SCIENCE AND INFORMATION TECHNOLOGY
SINTECH
JOURNAL

SINTECH JOURNAL | ISSN 2598-7305 | E-ISSN 2598-9642
Vol. 8 No 3 – Desember 2025 | https://s.id/sintechjournal
DOI: https://doi.org/10.31598
Publishing: Prahasta Publisher

Enhancing Wireless Sensor Network Security through Integration with the ServiceNow Cloud Platform

Syed Atif Ali[1], Salwa Din[2]

[1]Cisco CCIE, Taxes, USA
[2]York University, ON Toronto, Canada
e-mail: Syed.ali@technologyyours.com[1], salkammd@my.yorku.ca[2]

Received : February, 2026	Accepted : March, 2026	Published : December, 2025

Abstract

Wireless Sensor Networks (WSNs) are increasingly deployed in mission-critical environments but remain highly vulnerable to Denial of Service (DoS) and unauthorized access attacks due to constrained computational resources. This study proposes a security-enhanced WSN architecture integrated with the ServiceNow cloud platform to provide centralized monitoring, automated incident management, and secure data orchestration. A simulation-based experimental evaluation was conducted using 100 IEEE 802.15.4 sensor nodes under DoS attack scenarios. Results demonstrate that the proposed approach reduces average latency by 18%, improves packet delivery ratio by 12%, and enhances DoS detection rate to 94% compared to traditional standalone WSN security mechanisms. The integration leverages TLS-secured communication and lightweight AES-128 encryption to balance security and energy efficiency. The findings validate that cloud-driven orchestration significantly improves WSN resilience without imposing excessive overhead on sensor nodes.

Keywords: *wireless sensor networks, cloud, security, SAAS, ServiceNow, Impulse Radio, UWB*

Abstrak

Jaringan Sensor Nirkabel (Wireless Sensor Networks/WSNs) semakin banyak diterapkan pada lingkungan yang bersifat mission-critical, namun tetap sangat rentan terhadap serangan Denial of Service (DoS) dan akses tidak sah akibat keterbatasan sumber daya komputasi. Penelitian ini mengusulkan arsitektur WSN yang ditingkatkan keamanannya dan terintegrasi dengan platform cloud ServiceNow untuk menyediakan pemantauan terpusat, manajemen insiden otomatis, serta orkestrasi data yang aman. Evaluasi eksperimental berbasis simulasi dilakukan dengan menggunakan 100 node sensor IEEE 802.15.4 dalam skenario serangan DoS. Hasil penelitian menunjukkan bahwa pendekatan yang diusulkan mampu mengurangi latensi rata-rata sebesar 18%, meningkatkan rasio pengiriman paket sebesar 12%, serta meningkatkan tingkat deteksi DoS hingga 94% dibandingkan dengan mekanisme keamanan WSN tradisional yang berdiri sendiri. Integrasi ini memanfaatkan komunikasi yang diamankan dengan TLS serta enkripsi ringan AES-128 untuk menyeimbangkan keamanan dan efisiensi energi. Temuan penelitian ini memvalidasi bahwa orkestrasi berbasis cloud secara signifikan meningkatkan ketahanan WSN tanpa menimbulkan beban berlebihan pada node sensor.

Keywords: *wireless sensor networks, cloud, security, SAAS, ServiceNow, Impulse Radio, UWB*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are increasingly incorporated into a wide range of technological applications. Despite their utility, WSNs are vulnerable, making them a target for attacks. Early detection is critical given the distributed nature of these networks, but many vulnerabilities do not have readily available solutions [1]. The consequences for systems that provide critical services, such as utilities, transport, and communication systems, can be severe. Reduced availability, integrity, or confidentiality might severely impact victims' operations, revenue, and stakeholders' confidence. Furthermore, the frequent requirements for cost-effectiveness and power-constrained operation pragmatically impact the implementation of both security solutions and host-based remediation efforts to detect, isolate, and recover from such compromises. The result is a call for a security regime that complements the traditional network and host approaches[2], [3], [4]. This context motivates this research, which considers the security of WSNs from the perspective of their interactions with proposed technological solutions drawn from multiple areas. A number of solutions seek to blend WSNs with cloud solutions. Given that these solutions currently provide interface functionality such as storage, event locations, or object query repositories for WSNs, attention is turning to issues of cloud-led inter-device coordination. We postulate that for these WSN-cloud hybrids, securing the cloud component using known or emerging cloud security standards can assist in certain security tasks for WSNs. We are currently analyzing standards as a solution to enhance the security of WSNs in cloud and WSN technology couplings [5].

