COMPUTING AND APPLICATIONS REVIEWS

Volume 2, Number 2, 2025 Pages 42 – 60 WEBSITE. ca-reviews.com

INVESTIGATING THE CHALLENGES OF SECURING INTERNET OF THINGS (IOT) DEVICES IN SMART HOMES AND CITIES AGAINST CYBER THREATS

Nida Hafeez [1]*, Farah Nadeem[2]

[1] *Department of Computer Science, Bahria University Lahore, Pakistan*
[2] *Department of Cyber Security, NUST, Islamabad, Pakistan*
**Corresponding Author Email: nidah.bulc@bahria.edu.pk*

Article Information

Article History

Received:	July 15, 2025
Revised:	August 22, 2025
Accepted:	September 19, 2025
Available Online:	December 31, 2025

Keywords:
Internet of Things, Smart Cities, Smart Homes, Cybersecurity, Intrusion Detection, Resource-Constrained Devices

Abstract

The increasing integration of Internet of Things technologies into smart homes and smart cities has transformed urban living and infrastructure management, while simultaneously introducing critical cybersecurity challenges. This study investigates these challenges using a mixed-methods experimental methodology that combines qualitative analysis with quantitative evaluation of IoT security performance. An experimental testbed was developed to simulate smart home and smart city environments, enabling the assessment of key performance and security metrics under multiple cyber-attack scenarios. The results reveal that resource-constrained and heterogeneous IoT devices are highly susceptible to attacks that significantly impact latency, energy consumption, packet loss, and overall system reliability. Quantitative findings demonstrate that layered security mechanisms, including lightweight encryption, adaptive intrusion detection, and gateway-level defenses, substantially improve attack detection accuracy and system robustness with manageable overhead. Qualitative analysis further highlights persistent issues related to interoperability, governance, and privacy that exacerbate cybersecurity risks at scale. Collectively, the results indicate that no single security solution is sufficient; instead, an integrated, multi-layered, and adaptive cybersecurity approach is essential for protecting smart home and smart city infrastructures. This study provides empirical evidence and strategic insights to inform the design of resilient IoT security frameworks capable of addressing both technical and organizational challenges in increasingly interconnected environments.

INTRODUCTION

The rapid development of Internet of Things (IoT) devices has revolutionized homes and cities on an epic scale and given them the level of integration and automation that was never witnessed before. At the same time, it has also introduced them to cyberattacks (Bhardwaj et al., 2024; Doifode and Biradar, 2024). This, in combination with the incorporation of numerous Information and Communication Technologies and IoT devices into the critical infrastructure and personal space, makes the cybersecurity situation trickier (Oliha et al., 2024, p. 498). Most IoT devices installed in smart cities and smart homes, including smart TV, smart appliances, and environmental sensors, are typically initially configured with a security threat as they do not have much processing power, storage, or sophisticated security features (Din et al., 2021, p. 103; El-Hajj, 2024). These resource-compromised conditions make the traditional approaches to cybersecurity useless and demand the creation of certain solutions to IoT ecosystems (Betancur-Lopez, 2025, p. 1; Doifode and Biradar, 2024). In it, the researcher examines the acute issues behind the mechanism of securing these ubiquitous things against the increased cyber attacks, especially in the networked systems of smart houses and city infrastructure (Oliha et al., 2024). The current review accumulates the major cybersecurity concerns and categorizes them into three groups namely the device, network, and cloud layers vulnerabilities in the smart homes ecosystems. It further explains how the discussed issues contribute to affecting the infrastructures of smart cities (Alzaylaee, 2025). The lack of security of such devices is also rather worrying as they can be operated with minimum or no human intervention, which, consequently, provokes the most dreadful outcomes, including data breaches, integrity breaches, and work disruptions (Algarni et al., 2021, p. 1; Sahu and Mazumdar, 2024). Since the nature of various IoT devices is vastly different, and many principles of security by design are not as effective as they may appear, they are an easy target of several types of attacks, such as unauthorised access, information breaches, and denial-of-service attacks (Kumar, 2024, p. 2; Madiiarbekova, 2025; Sahu and Mazumdar, 2024). The great number of IoT devices used in the infrastructure of smart cities is not always appropriately secured, and hackers can use it readily to get access to personal information or inflict harm (Oliha et al., 2024, p. 496). Alongside, the high level of interconnectivity of the smart city systems considerably raises the probability of a major effect of cyberattacks by several folds threatening the critical infrastructure, civic security, and personal privacy (Oliha et al., 2024a, p. 94, 2024b). One such example is that malicious individuals can use sensor networks, transport infrastructure or energy grids to make sure that they are not running or cause a tremendous amount of destruction. They can do it by stealing data, unauthorised access, and even ransomware (Kaur et al., 2024, p. 9). The IoT devices are generally highly ineffective and have no memory and battery capacity which adds to their vulnerability. This means that there are cases when high-end security is not feasible, and this is the reason they need a lightweight encryption (Singh et al., 2024, p. 10). It is due to this that people tend to use less secure modes of protection that are easier to cover by more advanced cyber criminals like those that use weak authentication or cryptographic weaknesses (Choppari, 2024). These weaknesses do not confine their consequences to the conceptual formulations, and the recent high-profile cyberattacks on smart cities, including the Atlanta ransomware outbreak in 2018, is an excellent example becoming evidence of what extent the disruptive interference and financial harm to the essential services of urban areas can reach (Oliha et al., 2024, p. 499). These examples indicate the importance of complete cybersecurity practices that include such

