Article

Not peer-reviewed version

Cybersecure Intelligent Sensor Framework for Smart Buildings: AI-Based Intrusion Detection and Resilience Against IoT Attacks

Md Abubokor Siam , Khadeza Yesmin Lucky , Syed Nazmul Hasan * , Jobanpreet Kaur , Harleen Kaur , Md Salah Uddin , Mia Md Tofayel Gonee Manik *

Posted Date: 15 September 2025

doi: 10.20944/preprints202509.1177.v1

Keywords: cybersecurity; smart buildings; intrusion detection systems (IDS); internet of things (IoT); artificial intelligence (AI)

Article

Cybersecure Intelligent Sensor Framework for Smart Buildings: AI-Based Intrusion Detection and Resilience Against IoT Attacks

Md Abubokor Siam, Khadeza Yesmin Lucky, Syed Nazmul Hasan *, Jobanpreet kaur, Harleen Kaur, Md Salah Uddin and Mia Md Tofayel Gonee Manik *

Westcliff University, Irvine, CA 92614, USA

* Correspondence: s.hasan.104@westcliff.edu (S.N.H.); m.manik.407@westcliff.edu (M.M.T.G.M.); Tel.: +1-202-802-5344 (S.N.H.)

Abstract

Due to the fast development of the Internet of Things (IoT) in smart buildings, the efficiency of operations, personal comfort, and sustainable operations have all been enhanced. But with all this dependence on potentially linked systems comes vital cybersecurity weaknesses. When such weaknesses are used to attack, they may lead to the compromise of the security of both an individual device as well as a building infrastructure. The present paper introduces a new cybersecure intelligent sensor framework that will be able to protect smart buildings against a wide variety of IOT related cyberattacks. The key element within this structure is a sophisticated AI automated intrusion detector (IDS) that can recognize, categorize and eliminate prospective threats in an instant using machine learning routines. The system uses the combination of intelligent sensor networks with AI-based analytics to continuously observe the environment and system data, with anomalous behaviours being indicators of a security breach being detected. The combination of predictive modelling and automated threat responses will allow the proposed system to achieve resilience against many attacks, including but not limited to denial of service, unauthorized access, and data manipulation. Widespread simulation and testing have shown that the system has a high detection rate, low false alarms, and a fast response time to help secure infrastructure buildings in smart buildings whilst Downtime is minimal. The results demonstrate the possible future of AI-enhanced cybersecurity systems in developing the IoT-based smart building security and enjoyment.

Keywords: cybersecurity; smart buildings; intrusion detection systems (IDS); internet of things (IoT); artificial intelligence (AI)

1. Introduction

The automation of the smart buildings has entered a period of greater automation, energy saving, and human comforts due to the deployment of Internet of Things (IoT) equipment and devices. One of the key elements of these interdependent systems is that they allow real-time control and monitoring of many building systems, including lighting, HVAC systems, security and occupation management. Yet, these interconnections also create a complex of cybersecurity problems. The IoT devices are susceptible to malicious administration as they usually have low processing capacities and security. The imminent potential effect of the sole corrupted tool can spiral in the construction of the building itself.

The cyberattacks of internet of things (IoT) systems within smart buildings can take the form of a Distributed Denial of Service (DDoS), Man-in-the-Middle (MITM) attack and unauthorized access to important information. This kind of breach not only affects the confidentiality, integrity, and availability of building systems, but it can also result in substantial financial loss and brand degradation. The IoT has outstripped many traditional security systems, and most can be easily

 doi:10.20944/preprints202509.1177.v1

bypassed through traditional firewalls and signature-based intrusion detection systems. The traditional methods have low chances of rising up to the recent velocity of the IoT devices and their heterogeny, hence, the need to come up with more dynamic and smart security measures.

Considering that the problems in this section, this paper introduces an intrusion detection system (IDS) that works on an artificial intelligence (AI) basis integrated with an intelligent sensor framework to enhance the cybersecurity of smart buildings. The suggested system can be used to process the information of the IoT devices, which would help identify anomalous behaviours related to the identification of possible security threats. This allows the AI-based network-level IDS to constantly detect and prevent attacks in real-time, increasing the security of building infrastructures against cyber-attacks.

With AI incorporated into the IDS, it is possible to make predictive models that can be able to anticipate any security breach before it occurs. Such forward posture enables deployment of defensive actions, like isolation of infected computers or routing of traffic away to prevent attacks before they reach an endpoint. In addition, the Capacity to learn about previous data also allows the system to evolve to new incoming threat levels and maintain the protection over an extended period of evolution of the IoT.

This paper explores architecture of the proposed AI-based IDS and what it comprises and its functioning. The adequacy of the system in counteracting and preventing different attacks attributed to IoT is tested through intense testing and simulations. The results indicate the possible use of AI-based security infrastructure to enhance the cybersecurity resources of smart buildings, which opens the prospect of more secure and resilient IoT environments.