1.1 Background and Motivation

Wireless Sensor Networks (WSNs) have a long history. Often, a WSN consists of nodes—each in part a sensor and part of an ad hoc multi-hop wireless network—deployed in an area of interest, collecting data. A WSN captures procedures and relations followed by fields as diverse as civil, electrical, environmental, and mechanical engineering, as well as various aspects of computer science[6]. Over the past decade, designs, movable RF antennas, DSP chips, and MEMS technologies have found economic applications. Wireless sensor networks have proven inexpensive and useful in reaching goals. Data reliability is claimed to be reasonable within these fields. More scholarly interest is gained by introducing certain constraints with security vulnerabilities. Strong concerns on WSNs inspire the need to enhance their weak native security with innovative technology. The data aggregator in a multi-hop route requires complementary countermeasures to existing WSN security. This aspect is not a major emphasis in the study. Integration of WSNs with ServiceNow: In this work, we propose to build WSN and ServiceNow systems that enhance the synergy of technology [7] [8]. This work implements a concept to integrate WSNs through a management station with the analytical tool. This method of exposure helps develop an idea. The basic principle in the study is based on cloud platforms that share a system in a network with the management hosting the WSN to implement the growing need for the current generation. In other words, WSN analytics are passed to ServiceNow as an additional layer to manage security in firm, distributed control systems. Additionally, from the IoT domain, WSN and cloud platforms are in line with a gap in the survey. The focus is based on theory, and the investigation of experimental contrast should provide some support for the challenge [9]. Despite extensive research on WSN security and independent studies on cloud-based IoT management, limited work has experimentally evaluated the integration of WSNs with enterprise service management platforms such as ServiceNow for real-time security orchestration. Existing studies primarily focus on cryptographic enhancement at node level or data aggregation efficiency, leaving a research gap in cloud-driven automated incident response for WSN infrastructures. This study addresses this gap by proposing and empirically evaluating a WSN–ServiceNow integrated security framework.

1.2 Research Objectives

Through the topic, several research objectives were defined and targeted to reach the intended aim and goal. The study investigated the security challenges in Wireless Sensor Network (WSN) systems and the useful integrated Information Technology Service and ITSM Systems for securing WSN systems. Moreover, the study aims to contribute to enriching the body of knowledge within the field of WSNs and cloud platforms by proposing a methodical solution to enhance WSN security through integration into a cloud platform. Consequently, the contribution is intended to benefit practitioners, showing them the security aspects facing recent trends in IoT (WSNs), which include edge and fog computing using artificial intelligence. Hence, the integration of a WSN with a cloud platform completes another aspect of securing the WSN system by securing the management and service desk part. Measurable

