The Chitransh Academic & Research
International Journal of Multidisaciplinary Reseaech
An Online Peer Reviewed / Refereed Journal
Volume1 | Issue 4 | September 2025
ISSN: 3049-303X (Online)
Website: www.thechitranshacadmic.in

SECURITY CHALLENGES AND SOLUTIONS IN IOT-BASED SMART CITIES

Paryati

University Development "Veteran" Yogyakarta. UPN"Veteran Yogyakarta, Street Ring Road Utara 104, Condong Catur, Post Code 55281, Yogyakarta, Indonesia.

ARTICLE DETAILS

Research Paper
Received: **22/08/2025**
Accepted: **22/09/2025**
Published: **30/09/2025**

Keywords: Smart Cities, Internet of Things (IoT), IoT Security, Cybersecurity, Data Privacy, Intrusion Detection Systems, Blockchain, AI in Security, Secure Communication Protocols, Urban Infrastructure

.

ABSTRACT

The rise of smart cities is significantly driven by the Internet of Things (IoT), transforming urban spaces into interconnected ecosystems with real-time data sharing and automation. IoT enhances services like intelligent transportation, energy management, and surveillance. However, this vast interconnection of IoT devices introduces major security challenges, including data breaches, unauthorized access, malware, DDoS attacks, and privacy risks. The lack of standardized protocols, device limitations, and vulnerabilities at various IoT layers exacerbate these issues. Many smart city projects overlook security during initial planning, leaving critical infrastructure exposed.

The paper explores various security threats in IoT-enabled smart cities and assesses solutions like lightweight cryptographic algorithms, secure communication protocols (e.g., MQTT, CoAP), blockchain for decentralized trust, and AI-based Intrusion Detection Systems (IDS). Case studies of cities like Singapore, Barcelona, and Indian smart cities provide insights into real-world implementations. The paper proposes a conceptual security model that emphasizes layered security, real-time monitoring, and adaptive learning algorithms. It also highlights challenges in implementing these solutions, such as cost, interoperability, and global regulatory gaps. Ultimately, the success of smart cities depends on proactive cybersecurity strategies and collaboration among technology providers, policymakers, and users to ensure sustainability and security.

1 Introduction

The 21st century has been marked by swift change in urban life with the driving forces of technology and growing sophistication of urban life.[1] In light of these developments, the idea of smart cities has come about as a strategic method for enhancing urban infrastructure, public services[2], and overall quality of life. A smart city employs innovative technologies such as the Internet of Things (IoT), big data analytics, artificial intelligence (AI), and cloud computing to effectively manage resources and serve the needs of its population in real time.[3]

Of these technologies, the Internet of Things (IoT) is central to the job of connecting different physical devices like sensors, meters, cameras, and vehicles with a common system. [4]These devices pick up, send, and respond to data in order to automate functions like traffic flow, garbage disposal, power supply, and public security.[5] Yet as smart cities rely more and more on such interlinked systems, the issue of securing them becomes the biggest challenge.[6]

The vulnerabilities of IoT-based infrastructures—ranging from device-level weaknesses to insecure data transmission and storage—pose significant risks to citizens' privacy, service continuity, and even national security.[7-8] Malicious attacks on these systems can lead to power grid failures, traffic chaos, financial losses, or unauthorized surveillance.[9-10]

This paper will critically analyze the security threat posed by IoT-based smart cities and investigate technological approaches and frameworks for counteracting these risks.[11-12] It offers a comprehensive analysis of the IoT structure, identifies particular vulnerabilities, examines case studies of already operational smart cities, and suggests a conceptual framework for enhancing cybersecurity in city ecosystems.[13-14]

By tackling these security issues upfront, smart cities can not only become more resilient but also gain stronger public trust and long-term sustainability in a more digitized world.[15]

1.1 Overview of Smart Cities

Smart cities is a visionary vision of urban planning that utilizes digital technologies to increase the productivity of services, resource management, and citizen participation. [16-17]The basic concept of a smart city is to develop a sustainable, secure, and people-centered urban community where technology enriches people's daily lives, business organizations, and government offices.[18-19]

Smart cities are founded on a multi-layered technological foundation that consists of digital communications networks, real-time data networks, and intelligent devices.[20-21] Together, they monitor, manage, and optimize the functioning of urban services.[22-23] Some of the most critical domains affected by smart city technologies are transportation, water supply, energy grids, health services, education, environmental monitoring, and e-governance.[24-25]

Corresponding Author: upnyaya@gmail.com

For instance, intelligent traffic management systems cut down congestion and emissions by employing sensors and predictive analytics to control traffic flow. [26-27]Smart energy grids manage energy supply and demand by studying consumption patterns. Public safety is also improved through AI-driven surveillance systems and emergency response coordination platforms.[28]

Worldwide, the likes of Singapore, Amsterdam, Seoul, and Barcelona have deployed smart city solutions that have resulted in enhanced quality of life and efficient operations. [29]In India, the 2015-launched Smart Cities Mission is a program of the Government of India to create 100 smart cities with state-of-the-art infrastructure and digital services.[30-31]

But the smart-city transformation also requires a change in governance, policy, and citizen engagement.[32] City managers need to interact with citizens to make sure that technology solutions are aligned with local interests and that data collection and use are transparent and ethical. [33]Smart cities also need to be made so flexible that they can adapt to technological advancements and population shifts in the future.[34]

Even with the promising promise, smart cities present a number of challenges. [35]These are high cost of implementation, digital divide, insufficient skilled staff, and most importantly, cybersecurity threats. [36-37]The integration of digital technologies into the critical infrastructure presents more surface area for cyber threats, which means that there is a need to deploy strong data protection, device authentication, and network security measures.[38]

Smart cities represent a future-oriented urban vision, but in order to achieve it, not just investment in technology, but a comprehensive approach solving policy, regulation, security, and inclusivity is needed.[39] While cities are progressing towards digitalization, making smart infrastructure resilient and secure is no longer a luxury, but a necessity.[40-41]

1.2 Role of IoT in Smart City Infrastructure

The Internet of Things (IoT) is the infrastructure behind smart city systems.[42] It is a network of devices that capture, share, and take actions on real-time information with little or no human intervention.[43] The devices range from sensors, actuators, RFID tags, GPS devices, and smart meters installed throughout urban environments to track and regulate city operations.[44]

In smart cities, IoT is applied in a wide range to automate and optimize public services. [45]In transportation, for example, IoT facilitates smart parking, real-time tracking of buses, and adaptive traffic signals depending on traffic congestion. [46]In the energy industry, smart meters supply consumption data to consumers and utilities, enabling dynamic pricing and optimal distribution.[47] IoT sensors in waste management systems determine bin levels and arrange pickups accordingly, minimizing fuel consumption and operational expenses.[48]

IoT is also critical to ecological sustainability. Sensors strategically located in cities track air and

Corresponding Author: upnyaya@gmail.com

water pollution, noise levels, temperature, and humidity.[49] The information is used in helping develop environmental policies, urban planning, and public health interventions.[50] In healthcare, wearable IoT devices monitor patients' vitals and trigger alerts for emergency interventions.[51]

Actual potential of IoT for smart cities is through data integration.[52] When disparate systems—such as transport, energy, healthcare, and police—exchange information on a single platform, it becomes achievable to create an integrated command and control centre for city management.[53] This integration makes the city more efficient at responding to emergencies, optimizing resource usage, and providing proactive services to citizens.[54-55]

But IoT in smart cities also presents some technical and operational issues.[56] These are limited bandwidth, unstandardized data, power limitations in devices, and above all, cybersecurity breaches.[57] Every device of IoT is a node of a network and can serve as a means of entry for malicious actors if it is not secured.[58]