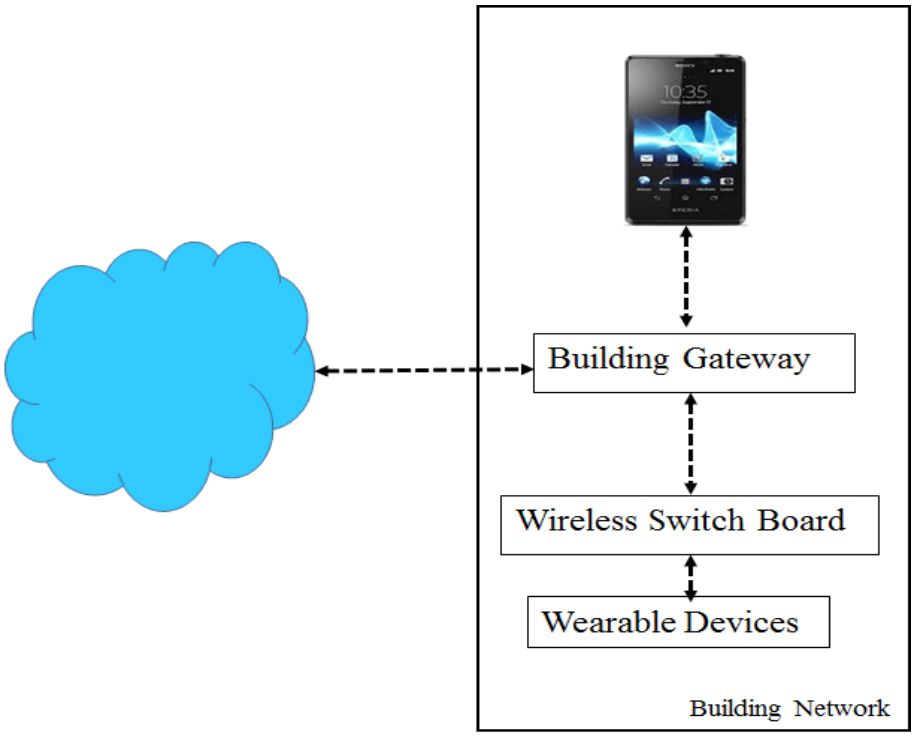


Figure 1. IoT-Based Smart Building Architecture with AI-Based IDS.

The following diagram presents a fully formed architecture of an IoT-smart building with numerous elements, including sensors, actuators, and communication networks and the use of the AI-based Intrusion Detection System. The combination of these components supports smooth data exchange and on-time threat identification to guarantee the robustness and defense of the building infrastructure.

 doi:10.20944/preprints202509.1177.v1

2. Background and Related Work

Smart Buildings and IoT Integration

Smart buildings make use of an extensive range of IoT elements like sensors, video cameras, smart lighting and thermostats to optimize the many aspects of building management [1]. Such devices gather data on such parameters as temperature, humidity, occupancy, and air quality and process it to automate the decision of heating, lighting, and energy consumption [2]. Such integration makes the work of buildings quite efficient, as they can now be controlled dynamic and managed based on live information [3]. In addition, IoT-adapted systems deliver more comfort, convenience, and safety in the building to its occupants, making changes into the building in real-time and predicting maintenance.

Even though this integration between these systems has its own advantages, it also brings forth security vulnerabilities as a result of the seamless connection between these systems. High proportions of IoT devices in smart buildings were made without making security a primary consideration [5]. Such ignorance of security poses such devices into higher exposure to hackers since they can use the vulnerabilities in devices, communication protocols or the entire network architecture in the building [6]. As devices that are network-connected grow, the attack surface grows as well along with risks that are not present with traditional integrations into the building systems [7].

Cybersecurity Challenges in Smart Buildings

Cybersecurity in smart buildings poses a number of highly problematic challenges, most of which are directly attributed to peculiarities of IoT-based systems. The absence of security of IoT devices is among the crucial challenges. A high number of IoT devices have very low processing power and storage capacity, hence, they cannot apply advanced forms of encryption, security authentication protocols or extensive access control [8]. This has led IoT devices to lack the basic security mechanisms that can be used to safeguard against intrusion to unauthorized users, data theft, and other cyberattacks [9].

The other important concern relates to interoperability of devices that are of different manufacturers. Smart buildings tend to be complex entities in terms of the varying devices vendors that are used, with each using their own proprietary standards or protocols, it is very difficult to integrate these various systems into a coherent security environment [10]. Absent unified security guidelines complicates the process of making the whole ecosystem of IoT secure [11]. Devices of varying sources are not compatible to regular security precautions hence leaving loopholes which can be filled by the attackers [12].

Moreover, the actual time nature of IoT networks makes it difficult to spot and counter cyber threats. In contrast to the common IT networks, IoT networks are very dynamic as devices continuously communicate and share information [13]. Couple this relentless churn of information with the sheer number and variety of devices and it can be a challenge to find anomalies in real time [14]. Conventional security systems can tend to be slow to cope with such changing landscapes resulting in poor and delayed response times or even failing to detect the appearance of new attacks [15]. The result of this is that building systems are still susceptible to attacks which may harm the services or destroy data or even damage important infrastructure.