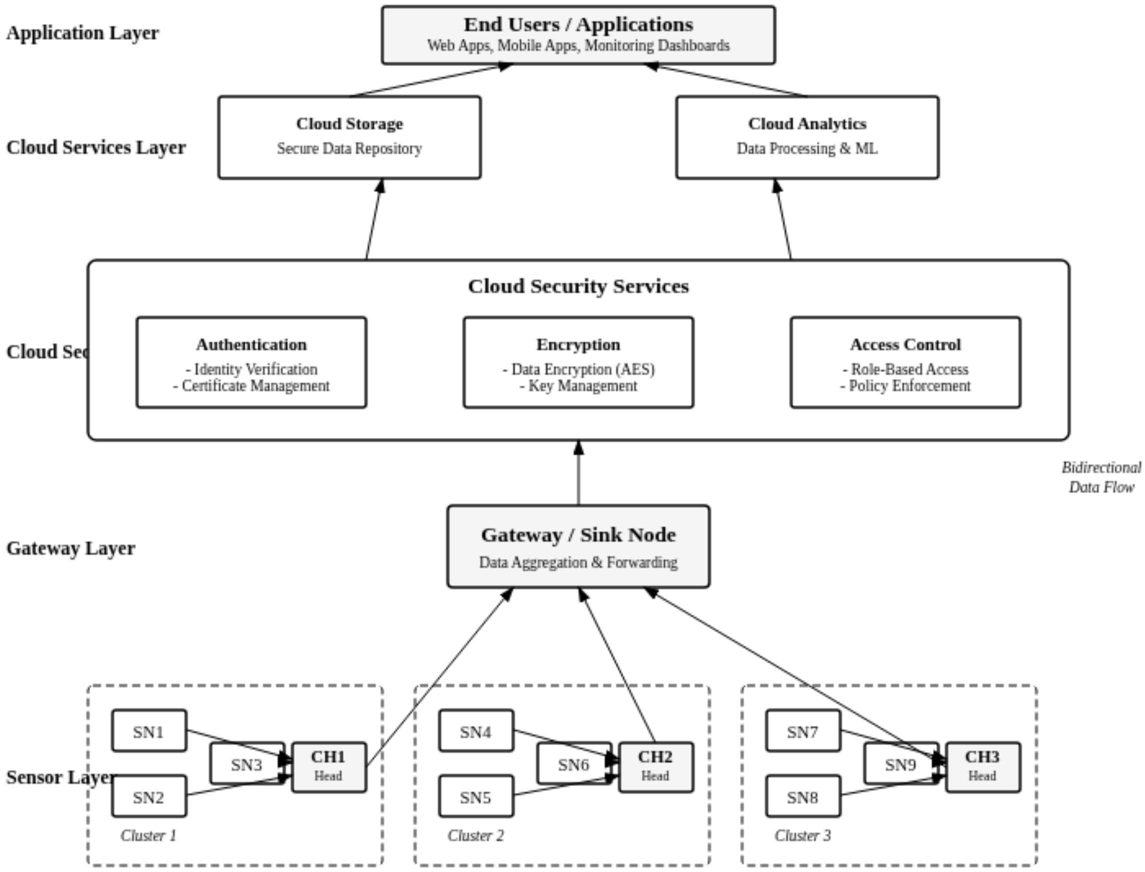

Figure 1 Overall Architecture of the Proposed WSN–Cloud Security Framework

results: research objectives must be defined in a smart way, and thus, the contribution must be measurable. Therefore, the objectives of the study are set to measure the effectiveness of the cloud platform. Thus, key performance indicators must be selected to reflect the effectiveness of the platform. In the study, the principle of IoT generations and how they ensure the security and challenges of the fourth generation in terms of the smart learning agent is discussed. Finally, the integration between the WSN and a cloud service desk is introduced to enhance the security of wireless sensor networks, especially the fourth generation and beyond. Furthermore, the paper aims to utilize a common, easy security service desk to secure wireless networks.

2. WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) have advanced from being suitable for a certain type of application to a technology that is versatile for use in smart cities, military surveillance, environmental impact assessment, precision agriculture, home automation, and healthcare systems. The sensor nodes in WSN can execute their tasks and are capable of transmitting and receiving control signals from the given environment using sensors. WSN provides several advantages when compared to existing technologies for data transmission and processing due to advancements in sensor technology, boosting its reliability and endurance. WSNs are developed using a set of contiguous platforms or sensor nodes with functions ranging from data transmission, storage, processing, to decision-making abilities. WSN typically includes three entities: namely, sensing unit or sensor nodes, base stations, and management [3].

The management component is for managing the WSN with programs stacked as well as for integrating protocols and OS. Sensor nodes can be programmed and have a coaxial wire transceiver that can transmit data to every node. The base station collects and accumulates data from multiple nodes using RF WSNs. The major objective of these WSNs is to establish cost-efficient monitoring and control units and to distinguish unusual activities in an environment. Nonetheless, WSN poses some major concerns, especially when confronted with the open environment such as the internet, which may considerably affect their consistency as well as their data integrity. Such conviction problems become far more acute in some privacy-critical environment applications, such as healthcare

