layered network architecture [3]
OS	Operating System for host or guest [3]
OSI	Open Systems Interconnection model for networking [3], [4]
PaaS	Platform as a Service for cloud computing [3]
PKI	Public Key Infrastructure for security prospects [3]

PRISMA is described through network- based and cloud computing model salutation giving Preferred. Reporting Items for Systematic Reviews and Meta-Analyses [1-4]	
SaS	Sensor as a Service in Virtual sensor networks using cloud computing [3]
SLA	Service Level Agreement by Service provider in cloud computing [3],[4],[5]
SSL	Secure Socket Layer [3]
SYNC	Synchronize message [3]
TLS	Transport Layer Security for layered transmission [3]
UDP	User Datagram Protocol for OSI-based networking
VM	Virtual Machines used in Cloud computing
WAF	Web Application Firewalls for cloud-based services [3]

In today's complicated cyber security world, threat detection alone won't be enough to keep hybrid cloud assets safe. If one wants to protect someone from both known and unknown threats, one needs multiple layers of real-time protection (zero-day). The solution must be able to provide rough and bottomless transfer examination and better threat intellect which separates suspicious traffic until it can be barren.

After a threat has infiltrated the corporate network, it puts the organization's assets at risk from cyber threats that are too high. To stay one step ahead of hackers, threats, including zero-day and other quick exploits, must be caught, and killed before they can get into the network. This level of advanced prevention is only possible if one uses a complete security solution that uses advanced methods on many different levels to keep things safe. Most importantly, a more complete cloud network security solution reduces the chances of a cloud breach and lessens the impact and damage if one does happen. One management interface, or "single pane of glass", should be both a source of truth for cloud network security and a command-and-control tool. This is called "unified management".

How important is this? With a lot of different security tools from different vendors or for different environments, security teams can't protect the whole company. This requires a wide range of different skills, but it also leads to policy and process gaps that let threats get through. Easy to use and work with the solution must be able to work with the organization's configuration management system.

In addition, the answer must be able to work well with cloud providers' services. The optimum objective is supposed to be to make things easier and more usable by cutting down on the number that security solutions that have to be installed and managed separately.

How important is this? Integration is important for some other reasons, such as being able to run borderless operations and making it easier for people to find someone. It is very important to have a cloud security platform that covers not only infrastructure security but also application security, cloud security posture management, and other things. It also helps make things easier to use because configurations and tasks can be done with the fewest possible clicks and navigation through complicated interfaces.

Visibility: - The dashboards, logs, and reports of the solution should give a complete picture of what's going on in real-time. They should also be able to give the information that one can act on.

How important is this? What can't see can't be kept safe at the very core of things. What one sees is also easy to understand and context-aware, which means that it connects to all the signals, events, and data streams that they look at.

Security Management that is aware of context: - Hybrid Cloud-based network security solutions have to be capable to unite and link data from public and private clouds, as well as from on-premises networks, to make sure that security policies are context-aware and consistent across all networks. It should be easy for changes to the

configuration of a network, an asset, or the security group that governs them to show up in the security policies that apply to them. How important is this? Integrating and automating security policies across a wide range of complex environments is important for smart and consistent management. Security platforms need to be able to quickly publish changes and adapt to security policies as they change. Asset, change, and configuration management frameworks play a big role in resolving vulnerabilities.

2. HYBRID CLOUD NETWORK SECURITY BACKGROUND

It has become clear that safe and secure transfer of information has emerged as a significant face up to the whole industrialized section in recent years. A better, healthier, and more secure association of networks can be considered for an organization or industry by utilizing network security tools, and attacks and network security measures define how this can be accomplished. It is the goal of this research to identify and address issues that can be addressed to increase the efficiency with which network security is managed.

2.1 Hybrid Cloud Security Methods for SaS in Virtual Sensor Networks

a. Cryptography: - There are mathematical functions called ciphers that are used in cryptography. These mathematical functions are used to encode and decode a message.

b. Firewalls: - *a* collection of workings or attributes that effort jointly to create a barrier between two networks.

c. Cloud Application Gateways: - A cloud application gateway is the first firewall in a cloud environment. It is also referred to as a proxy gateway, which is what it appears to be on the outside. Because they are made up of bastion hosts, they do perform the function of a proxy server, but they are not one. According to the ISO/OSI Reference Model, this software is used to run applications at the Application Layer. For clients behind a firewall to be able to connect to the Internet, they must first be organized and prioritized.

d. Packet Filtering: - Packet filtering is a technique that uses ACL (Access Control Lists) to allow packets to pass through routers that have been configured to filter them. According to the diagram, a router will by default pass through all traffic that is directed through it without imposing any restrictions. It is possible to define what types of access to the internal network are permitted for users from the outside world, and vice versa, using ACLs (Access Control Lists). Figure 1 depicts the hybrid cloud storage with cache memory organization with data security levels.