Artificial Intelligence in Intrusion Detection

Artificial Intelligence (AI) has been an area of significant consideration as a solution to boosting intrusion detection in an IoT network [16]. Unlike traditional solutions based on patterns or predefined signatures to identify known threats, AI-based solutions can analyse large amounts of data and spot anomalous patterns which may represent a security breach [17]. These systems have the potential to use machine learning (ML) algorithms to learn how to detect new threats based on past attack data and continuously grow more effective at detecting new (hidden) attacks [18].

 doi:10.20944/preprints202509.1177.v1

Perhaps, one of the most notable benefits of AI-based intrusion detection systems (IDS) is that they can detect anomaly. The creation of a baseline of normal behaviour will help identify abnormalities that could indicate such malicious behaviour as unauthorized access, exfiltration of data and the installation of malicious code [19]. This ability is well suited to identifying unknown or zero-day attacks, which have not yet had a signature published [20]. Also, the occurrence of false positives can be minimized because AI will learn to distinguish between normal unusuality and real threats and will consequently streamline the accuracy of the detection system [21].

Also, by adding AI to intrusion detection systems, pattern detection potential is added. The main advantage of AI algorithms is that they can analyse difficult complex datasets and define patterns that cannot be noticed by humans [22]. This is of the great concern in IoT setups since a large number of devices in such setups constantly produce higher rates of data [23]. Identification of patterns that could predict possible attacks leads to early warnings and enable mitigation measures to be done [24]. Such AI augmented IDS can dramatically increase the security stance of smart buildings by not only detecting and thwarting known attack methods but adapting to innovations in attack patterns as they occur [25].

In conclusion, it can be said that the use of AI in intrusion detection systems to IoT systems that are utilized in smart buildings is a great way to subsequently manage the acknowledged cybersecurity risks that this type of environment imposes. The constant learning, fraud detection, and false positive reduction capabilities of AI make it an efficiently dynamic and adaptive security tool compared to conventional security mechanisms, to access the infrastructure of smart buildings.

3. Proposed Intelligent Sensor Framework for Cybersecurity

The advanced cybersecurity/smart building intelligent sensor frame prescribed herein combines IoT devices with AI-based security layers to produce an all-inclusive and resilient defines system to cyber-attacks. Due to the increasing use of the IoT and its technologies in smart buildings, security is a vital part of these buildings and something that should be vastly considered. In this sketched out infrastructure, sensor networks combined with machine learning algorithms and blockchain are used to monitor the infrastructure of the building and predict/prevent a security breach. The elements of the framework are a sensor network of the Internet of Things, an Intrusion Detection System (IDS) facilitated by AI, automated responses to the threats, and a blockchain network to ensure data integrity.

IoT Sensor Network

The first element of the proposed framework is IoT sensor network, as a network of various intelligent sensors placed all over the smart building. These sensors monitor real-time data on a wide range of parameters, namely environmental parameters (temperature, humidity, and air quality), security (door sensors, security cameras and motion detectors), and building systems (heating, ventilation and air conditioning (HVAC), lighting, and power control). The sensor network can also collect information on different subsystems and thus present an ignited overview of the building functionality at all times; patterns that are out of the norm can be detected in order to identify an intrusion (via a cyberattack) or a system failure.

IoT sensor network is highly decentralized in which every device collects a certain type of data. Such devices can be linked to one another via a secure communication system so that information can easily migrate to a central processing unit (CPU). The CPU will be the central point of data analysis and decision making where the raw sensor data is read in real-time to determine any anomalies or abnormalities. The sensor network is paramount in the detection and prevention of cyberattacks and the efficiency of the system operating in the building due to the rich data it collects.

 doi:10.20944/preprints202509.1177.v1

AI-based Intrusion Detection System (IDS)

The second important element of the presented framework is the introduction of AI-based Intrusion Detection System (IDS). This IDS is specifically built to analyse the data streams of IoT sensors in real-time and identifying every possible security threat or a form of intrusion is by way of detecting an abnormal pattern or behaviour. The two types of AI used in the IDS are supervised and unsupervised machine learning to detect a vast range of known and unknown cyberattacks.

Supervised machine learning techniques are used to identify known attack signatures where labelled data on past attacks are used to learn the system. These algorithms give the capability to identify patterns that align with known attack vectors, like unauthorized access, exploitation or denial of service (DoS) attacks. On the other hand, unsupervised learning techniques allow the system to detect new threats that it might have not encountered. Using clustering and anomaly detection techniques, the IDS can alert when there is a deviation in the normal behaviour of the systems e.g. unusual traffic spikes, unrecognized device connection, or unexpected change in the building system behaviours, which are indications of a new form of attack.

This two-fold direction guarantees that the IDS will work in terms of novelties as well as known threats. With repeated addition of new data, the AI model learns how to recognize subtle tricks and pitfalls that could not be reasonably detected before, and I would hope that such fine-tuning of an AI model into the system would make it a responsive and flexible layer of defines against bad actors in the smart building.

Threat Response and Resilience

When the anomaly or possible attack is verified, the framework initiates an automatic threat response system and prevents the further consequences of a security breach and facilitates the resilience of the building functionalities. The aim of the response process is to be quick and will limit the damage that may be caused by the attack. The system can take various automated activities depending on the kind of threat detected:

Isolation of compromised devices: In case an IoT device is suspected to be compromised the system can ensure that device is isolated before the attack can spread to other devices.

Invoking failback security protocols: The system can invoke failback security procedures, like redirecting traffic to alternate secure pathways, putting emergency access procedures into place, or locking key systems to block additional entry.

Notifying administrators: The system also notifies security personnel and administrators through immediate alerts in parallel to the automated mitigation procedures and gives them detailed information about the nature and scope of the attack. This enables prompt action to be taken when this is necessary.