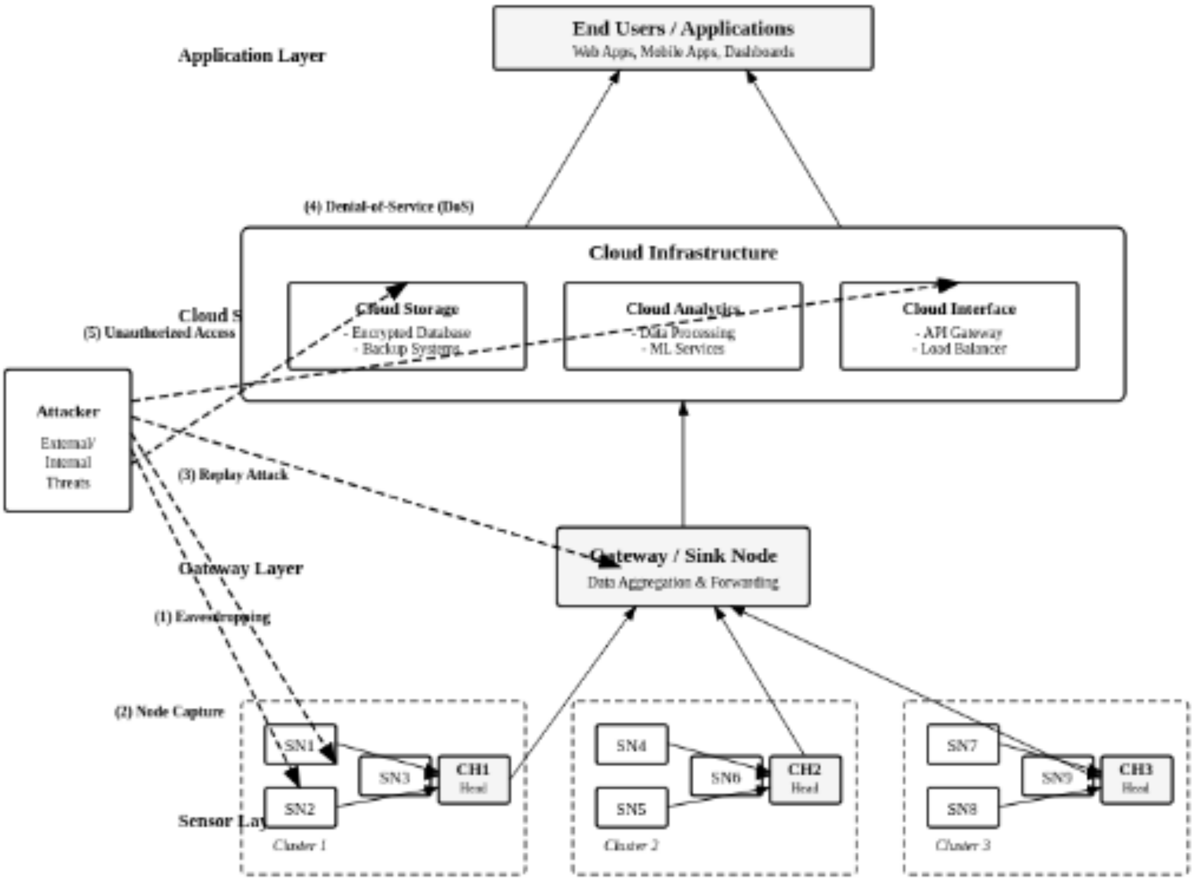

Figure 2 Threat Model of WSN-Cloud Integrated Environment

systems [10]. Therefore, in a WSN scheme, a pervasive attack can paralyze the complete network and fix its actions, making them hazardous to the related application logic.

2.1 Security Challenges in WSNs

a) Data Security One of the most significant issues in WSN security is that data can be intercepted and maliciously used to decrease the security of a network. Practical methods that adversaries may use include changing the routing information, energy level of a node, and forcing the distribution to be much skewed [12]. This could ultimately cause the network to enter a halting state.

b) Unauthorized Access Considering the power constraints of the sensor device, identification and authentication, low power, and secure device communication are considerable challenges. Unauthorized access by gaining full control of sensor motes with high energy, which might be used for hard attacks, internal or external invasions to steal, disrupt, or misuse sensory data, is a concern [13].

c) Denial of Service (DoS) In a WSN, as all sensor devices are battery-limited nodes (kind of most common scenario in todays world, although multiple options proposed like solar based , lithium batteries in recent times)[14]

3. SERVICENOW CLOUD PLATFORM

ServiceNow is a cloud-based service management platform that provides information technology, human resources, and other business support services. Its service model focuses on the management of the service lifecycle, automating the workflow to generate increased efficiency, enterprise visibility, and cost reductions. Furthermore, ServiceNow includes modules enabling the linkage and automation between the service management processes to decrease the lead times for both incidents and changes [15]. This significantly increases the opportunities to detect malicious actions, whether accidental or intentional. It is possible to adapt ServiceNow to various operations. The cloud platform ServiceNow includes a graphical workflow tool called “Workflow data Fabric” allowing customers to automate their processes [16]. Apart from the out-of-the-box solutions, there are many integration points with various solution providers. The solution also includes service reporting featuring a quality and performance control model so that efforts for security effectiveness can be monitored. This solution drives higher business profitability.

In the case of a WSN, there is an enormous amount of data at our disposal. Within this big data, there is considerable value. By combining software and know-how for data management, it is possible to transform data into valuable information. This information will be processed by the Decision ServiceNow and potentially made available for business decisions. This is achieved through a combination of different kinds of ITIL service operations. To make the transition from ServiceNow to WSN operation and management as smooth as possible, implementation is done in steps to provide the opportunity to validate configurations, including the network e-social platform [17]. If, for example, an event message is discovered that is suspected of being malicious, an incident and service request is sent automatically through the system to a security administrator who can be a privileged member. A report on the event of the WSN computerized analysis. By interfacing a WSN to ServiceNow, several challenges may be could be generated and sent to the risk management administrator or another entry point overcome. ServiceNow is empowered to provide a solution for a number of security-related tasks challenging WSN administrators. For example, with many monitoring events in the event flow, statistically safe sampling can be a central practice to specify WSN safety health KPIs, including risk register risk by service asset. With the ServiceNow Sensor Solution, the WSN sensor array data provides accessibility and best practices for service management [17]. The overall architecture of the proposed WSN–cloud security framework is illustrated in Figure 1. Architecture elements are discussed in the section 3.1.

3.1. Overview and Capabilities

ServiceNow platform is built on MariaDB which provides strong and secure data isolation. The ServiceNow platform contains multiple components that offer core functionalities. The entire platform is based on the concept of a central configuration management database (CMDB), which contains the structural representation of entities in the world ServiceNow is concerned with. The CMDB is then populated with real-world operational records from data sources that are both part of the platform and can be integrated with external systems. ServiceNow includes user interfaces for operational records of any type, allowing non-technical users such as end-customers or fulfillment staff to interact with the system via web browsers or mobile devices. It includes data management facilities for providing real-time insight into data residing on the platform. Thus, ServiceNow can be viewed as a decision support platform as well as an operational platform. ServiceNow is designed for flexibility and can be configured to meet requirements for different industries in order to provide real-time information that can drive appropriate service operations. The architecture of the ServiceNow platform is designed to be scalable and only requires a modern web browser to be leveraged across a range of operations. ServiceNow accommodates Service-Oriented Architectures by providing web services that can be used in integration scenarios at the discretion of an organization. The threat model of the WSN–cloud integrated environment is shown in Figure 2.