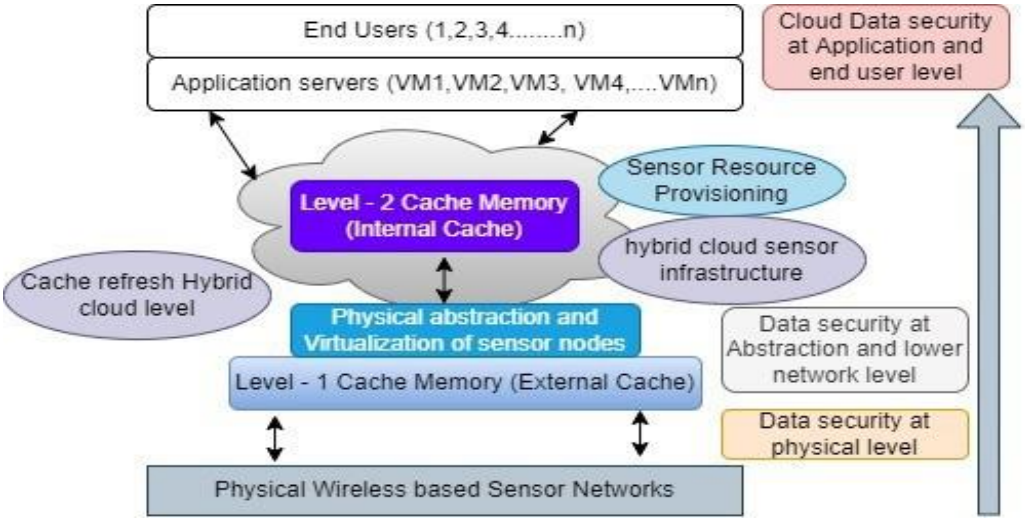

Figure 1 Hybrid Cloud Storage with cache memory organization with data security levels

Hybrid cloud storage has to have an upper-shown structure with three different levels of network security. One level will secure data security at the physical level, while the second level of data security is at the MAC layer of the cloud-based model. The topmost layer will have cloud data security at the application and end-user levels.

Mid-level will have 2 virtual cache memory concepts within the cloud to fasten the resource pooling while maintaining the integrity of the database.

Some systems join the safety measures of application layer gateways with the ease and speed of packet filtering to try to find a better balance between the two. In some of these systems, the application layer is in charge of making sure that new connections can be authenticated and approved. This is then followed by the transfer of all remaining data to the session layer, where packet filters keep an eye on the connection to make sure only packets that belong to an ongoing (and already approved) conversation are sent through the network.

A general threat by an attacker who is trying to get into the network through this method will have to get through an access router, a bastion host, and a choke router before they can get to services on the inside network.

3. HYBRID CLOUD GUARD FOR SENSOR AS A SERVICE

Check Point's Cloud Guard platform protects all of the assets and workloads across all multi-cloud environments, giving the power to automate security, stop threats, and manage performance. This is what Cloud Guard is all about Cloud network security. It's a virtual appliance that allows to use Check Point's advanced threat prevention and industry-leading catch rate in the dynamic and scalable cloud environment. It is made for easy use on cloud platforms and software-defined data centers. An appliance called Cloud Guard Network Security is a virtual machine that lets it use Check Point's top-notch security in a dynamic and flexible cloud environment. Features and benefits: Cloud Guard Network Security has the following main features and benefits:

By using Check Point's Threat Cloud, Cloud Guard protects businesses from advanced and multilayered threats. Cloud Guard also uses advanced threat extraction and emulation technologies to keep threats from getting through. Cloud Guard can be set up on a wide range of public cloud service providers and software-defined data center solution providers, and it works well with them.

There is a lot of fine-grained traffic inspection and control done by Cloud Guard on both incoming and outgoing traffic, as well as traffic that goes through the firewall. Cloud Guard's next-generation firewall lets it set very specific rules for matching traffic, like excluding traffic, verifying port configurations, and blocking applications at the application level. Network security that is automated and can be changed quickly: Objects and security groups that are defined by the cloud are always being updated, and security policies are automatically changed to reflect changes in the cloud environment. Besides that, Cloud Guard encourages the use of automation to deal with threats, remediate them, and run workflows.

Cloud Guard works with the best tools for configuration management, Infrastructure as Code, and continuous integration and delivery (CI/CD) through APIs. Cloud Guard is also very well-integrated with cloud-based tools and services, as shown below Consolidates log data from across the network and changes IP addresses to cloud object names so that network security and forensics can be more easily seen and tracked. Remote access to cloud resources is made more secure by Cloud Guard, which requires two-factor authentication for mobile access to the cloud. In addition, Cloud Guard encrypts data that Cloud Guard receives and sends, both ways. To provide highly scalable and dynamic secure remote access, Cloud Guard, for example, uses Virtual Machine Scale Sets (VMSS) on Azure. These are groups of virtual machines that work together to provide high-performance, dynamic, and secure remote access.

Manage context-aware infrastructures in the cloud and on computer or tablet*:* Cloud Guard's unified management console is easy to use, and customers always give it high marks in Check Point's surveys. Keeping track of security events can be done quickly and consistently across the whole environment. Cloud Guard Network Security adds to and complements the security services that cloud providers offer in the following ways. Cloud Guard Network Security is a self-service, automated, and adaptive solution that works with cloud-native security constructs to stop malicious activity in real-time. It works together with Cloud Guard Network Security. Using Cloud Guard, the cloud is protected with enterprise-level granularity, deep inspection, and advanced evasion protection, as well as proactive threat prevention for both known and unknown flaws in the cloud.