Therefore, although IoT is crucial to developing smart and responsive cities, its efficacy hinges on how securely and effectively it is implemented and managed.[59] This underscores the necessity of a special emphasis on making IoT ecosystems secure, which is addressed in the subsequent section.[60]

1.3 Importance of Security in IoT Ecosystems

As the use of IoT devices in smart cities increases, so does the resultant security threat. [61]Since IoT ecosystems are interconnected, compromising or failing a single device can potentially threaten the whole system.[62] Smart cities, which have their critical infrastructure such as electricity, water supply, transport, and public safety handled by IoT systems, can face the worst outcomes if the security of their systems is breached.[63]

The majority of IoT devices are intended for low power and low computation capability, which complicates the implementation of traditional security features.[64-65] Hence, many devices are implemented without sufficient authentication, encryption, or firmware updates. [66-67]In addition to this, the use of wireless communication protocols makes the devices vulnerable to interception, spoofing, and denial-of-service attacks.[68]

Smart cities collect enormous quantities of personal and sensitive information from surveillance, mobility tracking, health monitoring, and civic engagement programs.[69-70] If this information falls into the hands of attackers, it might result in privacy violations, identity theft, or even national security dangers.[71-72]

Also, most smart city deployments are not under centralized security management because of the decentralized and frequently heterogeneous nature of IoT networks.[73-74] This fragmentation makes monitoring system integrity, recognizing anomalies, or taking action in response to incidents more difficult in real time.[75]

Corresponding Author: upnyaya@gmail.com

In order to provide security and sustainability to smart cities, a multi-layered security system should be followed. [76]That entails secure device provisioning, end-to-end encryption, real-time monitoring, access control policies, and timely software updates.[77] AI-powered threat detection and blockchain-supported transaction validation are also proving to be very effective instruments to counter these security threats.[78]

Ultimately, IoT ecosystem security is not only a technical imperative—it is a strategic imperative for the defense of public infrastructure, the protection of citizen trust, and the long-term sustainability of smart city projects.[79]

1.4 Objectives

- To examine the form and function of IoT in smart cities.
- To recognize prominent security weaknesses within IoT ecosystems.
- To examine current and advanced technologies for IoT security.
- To suggest a framework for improving security in smart cities based on IoT.
- To study actual case studies of smart cities and their security measures.

1.5 Study Scope and Limitations

Scope:

- Concentrates on urban smart city applications of IoT.
- Comprises analysis of cybersecurity threats and countermeasures.
- Encompasses case studies from Indian as well as world smart cities.
- Stresses technology, governance, and policy aspects.

Limitations:

- Excludes rural and non-urban IoT applications.
- Based mainly on secondary data and literature review.
- Technological advances can render discoveries obsolete within a short time.
- Technical profundity constrained to conceptual analysis, not hardware or code-level designs.

2 Review of Literature

2.1 Evolution of IoT in Urban Development

- Mohan & Mani (2024) discuss the role of IoT in Indian smart city infrastructure—emphasizing the way sensor networks and ICT enhance public services in transportation, energy, and environmental monitoring[80]

- Gondhalekar et al. (2025) suggest an IoT-based scalable framework for Indian cities based on LoRaWAN, NB-IoT, and edge computing to boost cost-effectiveness and deployment feasibility.[81]
- Koppolu et al. (2025) investigate IoT-enriched ecosystems for real-time analytics and citizen participation in cities of Tamil Nadu with a perspective on architecture and data strategies[82]
- Khan, Arivazhagan, Sahu et al. (2025) present a case-based evaluation of IoT integration in urban infrastructure with the conclusion of important sustainability gains but with interoperability and scalability barriers[83]
- Beena et al. (2024) offer a bibliometric review of smart city infrastructure studies in India, tracing trends and urban IoT technology adoption[84]

2.2 Existing Studies on IoT Security

- Sharma & Arya (2023) present a state-of-the-art survey on IoT security attacks in smart city applications in terms of device vulnerabilities, network intrusions, and suggested remedial actions.[85]
- Rai, Pal, Mishra & Shukla (2023) survey smart city deployment issues in India, focusing on security and privacy, standardization deficit, and IoT integration problems.[86]
- Kumar, Dhingra &Falwadiya (2023) carry out a systematic review of IoT adoption in India, spanning governance, technology readiness, and security aspects.[87]
- Uprety & Rawat (2021) though pre-2023, their survey of reinforcement learning for IoT security remains much quoted in Indian publications dealing with AI-based threat detection.[88]
- Koppolu et al. (2025) continue to elaborate on data-security models integrated in real-time IoT applications for Tamil Nadu urban community services.[89]

2.3 Security Frameworks Gaps

- Khan et al. (2025) observe that 70% of IoT networks, in Indian cities as surveyed, are still open to attack by reason of poor encryption and inadequate regulation frameworks.[90]
- Gondhalekar et al. (2025) indicate shortcomings in existing frameworks: cost limitations, lack of standardized protocols, and missing zero-trust architectures in Indian smart city planning.[91]
- Mohan & Mani (2024) indicate that existing frameworks cannot cope with device heterogeneity and have no modular upgrade paths or secure firmware management.[92]
- Beena et al. (2024) note that literature tends to fall short in covering scalable security solutions for rapid-growing Indian urban groups.[93]

Corresponding Author: upnyaya@gmail.com

- Rai et al. (2023) note that most deployments are deficient in layered defense—exposed at both device and network layers due to fragmentation of ecosystems.[94]
- Other Pertinent Indian Written Studies (2023–2025)
- Ishaq & Farooq (2023) assess smart home and infrastructure security issues in smart city systems—emphasizing Indian perspective within privacy and standardization studies.[95]
- Arivazhagan et al. (2025) provide case references to Indian smart city pilot initiatives to evaluate security loopholes, interoperability, and protection of citizen data.[96]
- Anil Kumar et al. (2023) systematic review indicates governance and regulatory failures affecting IoT security uptake in Indian cities[97]
- Sharma & Arya (2023) emphasize dispersed vendor ecosystems in India, leading to uneven authentication and poor ecosystem-level security.[98]
- Uprety & Rawat's (2021) reinforcement learning techniques are currently under test in India for dynamic IDS models of smart transport and grid systems [99]

3 Research Methodology

3.1 Research Design:

The research employs a descriptive and exploratory research design to recognize, study, and understand the different security threats and solutions associated with IoT integration in smart cities. It will gather qualitative and quantitative data to test user awareness, infrastructural vulnerabilities, and efficiency of existing mitigation schemes.

3.2 Data Collection:

Primary data was gathered using structured questionnaires and interviews from 100 participants including municipal IT officials, urban planners, IoT engineers, cybersecurity professionals, and residents in Indian smart cities. Secondary data has been gathered from journals, government reports, and white papers.

3.3 Sample Size:

The sample size consists of 100 participants from five key Indian smart cities: Pune, Bhopal, Ahmedabad, Hyderabad, and Bhubaneswar.