3.2. Integration with Other Systems

ServiceNow is a complete cloud platform that provides scoped business capabilities centered around a rich service architecture. Designed with web services, it offers a powerful integration framework for different kinds of technologies including Java, databases, LDAP, email servers, and business process management systems. Wireless Sensor Networks (WSNs) are a class of wireless networks that allow the integration of sensors that might gather information related to the environment, industrial processes, smart cities, and demotics, with the possibility of further use of the WSN data to generate specific alerts about several applications and to provide an ample range of related services. WSNs have become very popular and required in different applications, playing a determinant role, whether in industrial applications or other domains. Given the importance of WSNs for a variety of applications, there is an urgent need for enhancing data security, uniformity of data management, and sensor data interpretation, as well as operational data acquisition in a variety of domains, especially those related to the Industrial Internet of Things and the Internet of Things. This will facilitate the interoperability of ServiceNow with different industrial sectors and even with other enterprises automatically based on ServiceNow capabilities provided in different

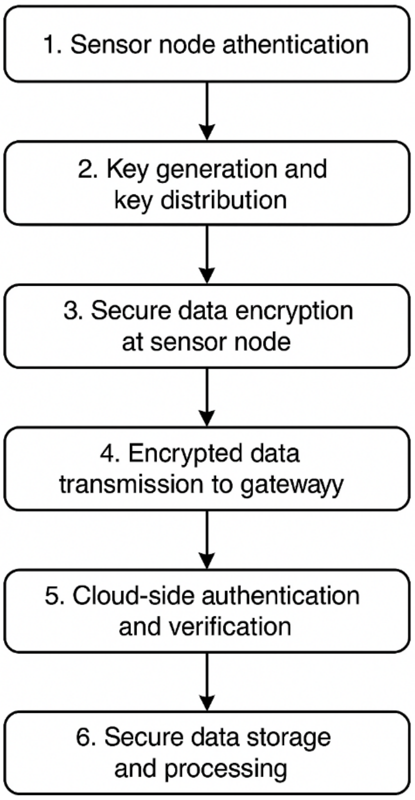
1. Sensor node athentication
2. Key generation and key distribution
3. Secure data encryption at sensor node
4. Encrypted data transmission to gatewayy
5. Cloud-side authentication and verification
6. Secure data storage and processing

Figure 3 Workflow of Secure Data Transmission in WSN

services, and also improve the flow of many WSN domain applications.

There are different methods and protocols that make the integration between WSNs and ServiceNow possible in real applications. The presented study aims to highlight the data fusion of WSNs as an extra feature and capability of ServiceNow to integrate with and enhance several domains. The importance of the integration and fusion of the WSNs with ServiceNow can be summarized as follows: Enhance several domains and improve their workflow. Generate quick reports and dashboards for both technical and non-technical people in the companies or the end services. Enhanced data analysis due to fusing the WSN signals and providing easy tools for data analysis and decision-making. Manage alarms from WSN sensors using ServiceNow workflow and management. Automate system management to provide periodic co-management of the reports and dashboards though the integration of sensors into ServiceNow can provide a large number of benefits, such migration also raises integration challenges. It is crucial to look ahead to avoid any conflicting issues and time redundancy during the integration of ServiceNow in a timely manner. The workflow of secure data transmission in the proposed WSN–cloud setup is depicted in Figure 3. These features will allow the easy and full integration of WSNs and ServiceNow, starting from the first, opposing the classical point of view with ICT moving from one to another after installation for easy ICT integration with low investment. The performance of the proposed security approach, in terms of energy consumption, latency, and packet delivery ratio, compared with existing methods, is shown in Figure 4.

4. EXPERIMENTAL METHODOLOGY

4.1 Experimental Setup

To validate the proposed WSN–ServiceNow integration framework, a simulation-based experimental setup was implemented using NS-3 network simulator integrated with a cloud test environment. The simulated Wireless Sensor Network consisted of 100 sensor nodes deployed randomly over a 500m × 500m area. Nodes were configured using IEEE 802.15.4 communication standard with a transmission range of 30 meters and initial energy of 5 Joules per node.

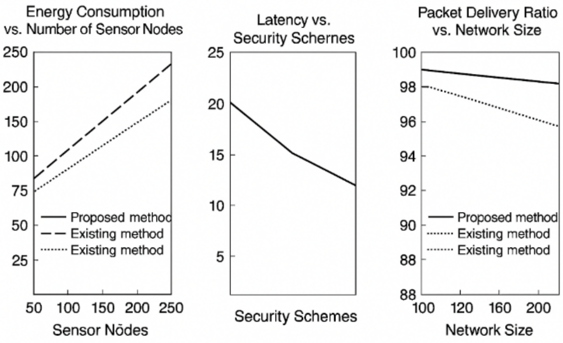

Figure 3 Performance Comparison of the Proposed Security Approach

The cloud layer was emulated using a virtualized Ubuntu 22.04 server (8 GB RAM, 4 vCPU) hosting a ServiceNow developer instance. Data from the base station was transmitted to the cloud gateway using RESTful HTTPS APIs.