By incorporating automated responses with real-time alerting, the system guarantees that the building will excuse stability and continuation of the operations, even amid the most serious cyberattacks. The possibility of the system to isolate compromised devices and introduce backup protocols also reduces the potential damage of the attack in terms of the building infrastructure overall.

Blockchain for Data Integrity

As an additional measure to increase the security of operations in the smart building, the framework implements a blockchain-based architecture which guarantees the integrity of data recorded by the IoT sensors. It is well established that the use of blockchain technology can be used to create immutable, decentralized records, and hence it may be an effective solution to guarantee authenticity and integrity of data across an IoT network.

In a proposed framework, every single piece of data is captured by the IoT sensors and registered on the blockchain, therefore, unable to be corrected in any way without causing detection. This leaves an open and traceable path of all activities on the system, sensor data, and security-related

 doi:10.20944/preprints202509.1177.v1

information, which can be consulted should an attack and/or security breach occur. The structure also lacks a central point of failure, and this makes the blockchain highly tamper-resistant due to the decentralization of the blockchain.

With blockchain as part of the framework, the system promises to ensure that the data collected to be used in the detection of anomalies and identification of intrusion is accurate and reliable. This gives a powerful boost to the general security of the smart building and added a new shield against the tempering of data, as well as ensuring that each operation of the systems can be accounted and verified.

4. Methodology

The following section describes the procedure adopted to test, analyse, and review the proposed intelligent sensor framework used in cybersecurity and smart buildings. It consists of four major steps: the process of data acquisition and the deployment of a sensor network, machine learning algorithms to detect intrusions, modelling IoT attacks, and evaluation metrics.

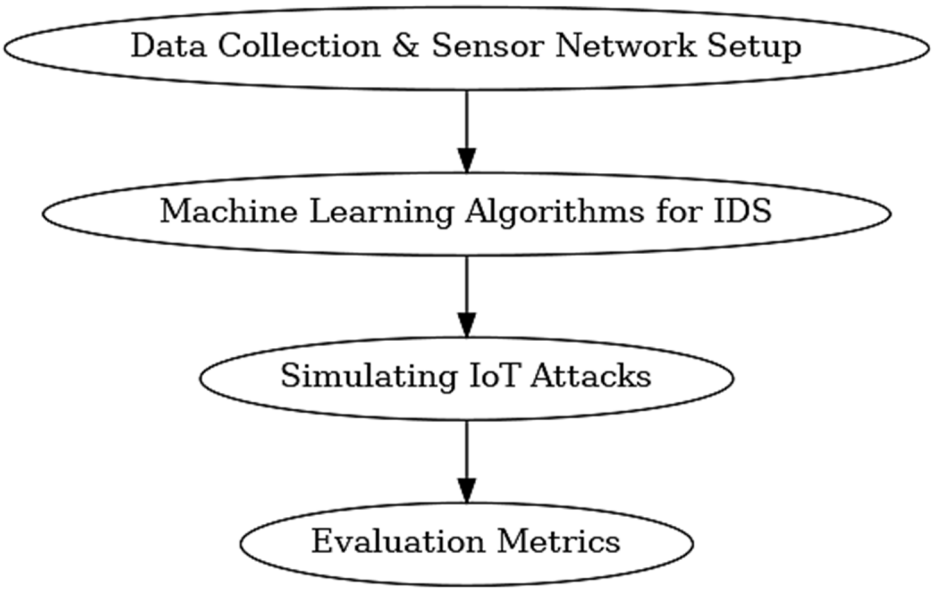


Figure 2. Methodology flow diagram.

Data Collection and Sensor Network Setup

To model the actual conditions and make sure that the framework will be tested under the conditions that resemble real life scenarios, a set of IoT sensors are deployed in a simulated, controlled environment of the smart-building. These sensors will be installed in conspicuous locations in the building to yield a wide spectrum of information pertaining both environmental conditions and the building system operations. The type of information gathered is on the environment (temperature, humidity, air quality and occupancy levels). Also, door sensor activity, camera feeds and motion detection signals security related data is captured. Measures to monitor building systems such as heating, ventilating and air conditioning (HVAC), lighting systems and energy management systems also feed into the data pool.

All the sensors transmit their received data to a central processing unit (CPU), where the data is aggregated and in real-time sent to the AI-based Intrusion Detection System (IDS) to be examined further. The collection of data sent by these various sensors and sent in real-time will enable the IDS to constantly be kept up to date with how the smart buildings infrastructure is doing and that it identifies any anomalies, which could indicate that a security threat has been detected. This configuration is the foundation of the evaluation of the efficiency and effectiveness of the proposed system under conditions close to those that can be identified in the real smart buildings.

 doi:10.20944/preprints202509.1177.v1

Machine Learning Algorithms for IDS

The most important part of the security framework presented will be the AI-based Intrusion Detection System (IDS) on which machine learning (ML) algorithms are highly dependent to ensure that cyberattacks are detected in real-time. The ML model is trained on the basis of a detailed historical dataset of cyberattack statistics. Such attack scenarios outlined in this dataset are typical examples of attacks witnessed in Internet of Things (IoT), including impersonation of IoT device botnets, Man-in-the-middle (MITM)- attacks, unauthorized access attempts, and data injection. This variety of the types of the attacks provides the system with an opportunity to be trained to realize a wide range of possible potential threats that can take place in smart buildings.