Cloud Guard Network Security also allows for truly unified and multi-cloud management of cloud security and compliance through a single management console, which is very important. As soon as the first connection is made, Cloud Guard automatically imports all cloud assets into the console. Cloud Guard security policies and logs are automatically updated when the IP address, name, or location of an instance or VM changes. Policies and logs also use cloud object names to make them easier to find and see, which makes them easier to find and see. A lot of people now use multiple cloud providers instead of just one. Most businesses use two or more cloud providers, according to the Check Point 2020 Cloud Security Report. According to a Gartner survey, more than 80% of respondents said their company runs workloads across multiple clouds. Check Point’s unified security management platform makes sure that all public and private cloud deployments, as well as on-premises deployments, have the

same visibility, policy management, logs, reporting, and control Using this table, one can see how Cloud Guard and the cloud network security solutions of the top cloud security companies compare.

3.1 Considering SaS Cloud security competitors, the Hybrid Cloud Guard is the best choice.

Cost of Ownership: Cloud Guard is the best choice for businesses that already have Check Point on-premises security and are moving to the cloud. It's the easiest, fastest, and most secure cloud network security with the lowest total cost of ownership. Cloud Guard stands out from its competitors because of the following: Anti-virus software is the most secure. It has the best catch rate in the industry when it comes to malware, ransomware, and other attacks. It has the best security effectiveness score with a 100% block rate, 100% malware prevention, 100% exploit resistance, and 0% false positives.

It has been named a long-term leader by third-party analysts. 21 years in a row, Gartner has been named Network Firewall Leader in its Magic Quadrant for Network Firewall, and NSS Labs has named Network Firewall Recommended. Over 28 years of security gateway intellectual property and cyber security technology innovation. Real-time detection and auto-remediation of both known and unknown flaws. When compared to its competitors, how easy it is to use (based on the three standard use cases that were tested). To get more information, please read this document. Cloud instance objects are used to enforce security policies across hybrid and multi-cloud environments automatically and dynamically. Cloud-native services, vulnerability scanners, and SIEM solutions are all part of the enterprise ecosystem that connect and work together very well. There is a seamless integration with Check Point's Cloud Guard platform of cloud security solutions. These include the powerful Cloud Guard Posture Management public cloud security management tool, Cloud Guard Intelligence which monitors and analyses multiple clouds, Cloud Guard Workload Protection which provides full protection for modern cloud workloads including serverless functions and containers, and Cloud Guard App Sec, which automates application security checks.

Network security for hybrid cloud was made for Sensors which are used to protect networks and their services from being changed, destroyed, or leaked, as well as to make sure the network works properly in critical situations without causing harm to the user or employee [6]. In addition, it includes provisions built into the computer network infrastructure, as well as policies set by the network administrator to protect the network and network-accessible resources from being accessed by people who aren't supposed to be there. Network security design constraints can be summed up as:

Hybrid Cloud Security Attacks Hybrid cloud Security attacks preferably for Sensor as a service for virtual sensor networks can be classified under the following categories:

Passive Hybrid cloud threats/Attacks

The attack makes use of experiential information to negotiate the system. Plain text attacks are an example of a passive attack in which the attacker is already aware of both plain text and cipher text.

Active hybrid cloud threats/Attacks

This type of attack requires the attacker to send data to one or both of the parties or block the data stream in one or both directions [7,8]. The attributes of active attacks are as follows,

Disruption can be defined as attacks on the accessibility of services, such as denial-of-service attacks. Modification compromises integrity.

Fabrication is an assault on authenticity.

"Man-in-the-middle" attacks and other forms of interception are used to compromise confidentiality. An attack on confidentiality or anonymity is made possible through traffic analysis. Traceback on a network and CRT radiation are examples of what can be included.

4. CONSIDERATION FOR HYBRID CLOUD-BASED NETWORK SECURITY FOR VIRTUAL SENSOR NETWORKS

- Scalable without bounds
- Remote access with confidentiality
- Traffic on a local level

- Control and surveillance
- Context-aware
- Management of security
- Automation
- Assistance to vendors
- Recognizing the industry
- Arrangements for
- Affordability
- Ownership costs total

Cloud Computing Security in the Hybrid Cloud: Advanced Threat Prevention and Comprehensive Protection Threat detection alone will not be sufficient to protect hybrid cloud assets in today's complex cyber security landscape. To protect against both known and unknown vulnerabilities, it must implement multilayered, real-time threat prevention (zero-day). Furthermore, these advanced capabilities must be deployed on both incoming and outgoing north-south traffic as well as east-west (lateral) traffic in both directions. Detecting a threat after it has infiltrated the corporate network exposes the organization's assets to an unacceptably high level of cyber security risk, putting the entire organization at risk. It is necessary to capture and neutralize threats before they can gain access to a network to stay one step ahead of malicious actors. This includes zero-day and other agile exploits. It is only through the use of a comprehensive security solution that employs advanced methodologies across multiple layers that this level of advanced prevention is made possible. First and most importantly, an improved overall level of Cloud Network Security reduces the likelihood of a cloud breach occurring as well as the impact and damage if one does.