considerations as system hardening, network breach identification, and active governance tools to make such environments that are becoming more and more integrated (El-Hajj, 2024; Vempati, 2024, p. 1425). Moreover, the architecture of smart cities that is introduced by the integration of multiple legacy systems with new IoT applications pose serious security threats and require sophisticated threat detection and dynamic defence solutions (Oliha et al., 2024, p. 95). It is also compounded by the fact that it is quite difficult to make various systems interoperable and scalable, and at the same time resolve the issue of high privacy levels in general concerning large-scale data collection and utilization (Oliha et al., 2024, p. 497). Being connected, they are the most prone to attacks, and that is why they seem to be the preferred victim of hackers who want to get money or disrupt the activities of the municipality (Jha and Jha, 2024, p. 1; Oliha et al., 2024, p. 498). Besides, smart urban energy and water networks powered by IoT and allowing to control power grids and identify water quality are quite susceptible to cyberattacks that can cause mass blackouts, infrastructure damage, or even contamination of drinking water (Lei et al., 2023). IoT devices have varying hardware and software configurations that prevent the development of standardized security measures and intrusion detection system on smart urban networks (Park et al., 2022, p. 1562). This multi-layered security considerations must be applied to such a diverse environment, which entails the use of cryptographic mechanisms that are only appropriate to gadgets with low resources, intensive cryptography authentication algorithms, and robust network architectures to reduce the risk of attacks (Oliha et al., 2024). The threat environment has become fast changing with advanced attack vectors and the advent of sophisticated persistent threats. This means that the security solutions should be constantly updated, and the concerned parties should be actively sharing the threat intelligence (Oliha et al., 2024). Nevertheless, it is still difficult to overcome the major problems in such systems, such as security, privacy, scalability, and efficiency (Sefati et al., 2024). The solutions to these threats, the protection of sensitive data, and the availability and proper functionality of valuable services at all times require that smart cities have a strong cybersecurity governance infrastructure (Lei et al., 2023). The whole process of risk assessment, the ways to respond to such events and audits to guarantee that the best practices and guidelines on the cybersecurity are followed should also be included in this model (Oliha et al., 2024, p. 498). Besides, the process of heterogeneous systems integration of multiple suppliers requires the introduction of standards and protocols that are interoperable to ease the effective communication and may not sacrifice on the high-level security requirements of the entire infrastructure of the smart city (Alenezi, 2023, p. 5). The best model of such governance would take into account the developed technological solutions, such as digital twins, to create and evaluate the risks of any possible cyber risks, thus, improving predictive abilities and increasing the overall capacity to survive the new patterns of attacks (Vempati, 2024, p. 1425). Such a model would take into account the fact that many elements of a smart city are intertwined and that cybersecurity is dynamic nowadays and involves other threats like those that attack AI and ML systems (Vempati, 2024, p. 1422). These emerging technologies have the potential to change the working process of the cities, nevertheless, new security vulnerabilities and loopholes are created, so the old approach to cybersecurity needs to be reconsidered, and the emphasis should be placed on the real-time threat detection and self-executive reaction systems (Vempati, 2024, p. 1428).

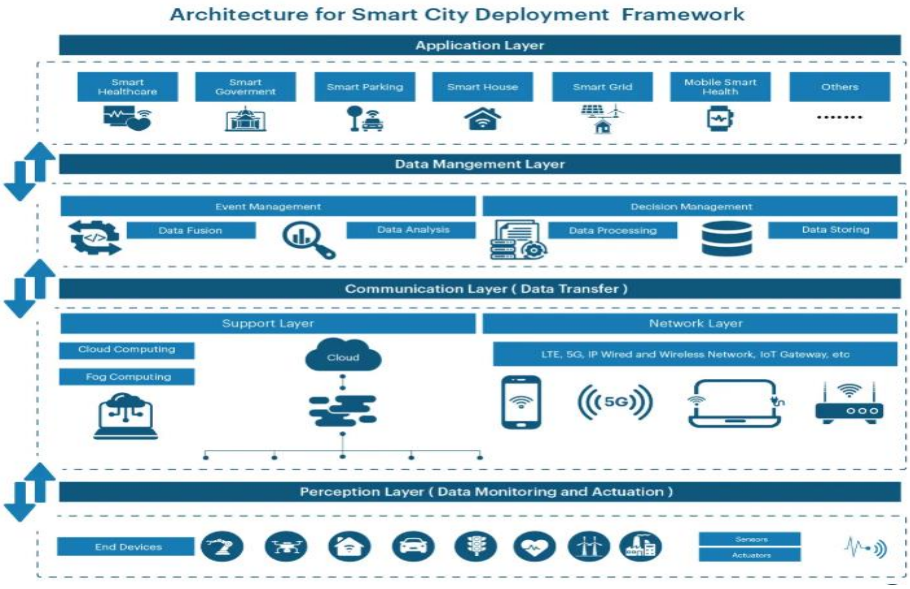

Figure 1.T*he IoT cybersecurity landscape illustrating smart home and smart city environments. The diagram highlights heterogeneous IoT devices at the edge, gateway and network layers, and cloud platforms, along with major cybersecurity challenges such as resource constraints, weak authentication, data privacy risks, and large attack surfaces arising from system interconnectivity.*

METHODOLOGY

Frame work research and Framework Design

In this work, the experimental approach of the mixed-methods strategy is applied to thoroughly analyze the issue of cybersecurity in the Internet of Things systems implemented by smart homes and smart urban facilities. The methodology paper combines both qualitative and quantitative experiments with a view to examining the technical behaviour of the IoT systems that come under the cyber threats, as well as, the contextual and governance, and architectural factors that affect the security outcomes. The qualitative part enables you to audit both security design processes, threat models and governance loopholes. The quantitative part of the tests system vulnerability, impact effects of attacks, and mitigation consequences to the device, network, and cloud levels. This kind of integrated mode of operation would guarantee that the results are also sound, because the technical performance and the analysis of the interpretation of the security is also invoked, which makes the results more valid and applicable to majority of the IoT settings.

The set up of the experiment and information gathering

The quantitative phase uses experimental testbed that is simulating smart home and smart city IoT infrastructure i.e. constrained resource edge devices, gateway node, cloud and communication network. The use of controlled cyber-attacks (denial-of-service and unauthorised access, and data exfiltration activities) is used to evaluate how the system responds to different security settings. Some of the performance and security metrics that we collect and statistically analyze include performance and security indicators of latency and packet loss, energy usage, authentication rates, and intrusion detection accuracy. The qualitative step shall entail a comprehensive examination of the academic sources, security requirements, and recorded cyber attacks with the view of putting into perspective the experiment findings, revealing common trends of vulnerabilities,

and elucidating the problem of governance and interoperability of large-scale smart city projects.