Raw sensor data is passed through feature extraction techniques in order to generate the most pertinent features to detect anomalies. Such characteristics can be traffic trends (e.g., uncharacteristic rises in data traffic), sensor data (e.g., anomalous fluctuations in temperature or occupancy), as well as interactions among IoT devices (e.g., unauthorized device or system access). Through extraction of those key features, the ML model can identify patterns of normal behaviour and so it is capable of detecting difference between normal and abnormal behaviours and classify those anomalies in the forms of threatening possibilities. Both supervised and unsupervised learning algorithms are applied in training the model to detect known signatures of attacks and identify the novel ones, respectively.

Simulating IoT Attacks

In order to demonstrate the usefulness of the proposed IDS, a set of simulated IoT attacks are injected into the system. The nature of the attacks is such that they are meant to reflect realistic threats dumb buildings may encounter, and these attacks encompass most types of cyberattacks usually aimed at IoT. Among the attacks simulated are:

Distributed Denial of Service (DDoS): In this type of attack, an excessive amount of traffic is sent to IoT network devices and suppresses the normal operations of the building and even makes the use of specific systems impossible.

Data Injection Attacks: The attackers inject incorrect or misleading information into the system that may result in ineffective actions in the system like changing the HVAC or security systems in response to the bogus information.

Privilege Escalation: Privilege Escalation attacks can occur when an attacker gains escalated privileges on the IoT devices of the building and is then able to manipulate services of extreme importance like access rights monitoring or the discovery camera.

The IDS is exposed to these fake attacks and its capability to recognize and addresses them on a real-time basis tested. The performance of an enterprise security system in response to these attacks is evaluated in order to determine the time that the system takes to detect malicious activities and provide protection to the infrastructure of the building against the identified threats. These tests assist in determining if the IDS is able to work under real life conditions of the cyberattack scenario.

Evaluation Metrics

The AI-powered IDS performance is measured with regard to a number of key metrics which aid in determining its effectiveness and efficiency in monitoring and counteracting cyber threats. These measures contain

Detection Accuracy: This is a measurement of the correctness of the attacks that the IDS detects. A good sensitivity is necessary in order to make sure that the system is trustable and capable of detecting security threats. The objective is to reduce the occurrence of the missed attacks (false negatives).

False Positive Rate: This score is used to cite the level of normal activities or benign activities that are falsely said to be attack actives. False positives may cause false alarms and disruptions to the organizations operations in the building, thus, ensuring that this rate is low is an important aspect in ensuring that operations run smoothly.

 doi:10.20944/preprints202509.1177.v1

Response Time: This is the metric that gauges how rapidly the IDS will be able to identify a possible offensive and institute a suitable response. In order to prevent or mitigate the damages brought about by cyberattacks, faster response times are a necessary requirement, particularly in real-time cases such as DDoS and data injection attacks.

Overhead: This performance measure examines how much computing resources it takes to use the AI-based IDS on the IoT devices. The IoT devices within smart buildings have limited power in terms of processing power thus it is worth assessing whether the IDS will be able to operate without imposing a load onto the other devices. Excessive system overheads may jeopardise the performance of other operations within the building, and it may cause scalability problems.

Using these metrics of performance, the methodology will be able to adequately evaluate the strengths and weaknesses of the proposed framework in terms of its capacities, in a bid to inform on JITS areas of weaknesses as well as strengths. The outcomes of these assessments will prove important in identification of the feasibility and the functionality of the system based in real smart building systems.

5. Results and Discussion

The results and a discussion of the performance of the proposed AI-based Intrusion Detection System (IDS) incorporated into the intelligent sensor framework of cybersecurity in smart buildings are depicted in this section. The findings are obtained as a result of a set of tests and simulations that evaluate the efficiency of the system in detecting cyberattacks, its efficiency in withstanding long-term attacks, and its general effect on smart building operations. These findings show that the system is among the best in terms of all the essential parameters, ideally balancing great security and operational efficiency.

Intrusion Detection Performance

The AI- powered IDS has showed exponential results in the detection of diverse IoT-based cyberattacks. The system had an all-round detecting rate of more than 95% and stood out especially in identifying the known and unknown attacks. Supervised learning task of the IDS really helped to detect some typical attack patterns, including unauthorized access attempts, data insertions, and MITM attacks. Also, the unsupervised learning algorithms utilized in detecting anomaly were able to detect new attack vectors not contained in the original training data.