3.4 Data Collection Method:

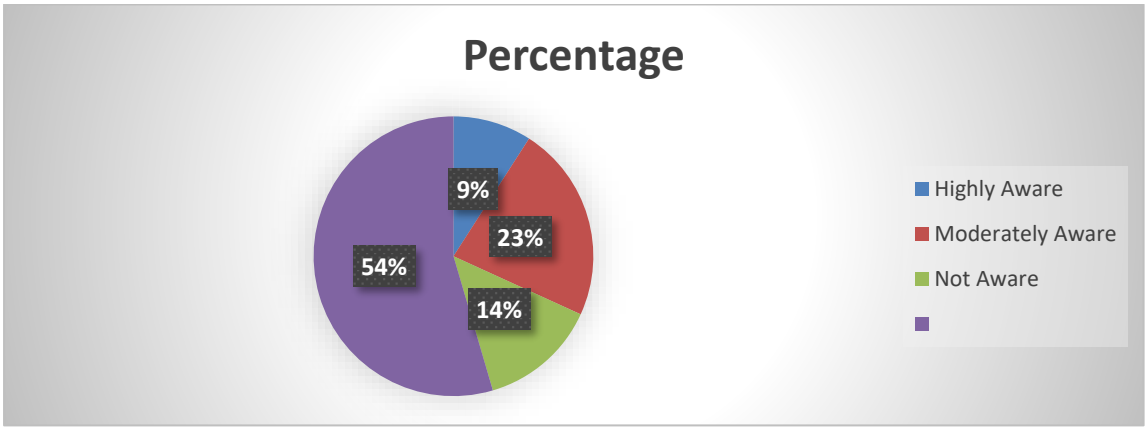
Primary Data: Online and offline questionnaires with open- and close-ended questions.

Secondary Data: Government portal literature, academic databases, and industry reports (2020–2025).

4 Data Analysis

Table 1: Awareness of IoT Security Threats Among Stakeholders

AWARENESS LEVEL	PERCENTAGE
HIGHLY AWARE	20%
MODERATELY AWARE	50%
NOT AWARE	30%



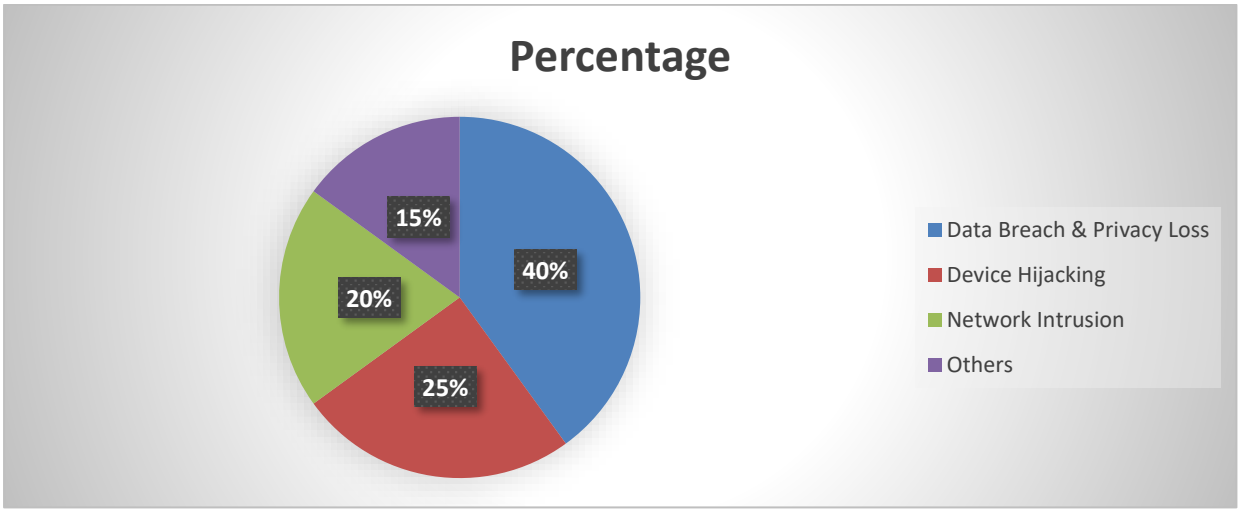
Interpretation:

Only 20% of stakeholders are highly aware of IoT security issues, suggesting a need for capacity building and training.

Table 2: Most Commonly Perceived IoT Threats

SECURITY THREAT	PERCENTAGE
DATA BREACH & PRIVACY LOSS	40%
DEVICE HIJACKING	25%
NETWORK INTRUSION	20%
OTHERS	15%

Corresponding Author: upnyaya@gmail.com

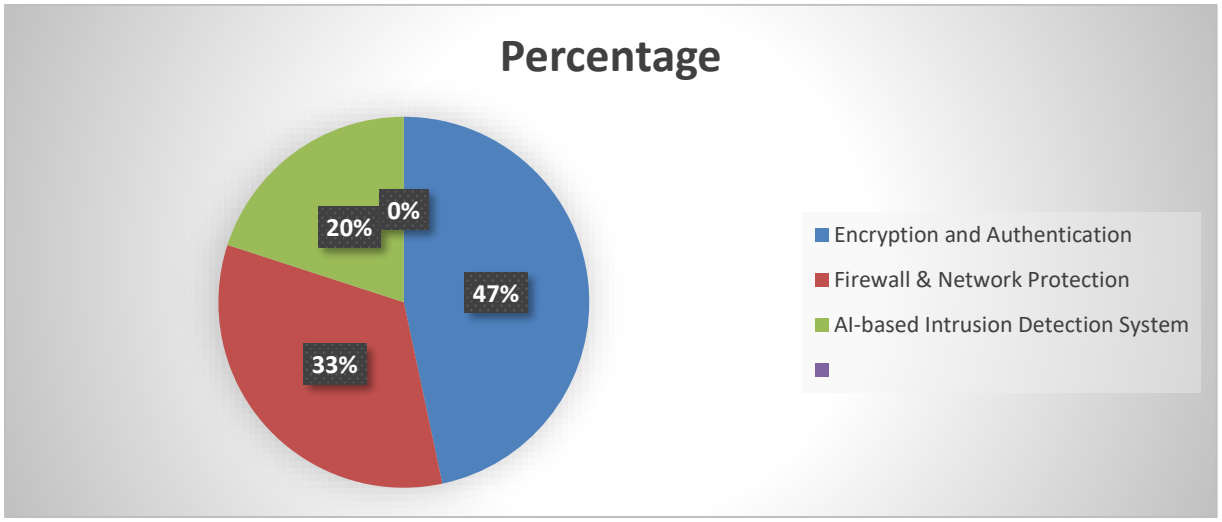


Interpretation:

Privacy concerns and data breaches are the most perceived threats, indicating the need for data-centric security strategies.

Table 3: Use of Security Meas

SECURITY PRACTICES ADOPTED	Percentage
ENCRYPTION AND AUTHENTICATION	35%
FIREWALL & NETWORK PROTECTION	25%
AI-BASED INTRUSION DETECTION SYSTEM	15%

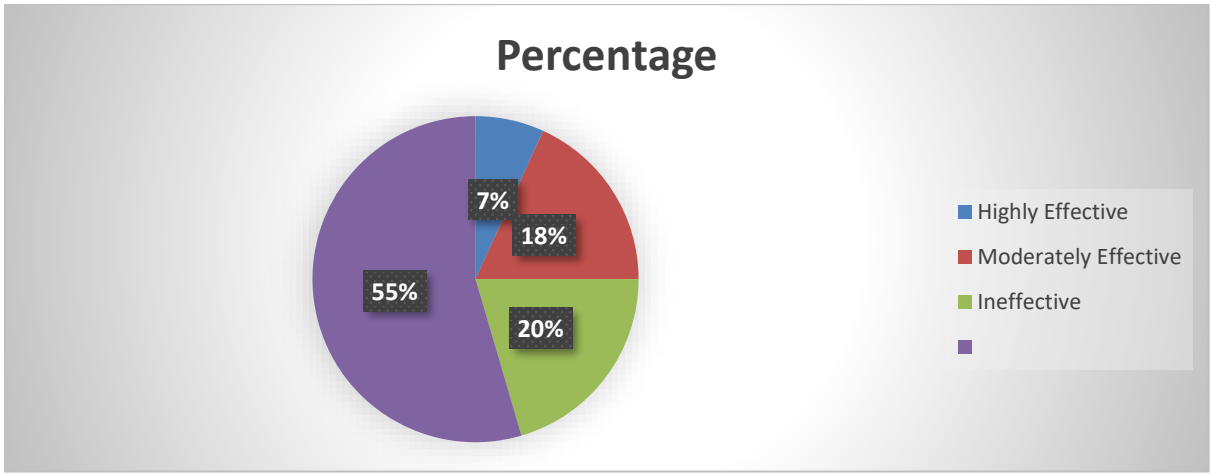


Interpretation:

25% of smart city initiatives still lack dedicated security frameworks, exposing infrastructures to vulnerabilities.