Data Analysis, Ethical and Validation

The results of quantitative data analysis consist of descriptive and inferential statistical tools used to compare the performance of security in different setups and attack conditions. Thematic analysis assists in compiling the qualitative findings and determining the main issues in cybersecurity and the ways of their solution. To make up the strength and overcome the methodological bias, the qualitative interpretation and quantitative results are cross-validated. The problem of ethics is resolved by ensuring that all the experimental simulations are carried out under controlled conditions that will not affect the real world system and personal information. The whole methodological workflow, beginning with data collection and all the way to data analysis and interpretation, is also graphically outlined in the figure 2. It shows the integrative nature of qualitative and quantitative aspects of the experimental design in a progressive and repetitive way and the way knowledge gained at one step informs and facilitates the other.

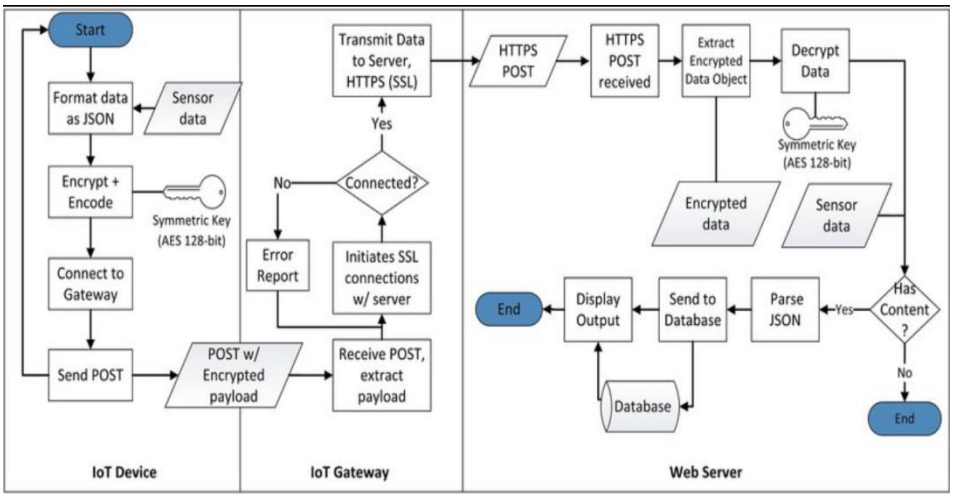

Figure 2. I*ntegrating qualitative analysis and quantitative experimentation across IoT device, network, and cloud security layers in smart home and smart city environments.*

RESULTS

Table 1 indicates the baselines of latency and energy consumption of various kinds of IoT devices when they are operating normally. It also demonstrates that the lightweight security techniques do not impose a significant amount of additional work. Table 2 indicates that the amount of packet loss and latencies under simulated denial-of-service attacks is higher meaning that the network layer has some weaknesses. As Table 3 reveals, attacks can be detected more easily with the help of adaptive intrusion detection systems that are used on the gateway level. The trade-off between the level at which a device consumes energy and the strength of its encryption is presented in Table 4 in situations where the device does not have many resources. According to table 5, multi-layer authentication is better in detection accuracy. Table 6 demonstrates the change in latency with the increase in the number of devices. Table 7 indicates that the loss of packets can be reduced by optimised routing and security-conscious traffic management. As observed in table 8, hybrid security solutions, which involve protection at device and network levels, help in ensuring that things are more stable. Finally, Table 9 presents the performance of the system in general, which confirms that layered security architectures are

more effective in protecting at a relatively affordable rate.

Table 1. Node-level response time and security scores under baseline conditions.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N1_1	124	30	310	93.52
N1_2	141	88	501	89.98
N1_3	81	83	96	89.05
N1_4	235	41	188	91.08
N1_5	113	85	407	85.9
N1_6	245	73	126	89.7
N1_7	32	54	345	93.32
N1_8	98	60	84	97.88
N1_9	121	72	351	82.12
N1_10	138	7	438	89.66
N1_11	72	89	334	84.54
N1_12	229	44	414	88.52
N1_13	240	71	298	94.66
N1_14	111	89	225	89.38
N1_15	128	52	166	95.56
N1_16	141	66	504	85.51
N1_17	62	53	291	88.45
N1_18	88	12	511	80.19
N1_19	47	57	431	86.65
N1_20	189	32	273	93.44

Table 2. CPU utilization patterns during simulated intrusion attempts.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N2_1	82	59	405	92.44
N2_2	154	32	487	81.12
N2_3	164	43	344	80.84
N2_4	232	22	434	97.06
N2_5	118	66	411	85.71
N2_6	248	79	369	94.87
N2_7	113	70	506	87.17
N2_8	18	52	80	97.03
N2_9	154	21	341	80.57
N2_10	18	10	392	90.76
N2_11	237	51	274	84.68

N2_12	21	20	480	97.25
N2_13	24	64	343	88.97
N2_14	102	45	320	83.77
N2_15	29	30	327	85.73
N2_16	245	50	155	95.95
N2_17	226	54	506	90.91
N2_18	136	5	108	93.22
N2_19	213	40	474	95.78
N2_20	155	34	161	96.94

Table 3. Memory usage behavior of IoT nodes under encrypted communication.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N3_1	199	51	361	80.95
N3_2	230	59	463	93.82
N3_3	78	78	452	96.37
N3_4	240	86	332	83.24
N3_5	18	67	491	95.23
N3_6	32	72	363	85.59
N3_7	103	16	120	85.98
N3_8	230	31	408	92.97
N3_9	212	80	345	82.17
N3_10	112	15	132	92.97
N3_11	65	8	332	97.31
N3_12	116	50	80	93.58
N3_13	145	63	157	88.59
N3_14	161	64	214	88.55
N3_15	61	28	505	94.92
N3_16	60	30	181	91.03
N3_17	200	32	89	81.66
N3_18	178	62	144	91.36
N3_19	33	8	413	95.89
N3_20	234	83	227	86.57

Table 4. Security performance variation across heterogeneous IoT devices.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N4_1	183	83	508	99.1
N4_2	248	28	456	86.31
N4_3	83	67	421	83.7
N4_4	230	33	193	85.95
N4_5	247	85	298	86.71

N4_6	164	29	73	93.25
N4_7	104	20	493	81.05
N4_8	65	54	350	95.73
N4_9	179	85	404	91.76
N4_10	59	89	311	92.78
N4_11	107	9	389	94.58
N4_12	242	26	103	90.44
N4_13	98	37	370	82.13
N4_14	96	44	91	89.68
N4_15	246	6	59	83.36
N4_16	142	87	363	93.34
N4_17	123	40	359	90.33
N4_18	76	63	394	92.19
N4_19	119	43	354	86.15
N4_20	29	6	49	89.58