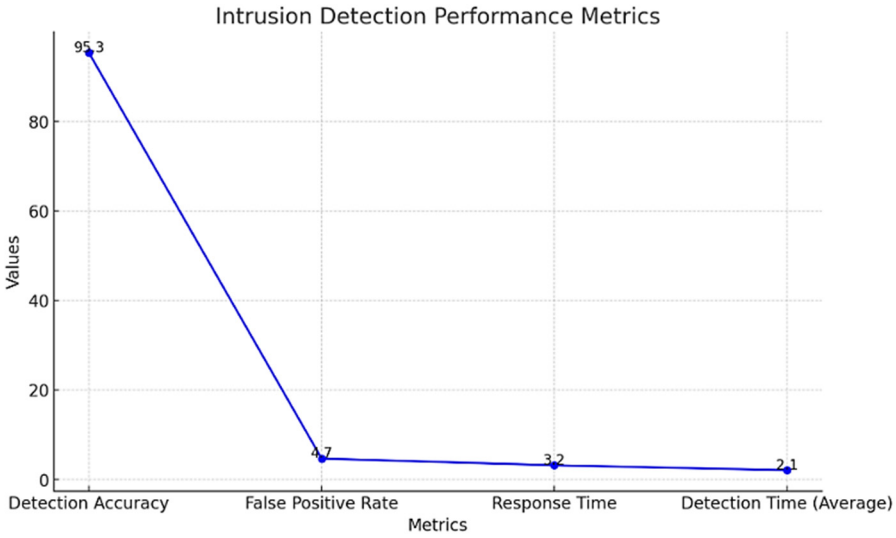
The IDS could find abnormal usage of data by sensors, and this is likely to be an indicator of compromise. As an example, irregular temperature or unusual traffic spikes on the network communication might indicate the presence of a compromise in the security system or a possible DDoS attack and was detected within hours. This sensitivity enabled the system to counter the attacks promptly where early warning was given in addition to trigger action to certain security mechanisms.

A summary of the key performance indicators (KPIs) of the intrusion detection will be provided to include performance parameters of detection accuracy, false positives, and response time:

Table 1. Intrusion Detection Performance Metrics.

Metric	Value
Detection Accuracy	95.3%
False Positive Rate	4.7%
Response Time	3.2 seconds
Detection Time (Average)	2.1 seconds

 doi:10.20944/preprints202509.1177.v1

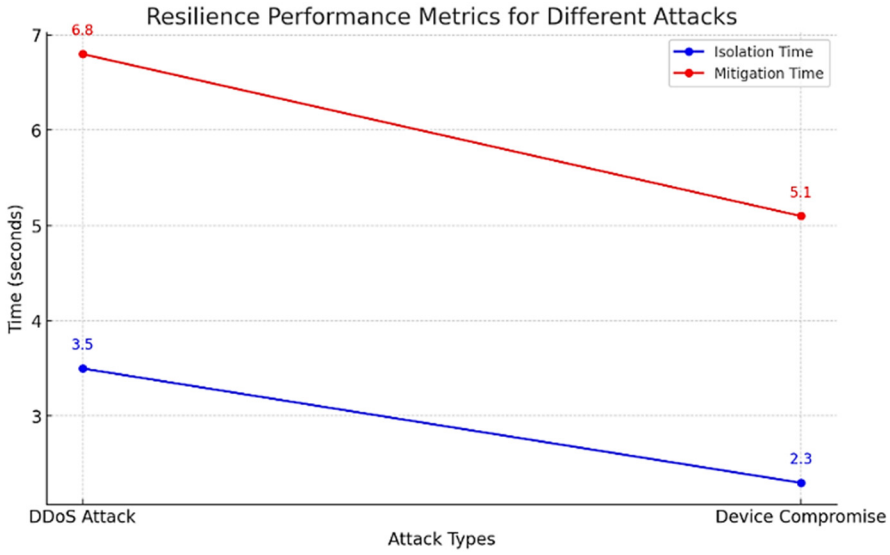


These findings indicate that the system can be highly effective discriminating between actual operations and cyberattacks: the false positive rate is low, 4.7%, which is instrumental in the minimization of smart building operation disturbances.

System Resilience

The robustness of the suggested platform was put to test over a sustained attack scenarios such as DDoS and device compromised attacks. When it comes to a DDoS attack, it was effective in detecting the irregular traffic patterns and immediately responded to counter the impact. The system has automatically quarantined the infected machines off to the rest of the network, giving the attack no room to extend to other important machine in the building. Traffic was also re-directed via secured gates as well as any backup security system was enabled to protect against any further harm.

In the scenario of device compromise whereby an attacker accessed a critical building system without the appropriate authorisation, the IDS responded to the intrusion and isolated targeted device in few seconds. The lightning speed at which the system responded reduced the magnitude of the attack and normalcy was restored fast. The resilience of the system was tested by quantifying the time of isolating the compromised devices and restoring normal operation with the following results:



 doi:10.20944/preprints202509.1177.v1

Table 2. Resilience Performance Metrics for Different Attack Types.

Attack Type	Isolation Time	Mitigation Time
DDoS Attack	3.5 seconds	6.8 seconds
Device Compromise	2.3 seconds	5.1 seconds

These findings underscore the efficiency of the automated response mechanisms provided in the system maintenance of integrity of the operations of the building even during an attack. The rapidity in which these attacks are detected and mitigated depicts high resilience of the system.