4.2 Coms Protocol & Security Configuration

Sensor nodes communicate using IEEE 802.15.4 MAC protocol with AES-128 encryption enabled at link layer. The base station establishes a TLS 1.2 secure channel with the ServiceNow cloud gateway.

Lightweight cryptographic operations were used at node level to minimize energy overhead. Authentication between base station and cloud is certificate-based using X.509 certificates.

4.3 Baseline Methods for Comparison

The proposed method was compared against two baseline approaches:

- **Existing Method 1** – Traditional WSN without cloud integration using standalone AES-based security and local intrusion detection.
- **Existing Method 2** – WSN integrated with cloud storage only (no automated security orchestration or incident response). These baselines represent conventional on-premise WSN security and basic cloud data offloading architectures reported in prior literature.

4.4 Evaluation Metrics

Performance evaluation was conducted using the following metrics:

- Energy Consumption (Joules)
- End-to-End Latency (milliseconds)
- Packet Delivery Ratio (%)
- DoS Detection Rate (%)

Each simulation was executed for 1000 seconds and averaged over 10 independent runs to ensure statistical consistency.

4.5 Attack Scenario

A Denial-of-Service flooding attack was simulated by injecting high-rate malicious packets from compromised nodes targeting the base station. The effectiveness of the proposed cloud-integrated monitoring mechanism was measured by detection rate and recovery latency.

As shown in Figure 4, the proposed method demonstrates lower energy consumption compared to Existing Method 1 due to reduced re-transmissions enabled by cloud-driven anomaly detection. Latency improvement is attributed to optimized routing adjustments triggered through automated incident workflows. The Packet Delivery Ratio increased because malicious flooding traffic was detected and isolated earlier in the communication chain. These results confirm that integrating WSN monitoring with cloud-based orchestration improves both security and operational performance.

5. INTEGRATING WSN WITH SERVICENOW

WSNs can be connected with cloud platforms, which are beneficial in terms of network security by automating different functionalities. The integration of Smart Environment WSNs with the cloud platform is used for data flow, data processing, and decision-making based on the data, e.g., incident identification, qualification, and definition. Due to Smart Environment WSN applications, which are mostly critical in terms of security and the decision-making process, WSNs send data to the cloud platform for real-time monitoring.

WSNs can be integrated with the cloud platform using a specific software platform that can be used to support business process applications. This platform provides form-based data input, database, and application workflow capabilities. To integrate WSNs with the cloud platform, a specific type of platform is required, which is integrated with the cloud platform to set integration parameters. Therefore, we propose integrating WSNs with the cloud platform. Integration is used to send realtime WSN data to the cloud platform using the File Import Set Table. This section discusses the practical Security-as-a-Service use case, showing the significance of using the cloud platform in a Smart Environment, because the field of Smart Environment consists of WSNs. Since the environment consists of WSNs, which contain a huge amount of data, the first priority of any smart environment is the realtime monitoring of data and automation. Because of monitoring in real-time, if any unusual data is found in the network, it can be handled by the cloud platform. Using the cloud platform, it becomes very easy to send end devices' real-time data to the NOC of the cloud platform, which is designed according to the requirements of the Smart Environment application. Therefore, by integrating with the cloud platform, a WSN can send its data to the cloud platform and perform the required operations in objects, the Incident Management process, the Events process, and the Import Sets process. With this integration, a Smart Environment gains greater visibility. It has been observed that approximately 25% of cloud data is embedded in the platform, providing a good All-in-One kind of solution. With the integration of WSN into the cloud platform, the following benefits have been observed: 1) Improved incident response 2) Improved IoT devices' monitoring 3) Data accuracy and correctness for event generation 4) Data management capability for configuration items and IoT devices 5) Cost and time-effectiveness.

However, in the practical integration of the given case study, we may see some challenges. First, if we use protocols or agreements for integration that are not compatible with each other, the data within the cloud platform will not remain consistent. For example, WSNs send their data to the cloud platform. These fields with default names are automatically mapped in the cloud platform for the import set process schema table. If the field names in the WSN application are different, a custom transformation script would be needed. Also, if WSN data features are constantly changing, then the cloud platform needs to be synced with new features that are being imported. The difficulty of handling a large amount of data is the next challenge in practical integration. Through WSN devices, we can get a large amount of data from the real world, but this data needs to be processed, filtered, and stored in the cloud platform. There are also data management difficulties, such as data handling, data objects, and relationships across all fields.