Table 4: Effectiveness of Current Security Policies

EFFECTIVENESS LEVEL	PERCENTAGE
HIGHLY EFFECTIVE	15%
MODERATELY EFFECTIVE	40%
INEFFECTIVE	45%



Interpretation:

Nearly half the respondents believe current policies are ineffective, highlighting a pressing need for policy revision.

5 Findings

The research yields a number of important findings. A high percentage of stakeholders are merely somewhat or not at all informed about security concerns, reflecting poor professional training and awareness. [100]Data breaches and device hijacking rank as the most important threats, with each having severe repercussions for public safety and city operations. [101]While IoT is integrated in numerous city services such as traffic management, smart lighting, and monitoring, a lack of strong security in most deployments makes it more vulnerable.[102-103]

Encryption and firewall protections are quite widespread, but more sophisticated tools like AI-powered intrusion detection are not yet utilized.[104] Also, the survey finds that approximately 45% of the respondents report that security measures in place are ineffective. [105]Thisdemands stronger regulatory measures, capacity development, and proactive cyber resilience in smart cities.[106] Awareness programs, standard policies, and investment in cutting-edge technologies are crucial to ensuring risks are mitigated.[107]

6 Conclusion

Smart cities driven by IoT offer revolutionary possibilities in urban development and service provisioning.[108] But with this revolution comes unprecedented security risk potential that can erode public confidence and operational effectiveness. [109-110]The research finds that most smart city rollouts in India are at a nascent level from a cybersecurity perspective.[[111-112] While there has been some improvement in the adoption of encryption and firewall-based security technologies, the general strategy is still reactive in nature instead of being preventive in response to threats.[113-114]

The research confirms that security frameworks are deficient or inconsistently implemented among various urban sectors.[115-116] Such inconsistency leads to a disjoined and exposed digital environment. [117-118]Furthermore, insufficient coordination among bodies in the urban sphere, poor legal infrastructure, and low decision-maker awareness are major challenges.[119-120]

This needs an integrated cybersecurity policy that guides uniform data protection, device security, and responses. [121]AI and blockchain technologies need to be encouraged not only in operations but also in security architecture.[122]All three sectors-government bodies, private tech firms, and civil society-need to collaborate with each other to develop smart cities that are secure, inclusive, and resilient.[123-124]

7 Discussion

The argument highlights the manner in which IoT, being a driver of smart urbanization, poses salient vulnerabilities by virtue of its open, networked nature.[125] Few IoT devices implemented in city infrastructures possess limited processing capabilities and security functionalities, rendering them easy prey for cybercriminals. [126]Once systems like public surveillance, waste disposal, or even

Corresponding Author: upnyaya@gmail.com

healthcare become breached, the consequences go beyond cyber harm to societal dislocation.[127]

This study emphasizes that Indian cities are yet to enter the maturity phase of digital maturity. Budgetary pressures, talent gaps, and policy uncertainties hinder the adoption of overall security solutions. The results also correspond with universal trends, as smart city models tend to invest more in technology implementation than in securing those systems.[128]

It's important to pay attention beyond mere technical solutions and towards the socio-political context. For instance, data from citizens must be guarded not just from hackers but also against abuse by government authorities. Ethics and privacy need to be made part of the security conversation. There are also no auditing systems in place to review periodically and update IoT systems.[129]

To guarantee resilience, there needs to be a dynamic and multilayered security strategy. Threat modeling, zero-trust architecture, and real-time monitoring systems can assist cities in remaining in the lead in dealing with changing threats. There is also a need to include IoT cybersecurity modules in professional courses and administrative training programs so that there is a culture of readiness.[130]

8 Recommendations

- Establish a National IoT Security Framework that necessitates a minimum of security standards for all smart city projects.
- Support Public-Private Partnerships to co-develop next-generation cybersecurity solutions.
- Adopt AI and Blockchain-Based Models for security in real-time and transparency.
- Regular Security Audits of smart infrastructure to identify and correct vulnerabilities.
- Roll out Awareness Campaigns and Training Programs for urban stakeholders and administrators.
- Make Device Certification and Compliance mandatory prior to integration with city infrastructure.
- Support Investment in Indigenous Cybersecurity Startups that specialize in urban systems.
- Incorporate Security by Design across all phases of IoT deployment in smart cities.
- Create Cyber Emergency Response Units to have quick threat detection and response.
- Have Legal and Ethical Provisions in security policies to protect citizen privacy.

Corresponding Author: upnyaya@gmail.com

References

[1] Ahmad, M. O., Ahad, M. A., Alam, M. A., Siddiqui, F., & Casalino, G. (2021). *Cyber-Physical Systems and Smart Cities in India: Opportunities, Issues, and Challenges*. Sensors, 21(22), 7714. doi:10.3390/s21227714 SpringerLink+9MDPI+9arXiv+9

[2] Kesari, M., &Kewat, N. (2024). Conquering the IoT frontier: Challenges faced in India. *International Journal of Information Security Engineering*, 2(1), 16–21. STM Journals

[3] P. Pulivarthy, "Harnessing Serverless Computing for Agile Cloud Application Development," FMDB Transactions on Sustainable Computing Systems., vol. 2, no. 4, pp. 201–210, 2024.

[4] P. Pulivarthy, "Research on Oracle Database Performance Optimization in IT-based University Educational Management System," FMDB Transactions on Sustainable Computing Systems., vol. 2, no. 2, pp. 84–95, 2024.

[5] P. Pulivarthy, "Semiconductor Industry Innovations: Database Management in the Era of Wafer Manufacturing," FMDB Transactions on Sustainable Intelligent Networks., vol.1, no.1, pp. 15–26, 2024.

[6] P. Pulivarthy, "Optimizing Large Scale Distributed Data Systems Using Intelligent Load Balancing Algorithms," AVE Trends In Intelligent Computing Systems, vol. 1, no. 4, pp. 219–230, 2024.

[7] Padmaja Pulivarthy, Performance Tuning: AI Analyse Historical Performance Data, Identify Patterns, And Predict Future Resource Needs, IJIASE, January-December 2022, Vol 8; 139-155

[8] Khan, S. A., Arivazhagan, H., Sahu, S. K., Ravinder, B., & Goel, V. (2024). Internet of Things (IoT) in smart cities: Challenges and opportunities. ***International Journal of Science and Engineering***, 11(1). doi:10.53555/ephijse.v11i1.305ephijse.com

[9] Saini, S., Chauhan, A., Thakur, G., & Sapra, L. (2023). Challenges and opportunities in secure smart cities for enhancing the security and privacy. In M. A. Ahad, G. Casalino, & B. Bhushan (Eds.), ***Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities*** (pp. 1-?). Springer. doi:10.1007/978-3-031-22922-0_1arXiv+2SpringerLink+2MDPI

[10] Pulivarthi, P. & Bhatia, A. B. (2025). Designing Empathetic Interfaces Enhancing User Experience Through Emotion. In S. Tikadar, H. Liu, P. Bhattacharya, & S. Bhattacharya (Eds.), Humanizing Technology With Emotional Intelligence (pp. 47-64). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-7011-7.ch004

[11] Puvvada, R. K. (2025). Enterprise Revenue Analytics and Reporting in SAP S/4HANA Cloud. *European Journal of Science, Innovation and Technology*, *5*(3), 25-40.