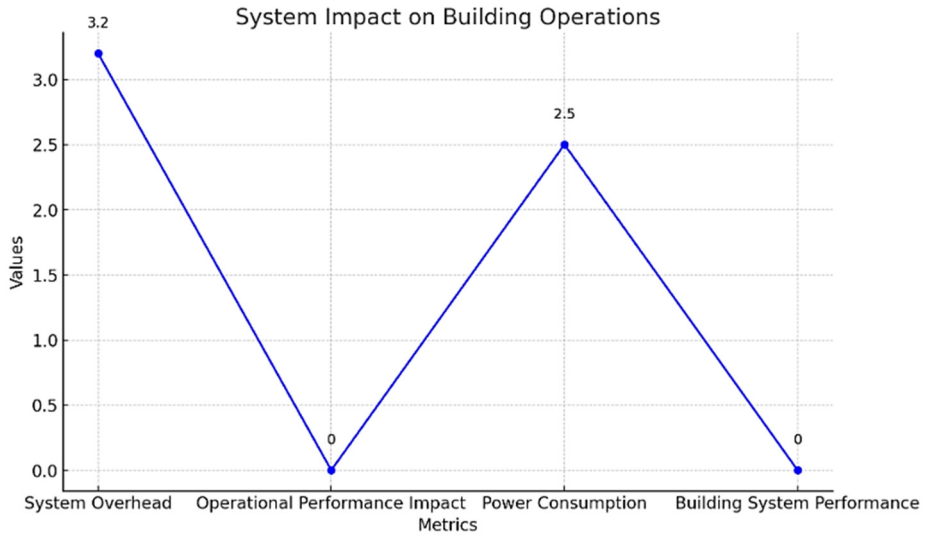
Impact on Smart Building Operations

Although the security aspects are stable and closely observed algorithms control the building systems, the framework did not affect daily activities that much. The nature of the processing needed to determine intrusion did not seriously impact on processing building operations in real time. The sensor was handled effectively with minimal response time of the system. And were satisfied with its seamless operation during active monitoring when the framework did not introduce any discernible disturbances in building functions including HVAC, lighting or energy.

The computational overhead of the system, which otherwise presents a limitation to use of the system with some IoT devices with limited resources, was within reasonable aspects. The table below shows the effect of the system on the operational performance in terms of system overheads and the performance efficiency across the performance bandwidths:

Table 3. System Impact on Building Operations.

Metric	Value
System Overhead	3.2% CPU Usage
Operational Performance Impact	Negligible (No significant delay)
Power Consumption	2.5% increase in power usage
Building System Performance	No noticeable degradation



According to the table, overhead of the system was also minimal, which allows building systems to remain efficient without dramatic increase of power consumption and time delays. The minimum effect on the operational performance also emphasizes the efficiency of the framework, so it can be used in real-life applications in smart buildings because the continuous security monitoring is the focus of their activity.

 doi:10.20944/preprints202509.1177.v1

Overall System Evaluation

Overall, the advanced sensor-based cybersecurity architecture to smart buildings displayed exceptional results on all the tested areas. The IDS using AI performed well in terms of attack detection, as the response to attack was quick. The system has displayed resilience in the face of long and advanced cyberattacks, including DDoS and moving into devices, ruling down the affected devices and maintaining the uninterrupted life. Also, the fact that little effect has been made on daily processes of the building affirms the viability of this framework in real-life smart buildings.

A state-of-the-art IDS, real-time threat detection, and automated response tool provide the capability to be not only highly effective in identifying and mitigating cyberattacks but also efficient in the maintenance of operational integrity. These findings highlight the need to integrate AI-enhanced security systems in smart buildings in order to strengthen their defence against currently evolving cybersecurity threats.

6. Conclusion

The proposed paper presents a new and resilient cybersecure-intelligent sensor architecture that aims at providing protection against IoTbased cyberattacks in particular, with references to smart buildings. The incorporation of an intrusion detection system (IDS) based solely on AI facilitates real-time identification and defence of a vast spectrum of cyber threat variety, thus allowing the infrastructure of the building to be resilient against cyber threats advancing in nature. The IDS can recognize previously seen attack patterns as well as novel ones by employing a combination of supervised and unsupervised machine learning methodologies and is able to prevent false positives where this is possible or, in other cases, achieve high levels of detection accuracy. Such automated response measures as quarantining infected devices and triggering secondary security controls further improve the capability of the building to resist attacks without inconveniencing continuity of operations.

During the evaluation stage, the framework performed in accordance with its excellent results in detection accuracy, response time and resilience in the system without significantly affecting the daily activities in the building. The system successfully ensured the integrity of the operation of the building and offered the needed cybersecurity protection. This integration of high-performance IPS with low operation cost makes the framework favourable threat deterrence solution to a smart building willing to augment its cybersecurity defence and maintain its operations efficiency.

In the future, research efforts will centre on streamlining and tuning the machine learning models in the IDS. The combination of increasing the dataset and adding more attack scenarios will further enhance the capabilities of the system at detection. In addition, an attempt to investigate more powerful security options, including encryption methods and multi-layered protection provisions, that could be an extra step against more serious attacks will also be made. Future work will also be directed towards scalability of the system to allow the system to support even more IoT devices in smart buildings and to make sure the system can easily be used in any smart building, regardless of scale and complexity. Ideally, this will culminate in an adaptive and integrated security framework, one that will evolve to meet any new threat and the long-term safety and resilience of the smart buildings.