Borderless: Regardless of how complex the hybrid (public/private/on-site) or multi-cloud environment is, the solution must operate transparently and consistently across all of them. To what extent is this significant? Security teams are unable to provide enterprise-grade protection when they are working with a fragmented stack of vendor-specific or environment-specific tools. This, in addition to necessitating a wide range of specialized skill sets, will inevitably result in policy and process gaps that will allow threats to slip through the cracks.

Context-Aware Security Management System: For security solutions to be effective, they must be able to aggregate and correlate data across the entire environment—public and private clouds, as well as on-premises networks—to ensure that security policies are contextually aware and consistent. Whenever a network, an asset, or a security group is reconfigured, the security policies that govern those configurations should be updated automatically.

Hybrid Cloud Protection Guard: The Highest Level of Hybrid Cloud Network Security: In addition to providing unified cloud-native security for all assets and workloads across multi-cloud environments, Check Point's Cloud Guard platform also empowers to automate security, prevent threats, and manage performance. In the dynamic and elastic cloud environment, Cloud Guard Network Security is a virtual appliance that brings Check Point's industry-leading threat prevention and detection rate to the fore. When deployed on multiple public cloud service providers and software-defined data center solution providers, Cloud Guard can be integrated seamlessly into the overall system architecture.

System-based Automated and agile network security at a huge scale: this is the goal. Cloud-defined elements (asset tags, objects, and security groups) are updated regularly, and security policies are automatically adjusted to reflect changes in the cloud environment as needed. As an added benefit to users, Cloud Guard encourages the automation of threat response, remediation, and workflow management processes. Integration with industry-leading configuration management, Infrastructure as Code, and continuous integration and delivery (CI/CD) tools is accomplished through APIs provided by the Cloud Guard product line. Furthermore, as discussed further below, Cloud Guard is tightly integrated with cloud-native tools and services.

For improved network security visibility and forensics: Cloud Guard consolidates incoming log data from across the enterprise's infrastructure and replaces IP addresses with cloud object names. By requiring two-factor authentication for mobile access, Cloud Guard protects remote access to cloud resources. Data in transit is also encrypted by Cloud Guard, which protects both incoming and outgoing data transmissions.

Cloud Guard, for example, makes use of Azure's Virtual Machine Scale Sets (VMSS) to provide highly scalable and dynamic secure remote access with automatically managed connectivity and load sharing, among other capabilities.

Configuring and managing context-aware infrastructures in the cloud and on-premises: In Check Point's regular customer satisfaction surveys, Cloud Guard's unified management console consistently receives high marks from users. Easy tracking of security events, as well as consistent enforcement of security policies across the entire environment, is possible.

5. HYBRID CLOUD NETWORK SECURITY ARCHITECTURE FOR SENSOR AS A SERVICE IN VIRTUAL SENSOR NETWORKS

As a complement to the security services provided by cloud providers, Cloud Guard Network Security adds to and enhances them in the following areas. A self-service, automated, and adaptive network security solution that works in conjunction with cloud-native security constructs to detect and prevent malicious activity in real-time is Cloud Guard Network Security. In addition to providing enterprise-grade granularity and control, deep inspection and advanced evasion protection, and proactive threat prevention against both known and unknown vulnerabilities, Cloud Guard also protects the cloud from cyber-attacks. Additionally, Cloud Guard Network Security enables truly unified and multi-cloud management of cloud security and compliance through a centralized management console, allowing for greater efficiency and productivity. When connect to the Cloud Guard console for the first time, all cloud assets are automatically imported, and any changes to instance/VM attributes such as IP address, name, or location are automatically reflected in Cloud Guard security policies and logs. Aside from that, cloud object names are used in both policies and logs to improve visibility and searchability.

It is becoming more common to have multiple cloud service providers on a single network. Check Point 2020 Cloud Security Report indicates that 68 percent of organizations use two or more cloud service providers, and a recent Gartner survey found that more than 80 percent of respondents indicated that their organization distributes workload across multiple cloud service providers. All public and private clouds, as well as on-premises environments, are managed with consistency by Check Point's unified security management platform. It also provides consistent visibility, policy management, logging, reporting, and control.

If creating a security cum network architecture of SaS with cloud integration and security features, it will be a 4-level model to address the communication and other relevant issues.

The four levels of the Hybrid cloud-based security model for Sensor as a service in a Virtual sensor network are:

- Lowest level: Physical Wireless Sensor Networks
- 2nd Level: Abstraction Level Gateway Interface
- 3rd Level: Cloud Server and Security Level
- Top Level: End user Server and Security Level

Figure 2 shows the Hybrid Cloud network architecture with security integrations for Sensor as a service in Virtual Sensor Network.