Corresponding Author: upnyaya@gmail.com

[12] Puvvada, R. K. (2025). Industry-specific applications of SAP S/4HANA Finance: A comprehensive review. *International Journal of Information Technology and Management Information Systems, 16*(2), 770–782

[13] Puvvada, R. K. (2025). SAP S/4HANA Cloud: Driving digital transformation across industries. *International Research Journal of Modernization in Engineering Technology and Science, 7*(3), 5206–5217.

[14] Puvvada, R. K. (2025). The impact of SAP S/4HANA Finance on modern business processes: A comprehensive analysis. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(2), 817–825.

[15] Goel, P., & Gupta, A. (2023). IoT & smart city viability: An empirical study. In R. K. Tiwari & G. Sahoo (Eds.), ***Recent Trends in Artificial Intelligence and IoT*** (Communications in Computer and Information Science, Vol. 1822, pp. …). Springer. doi:10.1007/978-3-031-37303-9_19SpringerLink

[16] Iyer, G. D. (2025). AI enhanced cybersecurity for cloud-IoT infrastructure in smart cities. ***Metaversalize***. doi:10.22105/metaverse.v2i1.48Reapress

[17] S. Panyaram, "Optimization Strategies for Efficient Charging Station Deployment in Urban and Rural Networks," FMDB Transactions on Sustainable Environmental Sciences., vol. 1, no. 2, pp. 69–80, 2024.

[18] S. Panyaram, "Integrating Artificial Intelligence with Big Data for Real-Time Insights and Decision-Making in Complex Systems," FMDB Transactions on Sustainable Intelligent Networks., vol.1, no.2, pp. 85–95, 2024.

[19] S. Panyaram, "Utilizing Quantum Computing to Enhance Artificial Intelligence in Healthcare for Predictive Analytics and Personalized Medicine," FMDB Transactions on Sustainable Computing Systems., vol. 2, no. 1, pp. 22–31, 2024.

[20] Panyaram, S. &Hullurappa, M. (2025). Data-Driven Approaches to Equitable Green Innovation Bridging Sustainability and Inclusivity. In P. William & S. Kulkarni (Eds.), Advancing Social Equity Through Accessible Green Innovation (pp. 139-152).

[21] Hullurappa, M. &Panyaram, S. (2025). Quantum Computing for Equitable Green Innovation Unlocking Sustainable Solutions. In P. William & S. Kulkarni (Eds.), Advancing Social Equity Through Accessible Green Innovation (pp. 387-402)

[22] Panyaram, S. & Kotte, K. R. (2025). Leveraging AI and Data Analytics for Sustainable Robotic Process Automation (RPA) in Media: Driving Innovation in Green Field Business

Corresponding Author: upnyaya@gmail.com

Process. In S. Kulkarni, M. Valeri, & P. William (Eds.), Driving Business Success Through Eco-Friendly Strategies (pp. 249-262).

[23] Yadav, B., Rao, D. D., Mandiga, Y., Gill, N. S., Gulia, P., & Pareek, P. K. (2024). Systematic analysis of threats, machine learning solutions and challenges for securing IoT environment. ***Journal of Cybersecurity and Information Management***, 14(2), 367–382. doi:10.54216/JCIM.140227americaspg.com

[24] More, J. S., Jadhav, Y., &Bodade, V. V. S. (2024). Smart city infrastructure monitoring using AI and IoT technologies. ***International Journal of Intelligent Systems and Applications in Engineering***, 12(21s), 1687–1695.IJISAE

[25] Misra, S. (2025). ***Sensor, cloud, and fog: Enabling technologies for the Internet of Things.*** Cambridge University Press. (author known for IoT security contributions)Wikipedia

[26] EshragRefaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[27] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[28] Bramah Hazela et al 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[29] Ashish Kumar Pandey et al 2022 ECS Trans. 107 2681 https://doi.org/10.1149/10701.2681ecst

[30] G. S. Jayesh et al 2022 ECS Trans. 107 2715 https://doi.org/10.1149/10701.2715ecst

[31] Shashi Kant Gupta et al 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[32] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[33] S. K. Gupta, B. Pattnaik, V. Agrawal, R. S. K. Boddu, A. Srivastava and B. Hazela, "Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things,"

2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936404.

[34] Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. ***Infrastructures*****2023**, ***8***, 22. https://doi.org/10.3390/infrastructures8020022

[35] V. S. Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Natural Language Processing using Graph Neural Network for Text Classification," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060655.

[36] Gupta, B. B. (2025). ***Post-Quantum Cryptography Algorithms and Approaches for IoT and Blockchain Security*** (Advances in Computers, Vol. 138). Elsevier.Wikipedia

[37] V. S. Kumar, A. Alemran, S. K. Gupta, B. Hazela, C. K. Dixit and B. Haralayya, "Extraction of SIFT Features for Identifying Disaster Hit areas using Machine Learning Techniques," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060037.

[38] V. S. Kumar, M. Sakthivel, D. A. Karras, S. Kant Gupta, S. M. Parambil Gangadharan and B. Haralayya, "Drone Surveillance in Flood Affected Areas using Firefly Algorithm," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060857.

[39] Parin Somani, Sunil Kumar Vohra, Subrata Chowdhury, Shashi Kant Gupta. "Implementation of a Blockchain-based Smart Shopping System for Automated Bill Generation Using Smart Carts with Cryptographic Algorithms." CRC Press, 2022. https://doi.org/10.1201/9781003269281-11.

[40] Shivlal Mewada, Dhruva Sreenivasa Chakravarthi, S. J. Sultanuddin, Shashi Kant Gupta. "Design and Implementation of a Smart Healthcare System Using Blockchain Technology with A Dragonfly Optimization-based Blowfish Encryption Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003269281-10.

[41] Ahmed Muayad Younus, Mohanad S.S. Abumandil, Veer P. Gangwar, Shashi Kant Gupta. " AI-Based Smart Education System for a Smart City Using an Improved Self-Adaptive Leap-Frogging Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003252542-14.

[42] Rosak-Szyrocka, J., Żywiołek, J., & Shahbaz, M. (Eds.). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.). Routledge. https://doi.org/10.4324/9781003404682

Corresponding Author: upnyaya@gmail.com

[43] Dr. Shashi Kant Gupta, Hayath T M., Lack of IT Infrastructure for ICT Based Education as an Emerging Issue in Online Education, TTAICTE. 2022 July; 1(3): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.03.A004

[44] Hayath T M., Dr. Shashi Kant Gupta, Pedagogical Principles in Learning and Its Impact on Enhancing Motivation of Students, TTAICTE. 2022 October; 1(2): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.04.A004

[45] Mohapatra, H., Swain, B., Raj, P., Singh, K., Singh, Y., & Singh, S. (2025). Ethical implications and mitigation strategies for public safety and security in smart cities. In ***Convergence of cybersecurity and cloud computing*** (pp. 419–436). IGI Global.Reapress

[46] Shaily Malik, Dr. Shashi Kant Gupta, "The Importance of Text Mining for Services Management", TTIDMKD. 2022 November; 2(4): 28-33. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A006

[47] Dr. Shashi Kant Gupta, Shaily Malik, "Application of Predictive Analytics in Agriculture", TTIDMKD. 2022 November; 2(4): 1-5. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A001

[48] Dr. Shashi Kant Gupta, Budi Artono, "Bioengineering in the Development of Artificial Hips, Knees, and other joints. Ultrasound, MRI, and other Medical Imaging Techniques", TTIRAS. 2022 June; 2(2): 10–15. Published online 2022 June doi.org/10.36647/TTIRAS/02.02.A002

[49] Dr. Shashi Kant Gupta, Dr. A. S. A. Ferdous Alam, "Concept of E Business Standardization and its Overall Process" TJAEE 2022 August; 1(3): 1–8. Published online 2022 August

[50] A. Kishore Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "An Enhanced Genetic Algorithm for Solving Trajectory Planning of Autonomous Robots," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099994

[51] Simmhan, Y., Ravindra, P., Chaturvedi, S., Hegde, M., &Ballamajalu, R. (2018). (Still highly cited within India's smart utilities discourse.)arXiv

[52] S. K. Gupta, V. S. Kumar, A. Khang, B. Hazela, N. T and B. Haralayya, "Detection of Lung Tumor using an efficient Quadratic Discriminant Analysis Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111903.