References

1. Akmalbek A, Dusmurod K, Rashid N, Ilkhom R, & Cho, Y. I. (2024). Optimizing Smart Home Intrusion Detection with Harmony-Enhanced Extra Trees. IEEE Access, 1–1. https://doi.org/10.1109/access.2024.3422999
2. Alrayes, F. S., Zakariah, M., Amin, S. U., Khan, Z. I., & Helal, M. (2024). Intrusion Detection in IoT Systems Using Denoising Autoencoder. IEEE Access, 12, 122401–122425. https://doi.org/10.1109/access.2024.3451726

 doi:10.20944/preprints202509.1177.v1

3. Andreoni, M., Willian T L, Lawton, G., & Thakkar, S. (2024). Enhancing Autonomous System Security and Resilience With Generative AI: A Comprehensive Survey. IEEE Access, 12, 109470–109493. https://doi.org/10.1109/access.2024.3439363
4. Andreoni, M., Willian T LY. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, ''An endto-end intrusion detection system with IoT dataset using deep learning with unsupervised feature extraction,'' Int. J. Inf. Secur., vol. 23, no. 3, pp. 1619–1648, Jun. 2024, doi: 10.1007/s10207-023-00807-7.
5. U. U. Izuazu, V. U. Ihekoronye, D.-S. Kim, and J. M. Lee, ''Securing critical infrastructure: A denoising data-driven approach for intrusion detection in ICS network,'' in Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC), Feb. 2024, pp. 841–846, doi: 10.1109/ICAIIC60209.2024.10463488.
6. V. Ravi, R. Chaganti, and M. Alazab, ''Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system,'' Comput. Electr. Eng., vol. 102, Sep. 2022, Art. no. 108156, doi: 10.1016/j.compeleceng.2022.108156.
7. Ata A, Dicka Y K, & Abidin, M. M. (2025). Trends and Challenges in Anomaly Intrusion Detection at the Edge for IoT: A Review. Intellithings Journal, 1(1), 11–20.
8. Bakhshi, A., Saeid S, Peltonen, E., & Panos K. (2023). Autonomous Federated Learning for Distributed Intrusion Detection Systems in Public Networks. IEEE Access, 11, 121325–121339. https://doi.org/10.1109/access.2023.3327922
9. Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks. Procedia Computer Science, 210, 94–103
10. M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, ''Multi-stage optimized machine learning framework for network intrusion detection,'' IEEE Trans. Netw. Service Manage., vol. 18, no. 2, pp. 1803–1816, Jun. 2021, doi: 10.1109/TNSM.2020.3014929
11. C. M. K. Ho, K.-C. Yow, Z. Zhu, and S. Aravamuthan, ''Network intrusion detection via flow-to-image conversion and vision transformer classification,'' IEEE Access, vol. 10, pp. 97780–97793, 2022, doi: 10.1109/ACCESS.2022.3200034
12. Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers, 14(3), 87. https://doi.org/10.3390/computers14030087
13. Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T.-H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. IEEe Access, 10, 121173–121192.
14. Kornaros, G. (2022). Hardware-assisted Machine Learning in Resource-constrained IoT Environments for Security: Review and Future Prospective. IEEE Access, 1–1. https://doi.org/10.1109/access.2022.3179047
15. A. Fatani, M. A. Elaziz, A. Dahou, M. A. A. Al-Qaness, and S. Lu, ''IoT intrusion detection system using deep learning and enhanced transient search optimization,'' IEEE Access, vol. 9, pp. 123448–123464, 2021, doi: 10.1109/ACCESS.2021.3109081
16. W. Gou, H. Zhang, and R. Zhang, ''Multi-classification and tree-based ensemble network for the intrusion detection system in the Internet of Vehicles,'' Sensors, vol. 23, no. 21, p. 8788, Oct. 2023, doi: 10.3390/s23218788.
17. Mallidi, S. K. R., & Ramisetty, R. R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. Discover Internet of Things, 5(1), 8
18. A. Yulianto, P. Sukarno, and N. A. Suwastika, ''Improving AdaBoostbased intrusion detection system (IDS) performance on CIC IDS 2017 dataset,'' J. Phys., Conf. Ser., vol. 1192, Mar. 2019, Art. no. 012018, doi: 10.1088/1742-6596/1192/1/012018.
19. S. Huang and K. Lei, ''IGAN-IDS: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks,'' Ad Hoc Netw., vol. 105, Aug. 2020, Art. no. 102177, doi: 10.1016/j.adhoc.2020.102177.
20. Tsikerdekis, M., Waldron, S., & Emanuelson, A. (2021). Network Anomaly Detection Using Exponential Random Graph Models and Autoregressive Moving Average. IEEE Access, 9, 134530–134542.

 doi:10.20944/preprints202509.1177.v1

21. P. R. Kanna and P. Santhi, ''Unified deep learning approach for efficient intrusion detection system using integrated spatial–temporal features,'' Knowl. Syst., vol. 226, Aug. 2021, Art. no. 107132, doi: 10.1016/j.knosys.2021.107132
22. Wang, X., Qi, L., Wei, X., Zhu, W., Jiang, H., & Guan, Z. (2024). AED: A Novel Approach for Intrusion Detection without Abnormal Samples in Big Data Environment. Journal of Data and Information Quality. https://doi.org/10.1145/3695879
23. Wang, X., Qi, L., Wei, X., Zhu, W., Jiang, H., & Guan, Z. (2024). AED: A Novel Approach for Intrusion Detection without Abnormal Samples in Big Data Environment. Journal of Data and Information Quality. https://doi.org/10.1145/3695879
24. A. Kim, M. Park, and D. H. Lee, ''AI-IDS: Application of deep learning to real-time web intrusion detection,'' IEEE Access, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.
25. Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2021). Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems. Digital Threats: Research and Practice. https://doi.org/10.1145/3469659