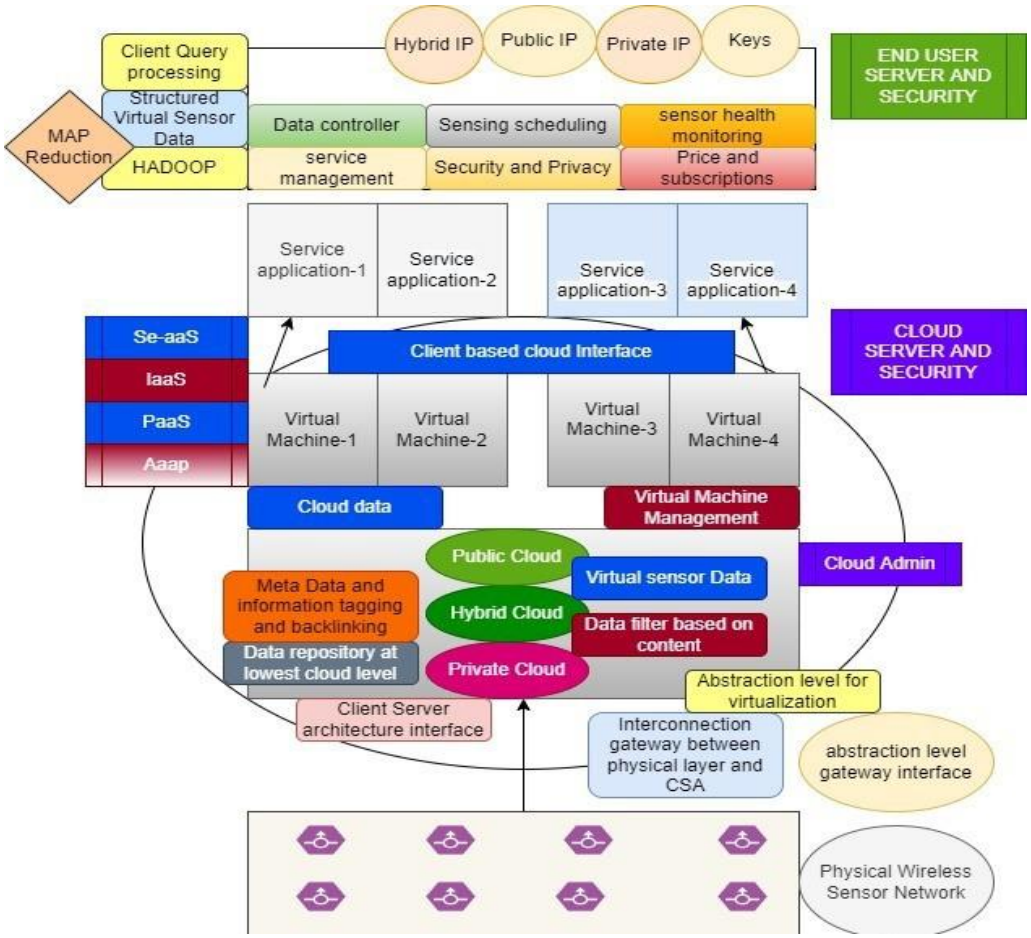

Figure 2 Hybrid Cloud network architecture with security integrations for Sensor as a service in Virtual Sensor Network

Below Table 2 describes the Security challenges and suggestions for several types of cloud-based sensors according to the Open Systems Interconnection model (OSI).

Table 2 OSI layer wise threat issues and Security recommendations for various cloud-based Sensors as a service

Layers of Networking	Network Security issues characteristics for Sensors as a Services	Private Cloud	Public Cloud	Hybrid Cloud
Application Layer	Flood Attacks, Trojan Malwares	Application monitoring is recommended. Application Firewall for web, anti-threat,	Filtering mechanisms and intrusion detection system. Higher Level	HTTP-Redirect scheme

		and antivirus for web. SQL injection detection. Use of Anti-Virus. Better OS Configuration	resource pooling and auditing.	
Transport Layer	Hypervisor Breach, Data Leakage, VMWare Breach	SSL-TSL Encryption is required. Anti-spyware for guest OS is required. Firewall required.	Computational pooling and auditing are needed. Homomorphism encryption. Reduced UDP response rate.	Rapid elasticity, SQL injection and resources pooling.
Network Layer (Upper Session Corrupt MAC)	TCP Flood, UDP Flood	SYNC cache is required. Symmetric protocol encryption.	IBE scheme for mapping. Behavioral assessment	Authentication and intrusion detection mechanism for prevention of collision.
Data Link Layer (Lower MAC)	DoS threat, MIPM, Spoofing Threat	IDS Access is required. Data coding is required. Authentication of identity required.	Network authentication needed. Time based stamping on packet.	Integrated firewalls. Multipurpose authentication. Multi casting in PKI. IBC for identity protection.

Table 3 depicts the Sensor-as-a-service in VSNs using a hybrid cloud architecture that includes an additional layer of network security.