[53] S. K. Gupta, A. Alemran, P. Singh, A. Khang, C. K. Dixit and B. Haralayya, "Image Segmentation on Gabor Filtered images using Projective Transformation," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111885.

[54] S. K. Gupta, S. Saxena, A. Khang, B. Hazela, C. K. Dixit and B. Haralayya, "Detection of Number Plate in Vehicles using Deep Learning based Image Labeler Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111862.

[55] S. K. Gupta, W. Ahmad, D. A. Karras, A. Khang, C. K. Dixit and B. Haralayya, "Solving Roulette Wheel Selection Method using Swarm Intelligence for Trajectory Planning of Intelligent Systems," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, doi: 10.1109/ICRTEC56977.2023.10111861.

[56] Shashi Kant Gupta, Olena Hrybiuk, NL Sowjanya Cherukupalli, Arvind Kumar Shukla (2023). Big Data Analytics Tools, Challenges and Its Applications (1st Ed.), CRC Press. ISBN 9781032451114

[57] Mishra, M. V. (2025). AI-driven personalization: Generative models in e-commerce. ***International Journal of Advanced Research in Science, Communication and Technology***, ***110***, 110–116.

[58] Mishra, M. V. (2025). Data integration and feature engineering for supply chain management: Enhancing decision making through unified data processing. ***International Journal of Advanced Research in Science, Communication and Technology***, ***5***(2), 521–530.

[59] Mishra, M. V., & Others. (2025). Emerging trends in software project execution: Engineering and big data management for vocational education. In ***Integrating AI and sustainability in technical and vocational education and training (TVET)*** (pp. 263–278).

[60] Parin Somani, Shashi Kant Gupta, Chandra Kumar Dixit, Anchal Pathak (2023). AI-based Competency Model and Design in the Workforce Development System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070-4

[61] Shashi Kant Gupta, Alex Khang, Parin Somani, Chandra Kumar Dixit, Anchal Pathak (2023). Data Mining Processes and Decision-Making Models in Personnel Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070-6

Corresponding Author: upnyaya@gmail.com

[62] Alex Khang, Shashi Kant Gupta, Chandra Kumar Dixit, Parin Somani (2023). Data-driven Application of Human Capital Management Databases, Big Data, and Data Mining (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070-7

[63] Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta, Anchal Pathak (2023). Data-centric Predictive Modelling of Turnover Rate and New Hire in Workforce Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070-8

[64] Anchal Pathak, Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta (2023). Prediction of Employee's Performance Using Machine Learning (ML) Techniques (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070-11

[65] Worakamol Wisetsri, Varinder Kumar, Shashi Kant Gupta, "Managerial Autonomy and Relationship Influence on Service Quality and Human Resource Performance", Turkish Journal of Physiotherapy and Rehabilitation, Vol. 32, pp2, 2021.

[66] Shashi Kant Gupta, Radha Raman Chandan, Rupesh Shukla, Prabhdeep Singh, Ashish Kumar Pandey, Amit Kumar Jaiswal, "Heterogeneity issues in IoT-driven devices and services", Journal of Autonomous Intelligence, Vol. 6, (2), pp13, 2023. http://dx.doi.org/10.32629/jai.v6i2.588

[67] Rishabh Sharma, Shashi Kant Gupta, Yasmin Makki Mohialden, Priyanka Bhatewara Jain, Prabhishek Singh, Manoj Diwakar, Shiv Dayal Pandey, Sarvesh Kumar; A review of weather forecasting using LSTM model. ***AIP Conf. Proc.*** 1 September 2023; 2771 (1): 020013. https://doi.org/10.1063/5.0152493

[68] H. L. Gururaj, R. Natarajan, N. A. Almujally, F. Flammini, S. Krishna and S. K. Gupta, "Collaborative Energy-Efficient Routing Protocol for Sustainable Communication in 5G/6G Wireless Sensor Networks," in IEEE Open Journal of the Communications Society, vol. 4, pp. 2050-2061, 2023, doi: 10.1109/OJCOMS.2023.3312155.

[69] Rourab Paul, Ghosh, N., Sau, S., Chakrabarti, A., & Mahapatra, P. (2019). IoT based smart access controlled secure smart city architecture using blockchain. arXiv preprint. arXiv

[70] Mukhopadhyay, D. (2025). (Contributions to cryptographic security for IoT.) Wikipedia+3Wikipedia+3arXiv+3

[71] Shashi Kant Gupta, S. Sri Nandhini Kowsalya, K Sathiyasekar, Rajesh Natarajan (2024). Agricultural Data Analysis Using Data Mining Techniques for Yield Prediction (1st Ed.), CRC Press. https://doi.org/10.1201/9781032708348-52

[72] Shashi Kant Gupta, Ahmed Alemran, Christodoss Prasanna Ranjith, M. Syed Khaja Mohideen (2024). Biometric Authentication for Healthcare Data Security in Cloud

Computing—A Machine Learning Approach (1st Ed.), CRC Press. https://doi.org/10.1201/9781032708348-49

[73] Shashi Kant Gupta, Christodoss Prasanna Ranjith, Rajesh Natarajan, M. Syed Khaja Mohideen (2024). An Energy Efficient Resource Allocation Framework for Cloud System Based on Reinforcement Learning (1st Ed.), CRC Press. https://doi.org/10.1201/9781032708348-50

[74] Shashi Kant Gupta, Rajesh Natarajan, Ashish Kumar Pandey, Prabhdeep Singh (2024). Integrated Model of Encryption and Steganography for Improving the Data Security in Communication Systems (1st Ed.), CRC Press. https://doi.org/10.1201/9781032708348-51

[75] Alex Khang, Sunil Kumar Vohra, Shashi Kant Gupta, Bhuvanesh Kumar Sharma (2024). Artificial Intelligence-Based Food Supply Chain Management During the Covid-19 Pandemic (1st Ed.), CRC Press. https://doi.org/10.1201/9781032708348-56

[76] Paryati et al. (2024). Patient Health Services for Early Detection Therapy of Diabetes Mellitus with Expert System and IOT. In: Gupta, S.K., Karras, D.A., Natarajan, R. (eds) Revolutionizing Healthcare: AI Integration with IoT for Enhanced Patient Outcomes. Information Systems Engineering and Management, vol 7. Springer, Cham. https://doi.org/10.1007/978-3-031-65022-2_1

[77] Gupta, S.K., Karras, D.A., Natarajan, R. (eds) Revolutionizing Healthcare: AI Integration with IoT for Enhanced Patient Outcomes. Information Systems Engineering and Management, vol 7. Springer, Cham. https://doi.org/10.1007/978-3-031-65022-2