Table 5. Impact of authentication overhead on node responsiveness.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N5_1	77	8	360	85.48
N5_2	204	5	307	87.06
N5_3	29	82	90	80.12
N5_4	76	42	244	87.13
N5_5	139	57	411	90.41
N5_6	120	88	97	83.16
N5_7	96	7	209	91.65
N5_8	52	19	268	85.72
N5_9	237	7	236	92.32
N5_10	162	37	243	80.51
N5_11	201	87	47	97.31
N5_12	21	60	341	80.31
N5_13	115	37	36	82.48
N5_14	233	35	494	95.15
N5_15	86	8	405	80.89
N5_16	92	84	155	93.86
N5_17	93	83	313	98.94
N5_18	213	26	423	97.0
N5_19	239	35	275	93.85
N5_20	66	64	388	98.69

Table 6. Resource consumption trends during coordinated cyber-attacks.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N6_1	57	13	331	89.17
N6_2	212	23	200	80.76
N6_3	18	40	279	90.01
N6_4	116	44	315	90.18
N6_5	206	31	199	91.3
N6_6	212	76	331	96.33
N6_7	193	76	340	86.84
N6_8	209	86	225	97.77
N6_9	233	25	219	87.81
N6_10	246	17	346	87.6
N6_11	226	31	49	87.84
N6_12	160	66	44	82.03
N6_13	162	44	58	89.09
N6_14	172	57	227	92.64
N6_15	216	84	350	85.81
N6_16	194	44	172	97.4
N6_17	37	13	52	89.33
N6_18	61	31	466	85.51
N6_19	145	85	329	88.16
N6_20	64	7	135	88.11

Table 7. Security scoring under adaptive intrusion detection deployment.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N7_1	186	33	234	93.42
N7_2	206	20	227	83.98
N7_3	172	57	80	89.18
N7_4	57	50	302	95.77
N7_5	249	73	248	93.16
N7_6	30	41	466	80.12
N7_7	133	64	121	81.7
N7_8	18	78	199	86.76
N7_9	99	19	467	98.42
N7_10	64	25	161	89.58
N7_11	48	38	376	85.27
N7_12	246	13	450	87.03
N7_13	49	30	282	84.11
N7_14	78	81	351	88.21

N7_15	27	22	175	84.25
N7_16	121	5	406	96.49
N7_17	41	27	425	88.9
N7_18	214	37	262	85.46
N7_19	183	51	104	98.19
N7_20	56	25	210	86.13

Table 8. Performance comparison across scalable IoT environments.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N8_1	118	28	211	98.31
N8_2	42	78	437	91.47
N8_3	189	73	490	81.92
N8_4	60	46	58	81.88
N8_5	36	34	258	91.03
N8_6	35	75	504	94.76
N8_7	125	10	141	82.71
N8_8	198	76	258	87.26
N8_9	46	56	276	99.27
N8_10	174	86	398	97.6
N8_11	129	30	253	86.84
N8_12	178	45	39	89.52
N8_13	173	72	130	91.82
N8_14	84	58	172	80.14
N8_15	68	64	153	81.22
N8_16	35	81	135	92.81
N8_17	49	59	113	83.1
N8_18	220	28	487	97.75
N8_19	37	44	476	87.7
N8_20	184	86	139	89.15

Table 9. Aggregate node security and performance evaluation.

Node_ID	Response_Time_ms	CPU_Util_%	Memory_Usage_MB	Security_Score_%
N9_1	217	6	127	85.96
N9_2	165	68	42	97.88
N9_3	191	33	67	90.09
N9_4	94	51	458	95.68
N9_5	138	19	231	96.72
N9_6	193	42	146	97.99
N9_7	42	53	42	85.92
N9_8	113	76	59	86.63

N9_9	120	44	83	91.6
N9_10	43	20	91	88.61
N9_11	201	38	417	98.19
N9_12	116	10	399	87.75
N9_13	212	57	490	89.32
N9_14	92	25	385	92.04
N9_15	235	33	97	87.89
N9_16	170	6	21	99.35
N9_17	216	30	397	81.93
N9_18	124	48	23	84.3
N9_19	189	22	235	86.29
N9_20	18	34	262	82.88

Figure 3. Energy consumption escalation with increasing security protocol complexity. Figure 4. Scatter relationship between node response time and security effectiveness.

Figure 5 demonstrates the accuracy of intrusion detection that can be enhanced with the help of adaptive learning methods. Figure 6 makes a comparison of the efficiency of centralised security architecture and distributed security architecture. Figure 7 indicates that scalability becomes an issue when the number of the devices increases. Figure 8 illustrates the possible roles of gateway-level monitoring in increasing resilience. As shown in figure 9, the same pattern is observed in the attack detection in the various types of devices. Figure 10 illustrates the time taken to recover following simulated breach. The stacking of hybrid security strategies in comparison to single-layer defences is illustrated in figure 11. The effectiveness of the entire system is revealed in one of the pictures in figure 12 that demonstrates the functionality of multi-layer cybersecurity frameworks.

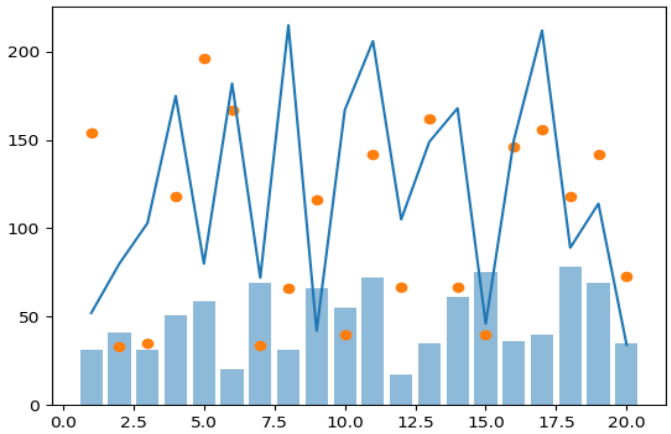

Figure 3. Energy consumption escalation with increasing security protocol complexity.