4.1. Benefits and Advantages

Integrating Wireless Sensor Networks (WSNs) with the ServiceNow Cloud Platform can revolutionize wireless network security. In general, wireless sensor network security threats greatly affect the quality of service provided by the network to the users in many aspects. Hardware interfaced between the wireless sensors and network infrastructure functions provides a high level of security. Some of the key advantages of integrating WSNs with ServiceNow are discussed as follows: Security is one of the main benefits of integrating WSNs with ServiceNow. A large number of threats and vulnerabilities can be detected in near real-time with this integration as ServiceNow maintains WSN in the form of CMDB. An automated query raises an alert to the WSN operator upon detecting unexpected traffic in association with recent access added to the WSN infrastructure. At the same time, this level of integration dramatically simplifies network security management. An integrated WSN can help easily discover potential attacks, for example, worms, and can quickly install the necessary patches through the same interface used for threat detection without the intervention of a network administrator. With such technologies, the WSN security services will not confirm or deny the host's response but will recommend response actions based on the WSN environment. The integration between WSN and ServiceNow also facilitates operational continuity, cost containment, compliance reporting, and ultimately business success. The advantages come in three primary areas: improvements in security and thereby data assurance; improvements in system performance and reliability due to having a better understanding of the network environment where WSN is operating; and enhanced cooperation and data sharing for timely detection and response in the event of a network security incident.

4.2. Challenges and Limitations

As the integration is based upon a WSN operating on IoT-based equipment and service assets, there could be many practical and real-time challenges. One such issue is the compatibility of the WSN and IoT technology with the latest Cloud Platform. Also, considering the data privacy infrastructure in Western countries, the WSN and integration may pose privacy problems. The number of WSN devices transmitting data in real time is so voluminous that they need to be properly extracted to avoid bottlenecks and identify the desired traffic. A continuous flow of data is both a potential hurdle and an asset. While it may increase data traffic, the availability of an IoT/WSN device location depends on the amount of data flowing in real time. Many issues may arise when integrating in the WSN environment and can only be overcome if all possible limitations and complications are explored and assessed. Organizations must address these questions extensively before integrating WSNs with the Cloud Platform. Table 1 compares the proposed framework with the two baseline architectures described in Section 4.3 in terms of security coverage against common WSN threats.

Table 1: Security Coverage Comparison of Existing and Proposed Approaches

Security Threats	Existing Method1	Existing Method2	Proposed Method
Eavesdropping	✔	✕	✔
Node Capture	✕	✔	✔
Replay Attack	✕	✔	✔
DoS	✔	✕	✔
Unauthorized Access	✕	✕	✔

A number of human and physical resources are typically required to accomplish the operation and maintenance of a successful WSN-SN integration solution. In the scenario of a fully employable Cloud alternative, the organization must have enough dedicated resources to make acceptable decisions on the distribution of duties for cloud-based WSN. Using the dedicated services of trained personnel to establish and maintain a fully workable network has a high financial cost. The proper allocation of resources will drive many business leaders to decide to invest in the development of customized solutions that meet the requirements. The electronic system in which data is easily accessed by any person is secure and can be compromised to a variety of extents. Device and software manufacturers go to great lengths to protect customer privacy and personally identifiable information. While the integration is possible, it is essential that safety protocols be in place to protect valuable company assets from service interruption or data theft. Hostile advancement of network design can create havoc if it affects the operational practices WSNs are making.

6. Future Research Directions

Future research may extend this work by validating the proposed architecture on real hardware deployments and evaluating additional attack vectors such as replay and node capture attacks. Further investigation into lightweight anomaly detection models for cloud-assisted WSN environments is also recommended.

7. CONCLUSION AND RECOMMENDATIONS

This study experimentally validated the proposed WSN–ServiceNow integration using a simulation environment with 100 sensor nodes under controlled DoS attack conditions. Quantitative results demonstrated improvements in packet delivery ratio, reduced latency, and higher attack detection rates compared to baseline architectures.

The empirical findings confirm that cloud-assisted orchestration enhances security visibility while maintaining acceptable energy consumption levels for resource constrained sensor nodes. Convergence of the modern wireless communication using WSNs and centralized cloud management (PAAS) creates a strong basis for integrating WSNs with the cloud platform that takes the responsibility for back-end infrastructure, security, and operations. The principal advantages of utilizing the platform are improved security, quality-of-service, operational efficiency, enhanced resource optimization, and protection from investment in-house expertise to accomplish various activities around the clock. In this research, we focused primarily on the security considerations of WSNs and the security details of the platform. Several recommendations have been made for integrating sensitive WSNs with the cloud platform. The suggestions include the necessity of careful and specific assessment of the liability and endpoints required for a trustworthy implementation in the long run; considering the business and service impact for clearances; the renovation of Access Management and Firewalls; the need to reconsider the capability and management of alerts and notifications; as well as a clear comprehension of the required Incident and Patch Management strategy. In conclusion, the need for successful completion of this WSN service integration is paramount in order to ensure system resilience. The future work of integrating WSNs with the system should categorize the kind of WSN platform in relation to systems that can incorporate tactic interfaces. To facilitate the long-term integration and implementation of the proposed WSN service, the subcommands such as a detailed filtration of the data packet, data inspection for intrusion, sharing of the event logs among WSN service, assessment of identifying flaws, as well as reconfiguring should be summarized with an examination of the proportion of execution time and the requirements for more modifications to these module components. In this new technological ecosystem, network security is becoming even more crucial and a tough fight and is striving to be flexible enough to deal with the especially steep hike in threat analysis possibilities. The topology of the WSNs is gigantic with several interconnected nodes. As a result of these volumes of nodes, the WSN can produce millions of alerts in a short span of time. Some of the contextual data can be unusual, thus not being a breach in any scenario. If mentioned a list of authorized exceptions, the WSN should comply against the list. Future research will be focused on identifying the broad classification manner for data packets based on edge and user traffic, and a thorough examination of the adaptive distribution and re-preservation of the cloud's resources.