Table 3 Hybrid cloud architecture with Network security add-on for sensor as a service in Virtual Sensor Networks

No.	Levels in the Architecture	Key Components and Attributes
1.	Lowest Level: Physical Wireless Sensors Networks	Sensor Nodes forming a cluster using optimum clustering algorithms, data aggregation at Base Station, and data transmission.
2.	2nd Level: Abstraction Level gateway Interface	Data abstraction over physical level to provide the same to different virtual machine which act as a sensor as a Service.
3.	3rd Level: Cloud Server and Security Level	Three layers of cloud storage and services are available with network level security issues consisting of virtualized data, abstracted data, and physical data.
4.	Top Level: End user Server and Security Level	Client side of architecture with of architecture with SAAS, PAAS, IAAS. Client side of architecture with of architecture with SAAS,

		PAAS, IAAs, and SaS with client-based security and privacy to manage and safeguard cloud data over the network to the end user.

5.1 Hybrid cloud Network Security Measures for virtual sensor networks

- Unwanted visitors should be barred from entering through a powerful firewall and proxy.
- It is recommended that install a powerful Antivirus software package as well as an Internet Security Software package.
- Strong passwords should be used for authentication, and they should be changed on a weekly or biweekly basis, respectively.
- A strong password should be used when connecting via wireless technology. In terms of physical security, employees should exercise caution.
- Obtain an analyzer or network monitor and keep it handy when the situation calls for it.
- Physical security measures, such as closed-circuit television, are being implemented in areas where people enter and exit the facility.
- To keep the organization's perimeter under control, security barriers are put up.
- Fire asphyxiates can be used in areas that are particularly vulnerable to fire, such as server rooms and Security offices.

5.2 Hybrid cloud Network Security Tools for virtual sensor networks

- N-map Scanner is a free and open-source network exploration and security auditing utility that can be downloaded from the internet.
- It is possible to scan the network for vulnerabilities for free using Nessus.
- A network protocol analyzer for UNIX and Windows operating systems, known as Wire Shark or Ethereal.
- When it comes to IP networks, Snort is a lightweight intrusion detection and prevention system that excels at traffic analysis and packet logging.
- A straightforward utility for reading and writing data across Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) network connections, Net Cat is available for free download.

6. LITERATURE REVIEW

Numerous writers have tried this approach and reported their results after a survey of the relevant literature.

Zuo et al., (2013) [9] suggest a hybrid cloud computing architecture that can facilitate a speedy transition from the current IT architecture to cloud computing by cutting costs, streamlining resource integration, and bolstering both business support and IT management. The cloud infrastructure is a hybrid of local private clouds and public clouds of various types. Private clouds and public clouds are structurally identical on the inside, sharing components such as the infrastructure and virtualization layer, the cloud platforms layer, the cloud bus layer, the cloud application layer, the management center, and the storage centers. Web apps and services are deployed and managed on the cloud platform layer, which also facilitates custom app creation and seamless app integration through standard APIs. The cloud bus layer is responsible for managing and monitoring the underlying cloud platform's services; it consists of a control bus, several node buses, and adapters.

Jiang et al., (2018) [10] enhance the interdomain communication performance of many VMs co-located with the same sensor hardware, it offers an improved solution based on shared memory. The method avoids transferring data across the TCP/IP stack at the virtual network interface by instead storing it in shared memory pages managed by the hypervisor. Shared data are mapped in the user space of each communicating VM to prevent security traps, cutting down on time-consuming system calls and kernel context shifts.

A special shared-device kernel module with two-way event channels is used to generate shared memory for the two talking virtual machines. It employs a circular buffer containing state flags to minimize communication system calls and waits to improve performance. The results of the experiments demonstrate that compared to standard

TCP/IP communication through a virtual network interface, the suggested method offers much greater throughput and significantly lower latency.

Kim et al., (2016) [11] provide a mobile security agent that can protect both other agents and hosts. The capacity of this security agent type to move from a single host to another and restart operations and service provisioning is crucial in offering security mechanisms against security issues in cloud computing. In addition, attackers can launch several existing assaults. Mobile-based, cloud-based distributed transaction processing now has great fault tolerance. According to the findings, the majority of attack messages were recognized, and the assault type was determined, in a certain amount of time.

Finogeev et al., (2017) [12] present piece dives into the difficulties of intrusion detection in supervisory control and data acquisition systems (SCADA) systems' WSNs. After doing an extensive study, the authors were able to construct a comprehensive taxonomy for describing external assaults and intrusion detection in sensor networks, as well as the effects of such attacks on various SCADA system components. The ZigBee Pro Feature Set specifies an in-built method for symmetric AES encryption with 128-bit keys, which has allowed the cryptographic encryption duties in wireless sensor networks to be completed. However, studies on the present status of wireless sensor network security have demonstrated that the key management issue is seldom handled at all.

Fortino et al., (2012) [13] define geographically dispersed sensor nodes that can be used to track the health of systems and people across many different fields of study. Massive volumes of contextual data are produced by a network of body sensors in a community of individuals, necessitating a scalable solution to storing and interpreting this data. To undertake real-time and offline evaluation and mining of body sensor data streams, cloud computing can offer a potent, scalable storage and processing infrastructure. This study introduces BodyCloud, a Cloud Computing-based system architecture for managing and monitoring data streams from bodily sensors. It includes important ideas like dynamic application deployment and management, sensor heterogeneity, and flexibility and scalability of resources.