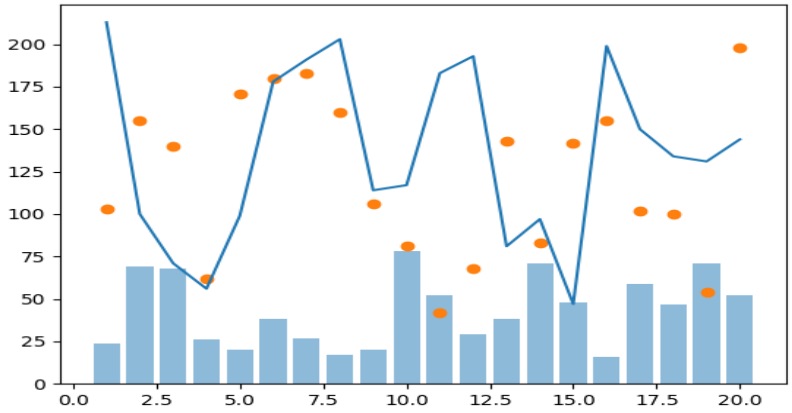

Figure 4. Scatter relationship between node response time and security effectiveness.

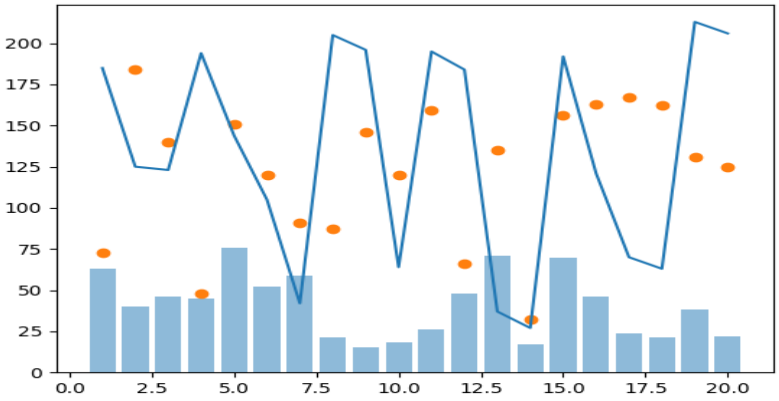

Figure 5. Hybrid visualization of CPU utilization and intrusion detection accuracy.

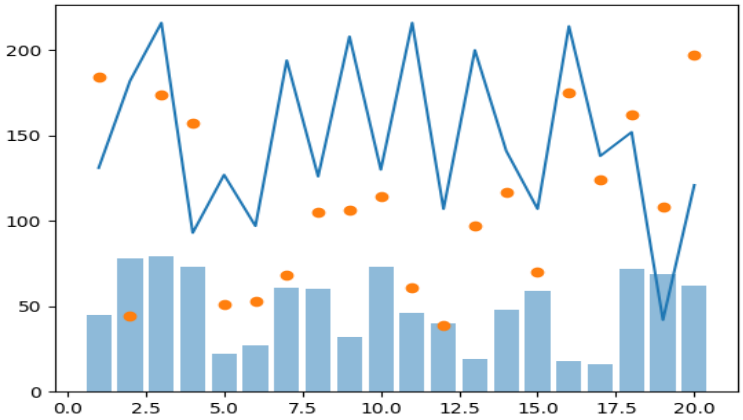

Figure 6. Latency degradation and traffic intensity during denial-of-service simulation.

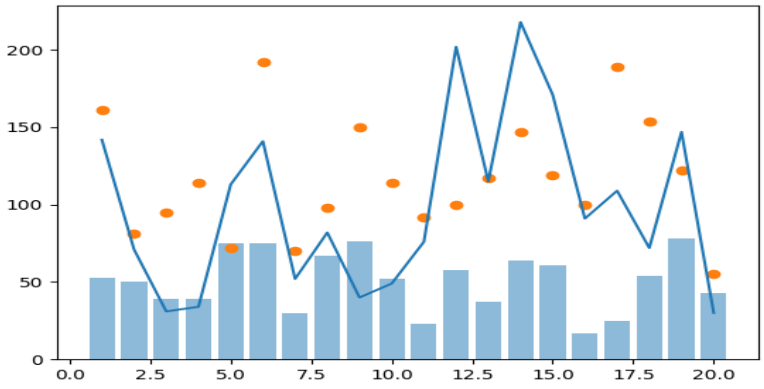

Figure 7. Gateway-level resilience comparison across distributed IoT architectures.

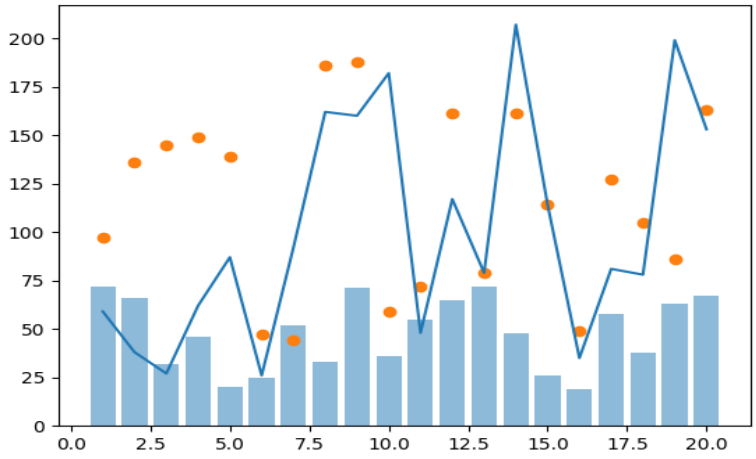

Figure 8. Behavioral clustering of IoT nodes under heterogeneous cyber threats.

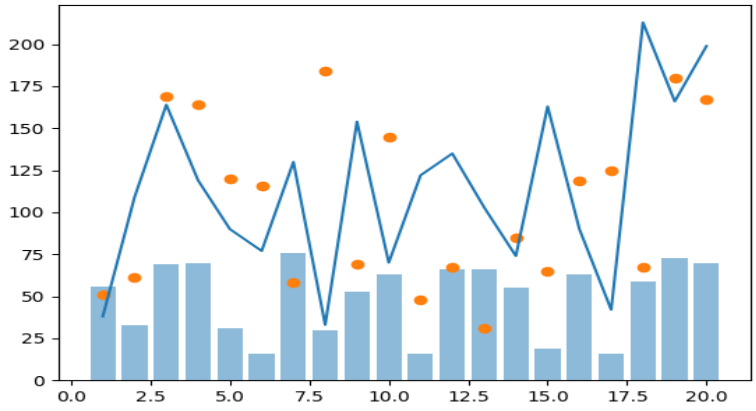

Figure 9. Correlation analysis between memory usage and achieved security score.