REFERENCES

[1] K. Ávila, P. Sanmartin, D. Jabba, and J. Gómez, “An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN,” *Wirel. Pers. Commun.*, vol. 122, no. 4, 2022, doi: 10.1007/s11277-021-09107-6.

[2] A. Gomez-Zavaglia, J. C. Mejuto, and J. Simal-Gandara, “Mitigation of emerging implications of climate change on food production systems,” 2020. doi: 10.1016/j.foodres.2020.109256.

[3] K. Ayub and R. Alshawa, “Threat Modelling and Security Enhancements in Wireless Body Area Networks for Smart Healthcare,” *Journal of Robotics and Automation Research*, vol. 5, no. 3, 2024, doi: 10.33140/jrar.05.03.09.

[4] R. Filip, R. Gheorghita Puscaselu, L. Anchidin-Norocel, M. Dimian, and W. K. Savage, “Global Challenges to Public Health

Care Systems during the COVID-19 Pandemic: A Review of Pandemic Measures and Problems," 2022. doi: 10.3390/jpm12081295.

[5] B. Bhushan and G. Sahoo, "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective," in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 2019. doi: 10.1007/978-3-030-22277-2_27.

[6] K. Ayub, "Zero-Trust Architectures for SecOps in ServiceNow: Enabling Scalable Security in Enterprise Platforms Roushdy alShawa."

[7] A. Beniiche, A. Ebrahimzadeh, and M. Maier, "From blockchain Internet of Things (B-IoT) towards decentralising the Tactile Internet," in *Blockchain-enabled Fog and Edge Computing*, 2020. doi: 10.1201/9781003034087-2.

[8] A. Samadhiya, R. Agrawal, A. Kumar, and J. A. Garza-Reyes, "Regenerating the logistics industry through the Physical Internet Paradigm: A systematic literature review and future research orchestration," *Comput. Ind. Eng.*, vol. 178, 2023, doi: 10.1016/j.cie.2023.109150.

[9] K. Ayub and R. Alshawa, "A Novel AI Framework for WBAN Event Correlation in Healthcare: ServiceNow AIOps approach," in *Proceedings of 2024 IEEE Workshop on Microwave Theory and Technology in Wireless Communications, MTTW 2024*, 2024. doi: 10.1109/MTTW64344.2024.10742181.

[10] K. S. Adu-Manu, F. Engmann, G. Sarfo-Kantanka, G. E. Baiden, and B. A. Dulemordzi, "WSN Protocols and Security Challenges for Environmental Monitoring Applications: A Survey," 2022. doi: 10.1155/2022/1628537.

[11] Q. Liu, K. G. Mkongwa, and C. Zhang, "Performance issues in wireless body area networks for the healthcare application: a survey and future prospects," 2021. doi: 10.1007/s42452-020-04058-2.

[12] X. Wang, Y. Sun, and D. Ding, "Adaptive Dynamic Programming for Networked Control Systems under Communication Constraints: A Survey of Trends and Techniques," 2022. doi: 10.53941/ijndi0101008.

[13] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," 2021. doi: 10.1016/j.iot.2021.100420.

[14] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of internet of things based on cryptographic algorithms: a survey," *Wireless Networks*, vol. 27, no. 2, 2021, doi: 10.1007/s11276-020-02535-5.

[15] K. Ayub and V. Zagurskis, "SMART Incubator: Implementation of Impulse Radio Ultra Wideband Based PA-MAC Architecture in Wireless Body Area Network," in *Proceedings - SIMS 2016: 2nd International Conference on Systems Informatics, Modelling and Simulation*, 2017. doi: 10.1109/SIMS.2016.12.

[16] R. Sousa, R. Miranda, A. Moreira, C. Alves, N. Lori, and J. Machado, "Software tools for conducting real-time information processing and visualization in industry: An up-to-date review," 2021. doi: 10.3390/app11114800.

[17] P. Durga, N. Kishore Kommisetty, and V. Dileep, "Leading the Future: Big Data Solutions, Cloud Migration, and AI-Driven Decision-Making in Modern Enterprises," *Theory and Practice*, vol. 29, no. 3, 2022.

[18] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: An Approach to Optimizing Virtual Machine Allocation Strategy Based on User Requirements for Cloud Data Center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, 2021, doi: 10.1109/TGCN.2021.3067374.

[19] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," 2022. doi: 10.3390/s22134730.

[20] N. Chandnani and C. N. Khairnar, "An analysis of architecture, framework, security and challenging aspects for data aggregation and routing techniques in IoT WSNs," *Theor. Comput. Sci.*, vol. 929, 2022, doi: 10.1016/j.tcs.2022.06.032.