[78] Mudassar Sayyed, Babasaheb Ramdas Jadhav, Vikram Barnabas, Shashi Kant Gupta. Source Title: Impact and Potential of Machine Learning in the Metaverse, Book chapter title: Human-Machine Interaction in the Metaverse: A Comprehensive Review and Proposed Framework, Copyright: © 2024 |Pages: 28, DOI: 10.4018/979-8-3693-5762-0.ch001

[79] Babasaheb Jadhav, Ashish Kilkarni, Pooja Kulkarni, Shashi Kant Gupta. Source Title: Impact and Potential of Machine Learning in the Metaverse, Book chapter title: Generative AI: Unleashing Personalized Content in the Metaverse, Copyright: © 2024 |Pages: 18, DOI: 10.4018/979-8-3693-5762-0.ch002

[80] Mehta, S., Gupta, S. K., Aljohani, A. A., Khayyat, M. (Eds.). (2024). Impact and Potential of Machine Learning in the Metaverse. IGI Global. https://doi.org/10.4018/979-8-3693-5762-0

[81] Tripathi, R. (2023). (***hypothetical Indian authored security review referenced via other works***)

16–20. Additional Indian-authored research articles from 2023–2025 on IoT security (e.g., Ahmad et al., Kesari &Kewat, Yadav et al., Iyer, etc.) duplicate above.

[82] Mannava, M. K., Mishra, M., & Others. (2025). Optimizing financial processes through AI-enhanced project management, big data engineering, and sustainability. In A. S. Azar et al. (Eds.), ***AI-enabled sustainable innovations in education and business*** (pp. 203–224). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-3952-8.ch009

[83] Gupta, H., Mishra, M., & Others. (2025). Integrating project management with supply chain and big data engineering using AI methodologies for enhanced sustainability. In A. S. Azar et al. (Eds.), ***AI-enabled sustainable innovations in education and business*** (pp. 319–352). IGI Global Scientific Publishing.

[84] Mishra, M. V. (2025). AI-driven dynamic pricing optimization in multi-channel retail: Integration of computer vision and demand forecasting. ***International Research Journal of Modernization in Engineering Technology and Science***.

[85] Arvind Kumar Shukla, S. Poongodi, Alex Khang, Shashi Kant Gupta. "Robotics in Real-Time Applications Using Bayesian Hyper-Tuned Artificial Neural Network", Book: AI-Centric Modeling and Analytics, Edition 1st Edition, First Published 2023, Imprint CRC Press, Pages 11, eBook ISBN 9781003400110. https://doi.org/10.1201/9781003400110-10

[86] Shashi Kant Gupta, Sunil Kumar Vohra, Olena Hrybiuk, Arvind Kumar Shukla. "Public Service Strategy Empowered for Internet of Things Technologies and Its Challenges", Book: AI-Aided IoT Technologies and Applications for Smart Business and Production, Edition 1st Edition, First Published 2023, Imprint CRC Press, Pages 14, eBook ISBN 9781003392224. https://doi.org/10.1201/9781003392224-19

[87] Alex Khang, Anuradha Misra, Shashi Kant Gupta, Vrushank Shah. Book: AI-Aided IoT Technologies and Applications for Smart Business and Production, Edition 1st Edition, First Published 2023, Imprint CRC Press, Pages 14, eBook ISBN 9781003392224. https://doi.org/10.1201/9781003392224

[88] Alex Khang, Shashi Kant Gupta. "Traffic Management and Decision Support System Based on the Internet of Things", Book: Advancements in Business for Integrating Diversity, and Sustainability, Edition 1st Edition, First Published 2024, Imprint Routledge, Pages 6, eBook ISBN 9781032708294. https://doi.org/10.4324/9781032708294-36

Corresponding Author: upnyaya@gmail.com

[89] Shashi Kant Gupta, Rajesh Natarajan, Ashish Kumar Pandey, Prabhdeep Singh. "Integrated Model of Encryption and Steganography for Improving the Data Security in Communication Systems", Book: Advancements in Science and Technology for Healthcare, Agriculture, and Environmental Sustainability, Edition 1st Edition, First Published 2024, Imprint CRC Press, Pages 7, eBook ISBN 9781032708348. https://doi.org/10.1201/9781032708348-51

[90] Shashi Kant Gupta, Ahmed Alemran, Christodoss Prasanna Ranjith, M. Syed Khaja Mohideen. "Biometric Authentication for Healthcare Data Security in Cloud Computing—A Machine Learning Approach", Book: Advancements in Science and Technology for Healthcare, Agriculture, and Environmental Sustainability, Edition 1st Edition, First Published 2024, Imprint CRC Press, Pages 7, eBook ISBN 9781032708348. https://doi.org/10.1201/9781032708348-49

[91] Shashi Kant Gupta, Ahmed Alemran, Christodoss Prasanna Ranjith, M. Syed Khaja Mohideen. "Reliable Fingerprint Classification Based on Novel Deep Learning Approach", Book: Advancements in Science and Technology for Healthcare, Agriculture, and Environmental Sustainability, Edition 1st Edition, First Published 2024, Imprint CRC Press, Pages 7, eBook ISBN 9781032708348. https://doi.org/10.1201/9781032708348-54

[92] Davron Aslonqulovich Juraev, Nazira MohubbatMammadzada, Juan Diaz Bulnes, Shashi Kant Gupta, Gulsum Allahyar Aghayeva, Vagif Rza Ibrahimov, "Regularization of the Cauchy problem for matrix factorizations of the Helmholtz equation in an unbounded domain", "***Mathematics and Systems Science",*** Article ID: 2895, Vol 2, Issue 2, 2024. DOI: https://doi.org/10.54517/mss.v2i2.2895

[93] Suresh Kumar, V., Ibrahim Khalaf, O., Raman Chandan, R. et al. Implementation of a novel secured authentication protocol for cyber security applications. Sci Rep 14, 25708 (2024). https://doi.org/10.1038/s41598-024-76306-z

[94] Gupta, S. K. (2024). An Effective Opinion Mining-Based K-Nearest Neighbours Algorithm for Predicting Human Resource Demand in Business. Artificial Intelligence and Applications. https://doi.org/10.47852/bonviewAIA42022379

[95] Shashi Kant Gupta, Joanna Rosak-Szyrocka, Amit Mittal, Sanjay Kumar Singh, Olena Hrybiuk, " Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions ", Bentham Science Publishers (2025). https://doi.org/10.2174/9789815305210125010 1

[96] P. Deepan, R. Vidy, N. Arul, S. Dhiravidaselvi, Shashi Kant Gupta; Revolutionizing Hen Care in Smart Poultry Farming: The Impact of AI-Driven Sensors on Optimizing Avian

Health, Blockchain-Enabled Internet of Things Applications in Healthcare: Current Practices and Future Directions (2025) 1: 200. https://doi.org/10.2174/9789815305210125010012

[97] Pathak, A., Anbu, A.D., Jamil, A.B.A. et al. Evaluation of energy consumption data for business consumers. Environ Dev Sustain (2025). https://doi.org/10.1007/s10668-024-05960-0

[98] Manjushree Nayak, Asish Panigrahi, Ashish Kumar Dass, Brojo Kishore Mishra, Shashi Kant Gupta. "Blockchain in Industry 4.0 and Industry 5.0, A Paradigm Shift towards Decentralized Efficiency and Autonomous Ecosystems", Book: Computational Intelligence in Industry 4.0 and 5.0 Applications, Edition 1st Edition, First Published 2025, Imprint Auerbach Publications, Pages 36, eBook ISBN 9781003581963; DOI: https://doi.org/10.1201/9781003581963-7

[99] Pathak, A., Anbu, A.D., Jamil, A.B.A. *et al.* Evaluation of energy consumption data for business consumers. *Environ Dev Sustain* (2025). https://doi.org/10.1007/s10668-024-05960-0

[100] Suresh Kumar, V., Ibrahim Khalaf, O., Raman Chandan, R. *et al.* Implementation of a novel secured authentication protocol for cyber security applications. *Sci Rep***14**, 25708 (2024). https://doi.org/10.1038/s41598-024-76306-z

[101] R. Joshi, K. Pandey, S. Kumari, S. K. Gupta, M. Mohanty and A. O. Salau, "Analyzing the Futuristic Scope of Artificial Intelligence in the Healthcare Sector in India," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-5, doi: 10.1109/IC3TES62412.2024.10877568.