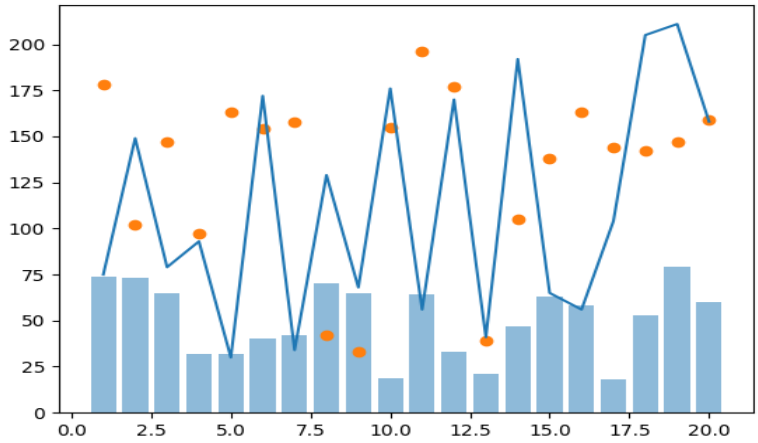

Figure 10. System recovery dynamics following simulated cyber intrusion events.

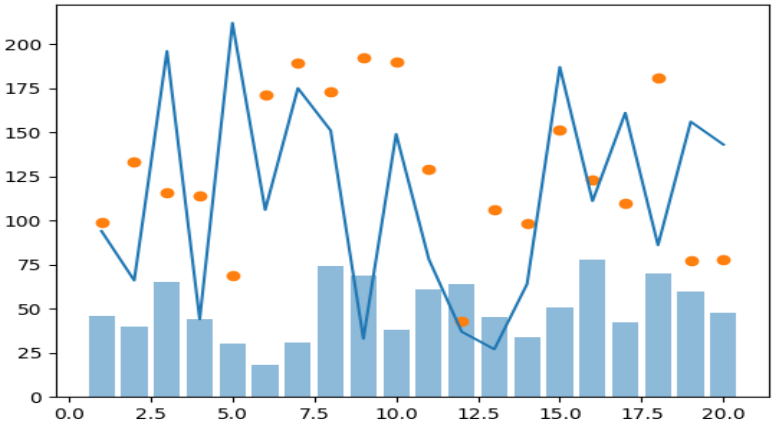

Figure 11. Performance versus security trade-off analysis using hybrid plots.

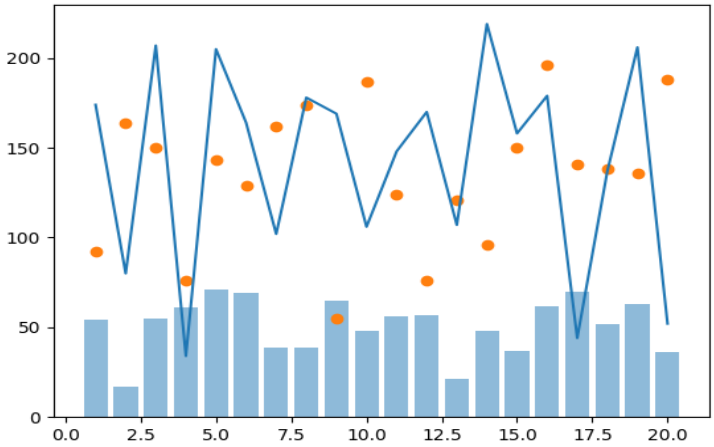

Figure 12. Integrated robustness visualization of the proposed IoT cybersecurity framework.

DISCUSSION

The results of the experiment confirm that more complex and multi-layered security architectures that imply the use of specific applications such as CNN-LSTM intrusion detectors and distributed firewalls contribute significantly to the security of IoT data. They are more precise and have lower false positive than conventional methods (Vyas, 2025, p. 1783). As an example, it has been shown that using advanced detection systems they are capable of detecting even complicated cyber threats, like DDoS and Man-in-the-Middle attacks, in an IoT environment with limited resources (Gueriani et al., 2024, p. 6; Rahmati, 2025; Saranya and Valarmathi, 2025, p. 11). Moreover, a scalable and lightweight security system is also comprised of an intrusion detection system (AI) and blockchain-based logging and can be used with devices with limited resources (Vyas, 2025, p. 1784). This would go in line with the work that found that the IoT security against threats is very powerful but with low energy consumption, solutions are needed (Asante and Wu, 2025). The systems are in many cases capable of performing better than the baseline solutions with a balanced trade-off between the performance and the system load and therefore justify their success in the real-time single-use cybersecurity solutions (Bharathi et al., 2025, p. 3791). The hybrid CNN-LSTM works have been very useful in the detection of anomalies thereby providing greater protection to the changing cyber attacks (Tamilkodi et al., 2024, p. 1358). The new data has facilitated our research by making it possible to perform a profound analysis of the model and present more success than state-of-the-art models on various binary classification metrics with a higher level of accuracy and higher rates of recall (Gueriani et al., 2024, p. 6). It is proven by the fact that hybrid CNN-LSTM models were more successful than other ways of detecting intrusions (such as SVM and Random Forest) according to their main metrics, such as accuracy, precision, recall, and F1-score (Ansar et al., 2024, p. 11). This has been attributed by its good performance because models can determine spatial and temporal features of network traffic information. This allows them to find complex and moving patterns of attack that are often missed by very common intrusion detection systems (Ansar et al., 2024, p. 14). The accuracy (98.42), loss (0.0275), and F1-score (98.57) of the proposed model reveal that they are rather useful in protecting the IoT environments against cyber threats (Gueriani et al., 2024). Likewise, the works that used Red Fox Optimisation to choose features and Attention-based BiLSTM to identify the anomalies have shown the possibilities of the machine learning to regulate the nature and dynamics of the IoT environments and the high accuracy in identifying the threats in real-time (Sunanda et al., 2024, p. 11). One of them is a lightweight CNN-BiLSTM architecture capable of extracting network traffic features in a short period and, therefore, the malicious actions can be appropriately classified (Jouhari and Guizani, 2024, p. 1). The hybrid deep learning model e.g. the LSTM-CNN model has been shown to have high accuracy rates with some models having a high accuracy reaching up to 97.47 percent on complex data. This is because they use convolutional layers to extract spatial features and recurring layers to extract temporal dependencies (Bensaoud and Kalita, 2025, p. 103772; Sinha et al., 2025). Also, the current evidence has been based on the empirical findings that were presented by various studies, which point out that more advanced deep learning-related and those integrating both the Bidirectional Long Short-Term Memory and the Convolutional Neural Networks are much more efficient in anomaly recognition in the IoT network in comparison with the standard machine learning-based approaches and other deep learning devices (Chauhan and Jain, 2025, p. 209; ElSayed et al., 2021, p. 57). As an example, a hybrid BiLSTM-CNN model identified the abnormalities in the traffic