Kaiwartya et al., (2017) [14] provide a paradigm for maximizing fault tolerance via virtualization in WSNs, with special attention paid to the diverse connectivity needs of IoT applications. Taking into consideration fault tolerance and communication latency in virtualization, a multi-objective optimization problem is analytically constructed. For this optimization issue, created an Adapted non-dominated sorting-based genetic algorithm (A-NSGA). When compared to the best methods currently available, the optimization framework performs very well. The superior optimization outcomes achieved with a fewer number of generations prove this to be the case. Time to optimize outcomes is reduced in comparison to state-of-the-art methods. This proves that the planned structure works as intended.

Boni et al.,(2020) [15] convey an alternative approach to wireless sensor security in intelligent settings. Based on the scaler distribution of a unique electronic device called the intrusion detection system (IDS), the suggested security system improves sensor efficiency by minimizing computing operations. The IDS also includes the notion of a trust table and a feedback signal to activate the detection and isolation mechanism in the event of an attack. Coordinating with other IDSs, it provides blanket protection for the whole network and closes any potential security gaps that could have been introduced.

7. COMPARATIVE ANALYSIS

Table 4 shows the Comparative findings of different Authors based on Sensor as a Service in Virtual Sensor Networks.

Table 4 Comparative analysis of different authors

Authors	Methods used	Findings
Zuo et al., (2013) [9]	Cloud Computing	By centralizing, virtualizing, and automating the deployment of IT resources, this design may lower the complexity of IT systems, quicken the pace at which infrastructure is deployed, and lighten the load on system administrators.

Jiang et al., (2018) [10]	VM with TCP/IP	This enhanced model provides superior communication performance, lower communication latency, and higher throughput, according to the assessment findings.
Kim et al., (2016) [11]	Cloud Computing	Using mobile agents, dynamic capabilities, and modifiable security rules, this study implements a secure node design inside an active network.
Finogeev et al., (2017) [12]	WSN and SCADA	Three hybrid key management strategies are provided, each of which makes use of a different routing information frame based on the routing protocols in use and the topology of the WSN.
Fortino et al., (2012) [13]	BodyCloud, Cloud Computing	A good system manages sensor heterogeneity, scales resources, and deploys applications dynamically. Implementation and testing are underway.
Kaiwartya et al., (2017) [14]	A-NSGA	The findings show that the framework successfully optimizes fault tolerance for virtualization in WSNs.
Boni et al.,(2020) [15]	IDS	The IDS frees the sensors from doing any computing tasks, which might increase their memory needs and energy consumption. By closing the security gap, the IDS provides an integrated strategy to protect WSNs.

8. CONCLUSIONS AND DISCUSSION

The primary objective of this work was to conduct a broad outline of various network and security issues that can be incorporated into Sensor as a Service for modern wireless sensor networks, specifically Virtual Sensor Networks [16,17]. Using the Private Cloud, Public Cloud Edge, and Hybrid cloud or Fog paradigms, this paper will examine the Private Cloud, Public Cloud or Edge, and Hybrid cloud or Fog paradigms, with an emphasis on identifying similarities and differences, attacks and breaking the intrusion, threats and making sure that the server is secured based on security and privacy concerns regarding sensor as a service. Considering the discussions in this work, it concluded that the security and privacy concerns associated with the ecosystem's heterogeneity present a significant challenge for researchers. Even if some of these flaws can be detected and corrected relatively quickly, data transfer creates numerous security and privacy vulnerabilities. The most significant disadvantages are security and privacy, which have prevented several bodies of cloud-based service users from implementing the complexities of computational offloading technology. As previously stated, these paradigms are vulnerable to a variety of security and privacy threats, most notably denial of service (DoS) and distributed denial of service (DDoS) attacks. For instance, if an attacker gains temporary access to Cloud services and resources, Cloud customers may suffer significantly [18,19].

Cloud systems suffer from high latency and high costs when it comes to communication and data storage. These issues exist due to the Cloud's centralized nature and geographic separation from the end devices that generate data. To address these shortcomings in the different versions of Cloud-based models, the hybrid cloud-based security architecture is introduced as a Cloud Computing extension [20]. While the hybrid Cloud shares a common perspective on providing high-quality service to customers, they each have their own distinct set of characteristics, as demonstrated in this work [2]. Notably, the Fog paradigm has been identified as the most effective and dependable system for addressing the current security and privacy challenges. To summarize, while the hybrid cloud can provide superior security to end devices in general and better privacy to the client in any VSN, certain characteristics of the hybrid cloud and Fog paradigm, such as decentralization of resource allocation, the integrity of the available resource constraints, homogeneity of the data structure in the database, and virtualized systems, make the hybrid cloud network security and Fog computing paradigm more vulnerable to security and privacy challenges than the centralized approach of the data transmission. As minimum structure and applications of regularity, addressability in the deployment of different cloud models cannot be directly implemented in the Fog paradigm. As a result, hybrid cloud sensor-as-service virtual sensor network systems require novel approaches to overcome these obstacles. Additionally, future research should consider novel techniques and mechanisms that are

compatible with the characteristics of the hybrid cloud for network security in any network and Fog paradigm in any wireless network, as well as cross-platform Countermeasure tools. As a result, they should serve as recommendations for feasible and cost-effective solutions.