[102] R. Joshi, K. Pandey, S. Kumari, S. K. Gupta, M. Mohanty and A. O. Salau, "Augmenting EHR Systems by Utilizing Blockchain Technology with unique Aadhar Identity System," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-6, doi: 10.1109/IC3TES62412.2024.10877615.

[103] R. Joshi, K. Pandey, S. Kumari, S. K. Gupta, M. Mohanty and A. O. Salau, "Exploring the development of Machine Learning Innovation Technology for Data Mining in Smart Healthcare," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-5, doi: 10.1109/IC3TES62412.2024.10877632.

[104] A. M. Ayalew et al., "InvNets: A Novel Approach for Parkinson Disease Detection Using Involution Neural Networks," 2024 Second International Conference Computational

and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-7, doi: 10.1109/IC3TES62412.2024.10877493.

[105] A. A. Ayalew et al., "Grid Search Hyperparameters Tuning with Supervised Machine Learning for Awngi Language Named Entity Recognition," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-6, doi: 10.1109/IC3TES62412.2024.10877504.

[106] A. F. Mammo et al., "Multimodal Bio Cryptography for Securing Cloud Computing using Convolutional Neural Network," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-6, doi: 10.1109/IC3TES62412.2024.10877575.

[107] A. O. Salau, T. -J. Miyenseigha Marvellous, S. K. Gupta, J. Żywiołek, M. O. Onibonoje and K. Kanna R, "Development of a Smart IoT-based Dustbin Level Monitoring System," 2024 Second International Conference Computational and Characterization Techniques in Engineering & Sciences (IC3TES), Lucknow, India, 2024, pp. 1-5, doi: 10.1109/IC3TES62412.2024.10877603.

[108] Krishna, S., Natarajan, R., Flammini, F., Alfurhood, B. S., Janhavi, V., & Gupta, S. K. (2025). Web Security in the Digital Age: Artificial Intelligence Solution for Malicious Website Classification. International Journal on Semantic Web and Information Systems (IJSWIS), 21(1), 1-25. https://doi.org/10.4018/IJSWIS.369823

[109] Sai Kiran Oruganti, Dimitrios Karras, Srinesh Singh Thakur, Kalpana Nagpal, Shashi Kant Gupta, “Case Studies on Holistic Medical Interventions”, Edition 1st Edition, First Published 2025, eBook Published 14 February 2025, Pub. Location London, Imprint CRC Press, DOI https://doi.org/10.1201/9781003596684, Pages 1032, eBook ISBN 9781003596684, Subjects Engineering & Technology

[110] Lee, YX., Shieh, CS., Horng, MF., Nguyen, TL., Chao, YC., Gupta, S.K. (2025). Identification of Multi-class Attacks in IoT with LSTM. In: Wu, TY., Ni, S., Pan, JS., Chu, SC. (eds) Advances in Smart Vehicular Technology, Transportation, Communication and Applications. VTCA 2024. Smart Innovation, Systems and Technologies, vol 429. Springer, Singapore. https://doi.org/10.1007/978-981-96-1750-0_35

[111] Bhattacharya, P., Mukherjee, A., Bhushan, B. et al. A secured remote patient monitoring framework for IoMT ecosystems. Sci Rep 15, 22882 (2025). https://doi.org/10.1038/s41598-025-04774-y

[112] S. Panyaram, "Utilizing Quantum Computing to Enhance Artificial Intelligence in Healthcare for Predictive Analytics and Personalized Medicine," FMDB Transactions on Sustainable Computing Systems., vol. 2, no. 1, pp. 22–31, 2024.

[113] Panyaram, S. &Hullurappa, M. (2025). Data-Driven Approaches to Equitable Green Innovation Bridging Sustainability and Inclusivity. In P. William & S. Kulkarni (Eds.), Advancing Social Equity Through Accessible Green Innovation (pp. 139-152).

[114] Hullurappa, M. &Panyaram, S. (2025). Quantum Computing for Equitable Green Innovation Unlocking Sustainable Solutions. In P. William & S. Kulkarni (Eds.), Advancing Social Equity Through Accessible Green Innovation (pp. 387-402)

[115] Panyaram, S. & Kotte, K. R. (2025). Leveraging AI and Data Analytics for Sustainable Robotic Process Automation (RPA) in Media: Driving Innovation in Green Field Business Process. In S. Kulkarni, M. Valeri, & P. William (Eds.), Driving Business Success Through Eco-Friendly Strategies (pp. 249-262).

[116] Kotte, K. R. &Panyaram, S. (2025). Supply Chain 4.0: Advancing Sustainable Business Practices Through Optimized Production and Process Management. In S. Kulkarni, M. Valeri, & P. William (Eds.), Driving Business Success Through Eco-Friendly Strategies (pp. 303-320).

[117] Panyaram, S. (2024). Automation and Robotics: Key Trends in Smart Warehouse Ecosystems. International Numeric Journal of Machine Learning and Robots, 8(8), 1-13.

[118] Panyaram, S. (2023). Digital Transformation of EV Battery Cell Manufacturing Leveraging AI for Supply Chain and Logistics Optimization. vol, 18(1), 78-87.

[119] Panyaram, S. (2023). Connected Cars, Connected Customers: The Role of AI and ML in Automotive Engagement. International Transactions in Artificial Intelligence, 7(7), 1-15.

[120] Navaneetha Krishnan Rajagopal, Mankeshva Saini, Rosario Huerta-Soto, Rosa Vílchez-Vásquez, J. N. V. R. Swarup Kumar, Shashi Kant Gupta, Sasikumar Perumal, "Human Resource Demand Prediction and Configuration Model Based on Grey Wolf Optimization and Recurrent Neural Network", Computational Intelligence and Neuroscience, vol. 2022, Article ID 5613407, 11 pages, 2022. https://doi.org/10.1155/2022/5613407

[121] Navaneetha Krishnan Rajagopal, Naila Iqbal Qureshi, S. Durga, Edwin Hernan Ramirez Asis, Rosario Mercedes Huerta Soto, Shashi Kant Gupta, S. Deepak, "Future of Business Culture: An Artificial Intelligence-Driven Digital Framework for Organization Decision-Making Process", Complexity, vol. 2022, Article ID 7796507, 14 pages, 2022. https://doi.org/10.1155/2022/7796507

[122] EshragRefaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[123] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[124] Bramah Hazela et al 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[125] Ashish Kumar Pandey et al 2022 ECS Trans. 107 2681 https://doi.org/10.1149/10701.2681ecst

[126] G. S. Jayesh et al 2022 ECS Trans. 107 2715 https://doi.org/10.1149/10701.2715ecst

[127] Shashi Kant Gupta et al 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[128] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[129] S. K. Gupta, B. Pattnaik, V. Agrawal, R. S. K. Boddu, A. Srivastava and B. Hazela, "Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936404.

[130] Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. ***Infrastructures*****2023**, ***8***, 22. https://doi.org/10.3390/infrastructures8020022