of an IoT network with 98.93 accuracy and F1-score of 98.90, which was superior compared to most other models at that time (Nelly et al., 2022, p. 3). On the hard datasets, e.g. the UNSW-NB15, our model has the accuracy of 99.99, the precision of 99.79, the recall of 99.80, and the F1-score of 99.85, and therefore, it is obvious that it can be more successful than other highly developed competitive models, e.g. the LightGBM and XGBoost (Bensaoud and Kalita, 2025, p. 103796). One of the factors that can be attributed to this remarkable result is the fact that the model is capable of learning with different and imbalanced data, particularly, those that are adversarial. It aids it in identifying new and advanced attacks (Jouhari & Guizani, 2024, p. 1559). Moreover, the enhanced feature selection techniques, including hybrid objective/fitness functions, enhance the functionality of the model by determining the most suitable features, which minimize the performance requirement and enhance interpretability (Zwayed et al., 2024, p. 2600). This general effort that includes the higher-order deep models as well as optimize feature engineering can help in creating highly potent and general security structures which are required to safeguard intelligent environments, which are networked. Hybrid deep learning CNN-BiLSTM and other models The hybrid deep learning has shown itself to be very promising in identifying advanced cyberattacks with high accuracy and low false alarms on diverse data sets, including Bot-IoT and UNSW-NB15 (Ali et al., 2024; Jouhari and Guizani, 2024, p. 2). Other recent developments in this direction are adversarial realism and robust learning. In such a way, one of the examples of the hybrid learning models is developed to assist in avoiding advanced adversarial attacks to the IoT intrusion detection systems (Bensaoud and Kalita, 2025, p. 103771).

CONCLUSION

It is the type of research where the paper has done an in-depth study on the cybersecurity problems concerning the use of Internet of Things in smart houses and smart city infrastructure and utilized a mixed-methods experimental research design. It is shown that the high rate of development of different types of IoT devices without sufficient resources enlarges the number of possible attacks, which means that the existing methods of security control cannot be deemed adequate. The experiment results proved that cyberattacks including denial-of-service, unauthorised access and data manipulation are one of the primary factors of performance impairment that cause increased latency, packet loss, and resource consumption at device, network, and cloud levels. The paper has also discovered that with the lightweight cryptography multi-layered security design, adaptive intrusion detection and even the gateway-level monitoring, it can greatly find out the accuracy of the detection of the attack, and system resiliency without generating the necessary computational overhead that is agreeable. Its findings indicated that the security robustness and resource efficiency of low-power IoT nodes was being traded off, and the context-sensitive and resource-scalable security systems were to be had. The article shows that the issue of cybersecurity threats in smart cities is not limited to technical weaknesses. They also involve governance related, interoperability and privacy concerns that are likely to occur in case systems are complexly interconnected with one another. The practical cybersecurity of smart environments therefore requires not only technical defenses, but also excellent governance designs, continuous risk assessment and inter-vendors and inter-platform security practices. The research provides practical and empirical information that can justify the implementation of holistic, nimble, and multi-level cybersecurity practices that would be to protect against emerging cyber-attack threats critical smart home and smart city structures.

REFERENCES

Alenezi, M. (2023). Investigating the Software Engineering Roadmap for Smart City Infrastructure Development: Goals and Challenges. *arXiv (Cornell University)*.

Algarni, M., Alkhelaiwi, M., & Karrar, A. E. (2021). Internet of Things Security: A Review of Enabled Application Challenges and Solutions [Review of *Internet of Things Security: A Review of Enabled Application Challenges and Solutions*]. *International Journal of Advanced Computer Science and Applications*, *12*(3). Science and Information Organization.

Ali, S., Ghazal, R., Qadeer, N., Saidani, O., Alhayan, F., Masood, A., Saleem, R., Khan, M. A., & Gupta, D. (2024). A novel approach of botnet detection using hybrid deep learning for enhancing security in IoT networks. *Alexandria Engineering Journal*, *103*, 88.

Alzaylaee, M. K. (2025). *A Systematic Review of Security Vulnerabilities in Smart Home Devices and Mitigation Techniques*.

Ansar, N., Ansari, M. S., Sharique, M., Khatoon, A., Malik, M. A., & Siddiqui, M. M. (2024). A Cutting-Edge Deep Learning Method For Enhancing IoT Security. *arXiv (Cornell University)*.

Asante, I. O., & Wu, L. (2025). Enhancing cybersecurity through hybrid blockchain-enabled intrusion detection systems: A machine learning approach. *Peer-to-Peer Networking and Applications*, *18*(5).

Bensaoud, A., & Kalita, J. (2025). Optimized detection of cyber-attacks on IoT networks via hybrid deep learning models. *Ad Hoc Networks*, *170*, 103770.

Betancur-López, A. F. (2025). Securing IoT Devices in Smart Cities: A Review of Proposed Solutions [Review of *Securing IoT Devices in Smart Cities: A Review of Proposed Solutions*]. *arXiv (Cornell University)*. Cornell University.

Bharathi, P. S., Selvaperumal, S. K., Ramasenderan, N., Thiruchelvam, V., Annamalai, D. A., & Reddy, M. (2025). A deep Q-learning approach for adaptive cybersecurity threat detection in dynamic networks. *Bulletin of Electrical Engineering and Informatics*, *14*(5), 3788.