Conflict of Interest: The author declares that there is no conflict of interest.

9. REFERENCE

1. Aljumah, A.; Ahanger, T.A. Fog Computing, and Security Issues: A Review. In Proceedings of the 7th International Conference on Computers Communications and Control (ICCCC), Oradea, Romania, 8–12 May 2018; pp. 237–239.
2. A Review and Future Directions. In Fog/Edge Computing For Security, Privacy, and Applications; Springer: Cham, Switzerland, 2021; pp. 293–325.
3. Ometov, A.; Molua, O.L.; Komarov, M.; Nurmi, J. A Survey of Security in Cloud, Edge, and Fog Computing. *Sensors* **2022**, *22*, 927. https://doi.org/10.3390/s22030927
4. Chalapathi, G.S.S.; Chamola, V.; Vaish, A.; Buyya, R. Industrial Internet of Things (IIoT) Applications of Edge and Fog Computing:
5. Alhroob, A.; Samawi, V.W. Privacy in Cloud Computing: Intelligent Approach. In Proceedings of the International Conference on High-Performance Computing Simulation (HPCS), Orléans, France, 16–20 July 2018; pp. 1063–1065.
6. Parikh, S.; Dave, D.; Patel, R.; Doshi, N. Security and Privacy Issues in Cloud, Fog and Edge Computing. Procedia Comput. Sci. **2019**, 160, 734–739. [CrossRef]
7. Ometov, A.; Chukhno, O.; Chukhno, N.; Nurmi, J.; Lohan, E.S. When Wearable Technology Meets Computing in Future Networks: A Road Ahead. In Proceedings of the 18th ACM International Conference on Computing Frontiers, Virtual Event, Italy 11–13 May 2021; pp. 185–190.
8. Xiao, Z.; Xiao, Y. Security and Privacy in Cloud Computing. IEEE Commun. Surv. Tutor. **2013**, 15, 843–859. [CrossRef]
9. Zou, Caifeng, Huifang Deng, and Qunye Qiu. "Design and implementation of hybrid cloud computing architecture based on cloud bus." In *2013 IEEE 9th international conference on Mobile ad-hoc and sensor networks*, pp. 289-293. IEEE, 2013.
10. Jiang, Congfeng, Tiantian Fan, Yeliang Qiu, Hongyuan Wu, Jilin Zhang, Neal N. Xiong, and Jian Wan. "Interdomain I/O optimization in virtualized sensor networks." *Sensors* 18, no. 12 (2018): 4395.
11. Kim, Donghyun, Sungmo Jung, Dae-Joon Hwang, and Seoksoo Kim. "Mobile-based dos attack security agent in sensor networking." *Wireless Personal Communications* 86 (2016): 91-107.
12. Finogeev, Alexey G., and Anton A. Finogeev. "Information attacks and security in wireless sensor networks of industrial SCADA systems." *Journal of Industrial Information Integration* 5 (2017): 6-16.
13. Fortino, Giancarlo, Mukaddim Pathan, and Giuseppe Di Fatta. "Bodycloud: Integration of cloud computing and body sensor networks." In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pp. 851-856. IEEE, 2012.
14. Kaiwartya, Omprakash, Abdul Hanan Abdullah, Yue Cao, Jaime Lloret, Sushil Kumar, Rajiv Ratn Shah, Mukesh Prasad, and Shiv Prakash. "Virtualization in wireless sensor networks: Fault-tolerant embedding for the internet of things." *IEEE Internet of Things Journal* 5, no. 2 (2017): 571-580.
15. Boni, Kenneth Rodolphe Chabi, Lizhong Xu, Zhe Chen, and Thelma Dede Baddoo. "A security concept based on scaler distribution of a novel intrusion detection device for wireless sensor networks in a smart environment." *Sensors* 20, no. 17 (2020): 4717.
16. NIST Special Publication 800-145: Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (accessed on 21 December 2021).

17. Edge Computing Learning Objectives. Available online: https://www.cloudflare.com/en gb/learning/serverless/glossary/what-is-edge-computing/ (accessed on 21 December 2021).
18. Spatharakis, D.; Dimolitsas, I.; Dechouniotis, D.; Papathanail, G.; Fotoglou, I.; Papadimitriou, P.; Papavassiliou, S. A Scalable Edge Computing Architecture Enabling Smart Offloading for Location Based Services. Pervasive Mob. Comput. **2020**, 67, 101217. [CrossRef]
19. Jadeja, Y.; Modi, K. Cloud Computing—Concepts, Architecture, and Challenges. In Proceedings of the International Conference on Computing, Electronics and Electrical Technologies (ICCEET), Nagercoil, India, 21–22 March 2012; pp. 877–880.
20. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and Privacy in Fog Computing: Challenges. IEEE Access 2017, 5, 19293–19304. [CrossRef]