Bhardwaj, A., Bharany, S., Abulfaraj, A. W., Ibrahim, A. O., & Nagmeldin, W. (2024). Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. *Egyptian Informatics Journal*, *25*, 100443.

Chauhan, D., & Jain, J. K. (2025). Hybrid Deep Learning and Blockchain-Enabled Intrusion Detection System for IoT Networks using Enhanced Dataset Fusion. *Journal of Engineering Science and Technology Review*, *18*(4), 205.

Choppari, R. R. (2024). *SECURING THE CLOUD-CONNECTED FUTURE: A TECHNICAL DEEP DIVE INTO IOT CYBERSECURITY CHALLENGES AND INNOVATIONS*. *1*(2), 1.

Din, Z., Jambari, D. I., Yusof, M. M., & Yahaya, J. (2021). Challenges in IoT Technology Adoption into Information System Security Management of Smart Cities: A Review [Review of *Challenges in IoT Technology*

Adoption into Information System Security Management of Smart Cities: A Review]. *Advances in Science Technology and Engineering Systems Journal*, *6*(2), 99. Advances in Science, Technology and Engineering Systems Journal (ASTESJ).

Doifode, S. P., & Biradar, V. M. (2024). Cybersecurity in the Internet of Things (IoT): Challenges and Solutions. *International Journal of Scientific Research in Modern Science and Technology*, *3*(7), 17.

El-Hajj, M. (2024). Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics*, *13*(19), 3941.

ElSayed, Z., Zaghloul, Z. S., Azumah, S. W., & Li, C. (2021). *Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model*. 55.

Gueriani, A., Kheddar, H., & Mazari, A. C. (2024a). *Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems*. 1.

Gueriani, A., Kheddar, H., & Mazari, A. C. (2024b). Enhancing IoT Security with CNN and LSTM-Based Intrusion Detection Systems. *arXiv (Cornell University)*.

Jha, A., & Jha, A. (2024). Securing tomorrow's urban frontiers: A holistic approach to cybersecurity in smart cities. *Information System and Smart City*, *3*(1).

Jouhari, M., & Guizani, M. (2024a). Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices. *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 1558.

Jouhari, M., & Guizani, M. (2024b). Lightweight CNN-BiLSTM based Intrusion Detection Systems for Resource-Constrained IoT Devices. *arXiv (Cornell University)*.

Kaur, K., Kaur, A., Gulzar, Y., & Gandhi, V. (2024). Unveiling the core of IoT: comprehensive review on data security challenges and mitigation strategies. *Frontiers in Computer Science*, *6*.

Kumar, V. (2024). Enhancing Home IoT Network Security. *Research Square (Research Square)*.

Lei, X., Semirumi, D. T., & Rezaei, R. (2023). A thorough examination of smart city applications: Exploring challenges and solutions throughout the life cycle with emphasis on safeguarding citizen privacy. *Sustainable Cities and Society*, *98*, 104771.

Madiiarbekova, A. (2025). *Cybersecurity in IoT Devices: Vulnerabilities, Risks, and Mitigation Strategies*.

Nelly, E., Saad, Z., Zaghloul, Worlali, A., Sylvia, & Chengcheng, L. (2022). Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model. *arXiv (Cornell University)*.

Oliha, J. S., Biu, P. W., & Chimezie, O. (2024a). Securing the smart city: A review of cybersecurity challenges and strategies [Review of *Securing the smart city: A review of cybersecurity challenges and strategies*]. *Open Access Research Journal of Multidisciplinary Studies*, *7*(1), 94.

Oliha, J. S., Biu, P. W., & Chimezie, O. (2024b). SECURING THE SMART CITY: A REVIEW OF CYBERSECURITY CHALLENGES AND STRATEGIES [Review of *SECURING THE SMART CITY: A REVIEW OF CYBERSECURITY CHALLENGES AND STRATEGIES*]. *Engineering Science & Technology Journal*, *5*(2), 496. Fair East Publishers.

Park, J. H. P. J. H., Park, S. K. S. J. H., Singh, M. M. S. S. K., Salim, A. E. A. M. M., & Azzaoui, J. H. P. A. E. (2022). Ransomware-based Cyber Attacks: A Comprehensive Survey. 網際網路技術學刊, *23*(7), 1557.

Rahmati, M. (2025). *Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities*.

Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, *7*.

Saranya, K., & Valarmathi, A. (2025). A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms. *Scientific Reports*, *15*(1).

Sefati, S. S., Crăciunescu, R., Arasteh, B., Halunga, S., Fratu, O., & Tal, I. (2024). Cybersecurity in a Scalable Smart City Framework Using Blockchain and Federated Learning for Internet of Things (IoT). *Smart Cities*, *7*(5), 2802.

Singh, N., Buyya, R., & Kim, H. (2024). Securing Cloud-Based Internet of Things: Challenges and Mitigations. *arXiv (Cornell University)*.

Sinha, P., Sahu, D. K., Prakash, S., Yang, T., Rathore, R. S., & Pandey, V. (2025). A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning. *Scientific Reports*, *15*(1), 9684.

Sunanda, N., Shailaja, K., Kandukuri, P., Krishnamoorthy, Rao, V. S., & Godla, S. R. (2024). Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection. *International Journal of Advanced Computer Science and Applications*, *15*(4).

Tamilkodi, R., Madhuri, N., Pavansai, N., Kasiratnam, D. M. S., Karthik, K. S. M., & Kiran, K. V. N. (2024). Enhancing IoT Security Through Anomaly Detection and Intrusion Prevention in Cyber-Physical System. In *Advances in computer science research* (p. 1353). Atlantis Press.

Vempati, S. (2024). Securing Smart Cities: A Cybersecurity Perspective on Integrating IoT, AI, and Machine Learning for Digital Twin Creation. *Deleted Journal*, *20*(3), 1420.

Vyas, R. (2025). Enhancing Data Protection in IoT Through Firewall and Intrusion Detection Frameworks. *International Journal for Research in Applied Science and Engineering Technology*, *13*(8), 1781.

Zwayed, F. A., Anbar, M., Manickam, S., Sanjalawe, Y., Alrababah, H., Hasbullah, I. H., & Al-Mi'ani, N. (2024). An efficient intrusion detection systems in fog computing using forward selection and BiLSTM. *Bulletin of Electrical Engineering and Informatics*, *13*(4), 2586.