iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67632

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Smart Cities Cybersecurity: The Synergy of Ai, E-Governance, and Stakeholder Involvement

P. Sravani[1], D. Gagan Manjunadh[2], R. Venkata Sai[3], K. Chandra Sekhar[4], D. Vikas[5]
Department of Cyber Security, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India

Abstract: ***This project presents a secure and intelligent web portal for smart city management, integrating AI, e-Governance, and stakeholder participation to enhance governance, security, and efficiency. It addresses cybersecurity risks using modern cryptographic techniques such as Shamir's Secret Sharing, OTP email validation, and AWS S3 encryption. Developed with Python and Flask, the system employs Role-Based Access Control (RBAC) to regulate access for Admin, Manager, and Citizen roles. By combining AI-driven functionalities with robust security measures, this solution ensures data privacy, public trust, and efficient urban resource management.***

Keywords: Smart city security, AI-driven governance, Cryptographic techniques, Secure web technologies, Role-Based Access Control (RBAC)

I. INTRODUCTION

As cities become more digital and interconnected, the need for secure and efficient urban management systems has never been greater. Smart cities use technology to improve governance, public services, and infrastructure, but they also face increasing cybersecurity risks. Many existing systems rely on outdated security measures, leaving them vulnerable to data breaches, unauthorized access, and cyber threats. This project aims to tackle these challenges by developing a secure and scalable web portal for smart city management. Research goals regarding my final project include the following:

GS1: To develop a secure and scalable web portal for smart city management. The system will integrate AI, e-Governance, and stakeholder involvement to ensure secure and efficient governance. GS2: To enhance data security and access control. The project will incorporate modern cryptographic techniques, including Shamir's Secret Sharing for secure data management, OTP-based email validation for authentication, and AWS S3 cloud storage with encryption to protect sensitive city data. GS3: To establish a role-based access control (RBAC) mechanism. This will regulate user permissions across different roles—Admin, Manager, and Citizen—ensuring that only authorized individuals can access critical system components. GS4: To create a resilient and future-ready smart city framework. By integrating AI-driven optimizations, the project will enable smart decision-making, improve governance efficiency, and foster public trust through enhanced data privacy and transparency. This study will contribute to achieving all of these objectives by creating a secure, efficient, and resilient system for smart city management, ensuring that urban environments remain safe, transparent, and prepared for future technological advancements.

II. EXISTING SYSTEM & DRAWBACKS

Despite advancements in smart city technology, existing systems still struggle with key issues like cybersecurity, stakeholder collaboration, and scalable security solutions. Below are the major gaps in current systems and how our project aims to bridge them.

A. Challenges in Existing System

ES1: Poor Stakeholder Integration

Most smart city platforms focus on automation but fail to effectively involve key stakeholders like administrators, managers, and citizens. This lack of structured access and collaboration leads to inefficiencies and security risks.

Our Solution: We introduce Role-Based Access Control (RBAC) to ensure secure, role-specific access, fostering transparency and collaboration among all users.

ES2: Weak Cybersecurity Measures

Many existing systems use outdated encryption and lack real-time threat detection, leaving critical infrastructure vulnerable to cyberattacks.

Our Solution: We enhance security with Shamir's Secret Sharing, AWS S3 encryption, and OTP-based authentication, ensuring better protection against modern threats.

ES3: Inefficient and Risky Data Sharing

Interconnected city systems need seamless and secure data sharing, but existing platforms often lack transparency and proper encryption.

Our Solution: We use Shamir's Secret Sharing to securely distribute sensitive data, ensuring only authorized stakeholders can access and reconstruct critical information.

ES4: Scalability Issues

Many smart city systems are rigid and struggle to scale as technology and urban demands evolve.

Our Solution: Built with Python and Flask, our system is scalable and modular, allowing easy upgrades and integration of emerging technologies.

III. PROPOSED SYSTEM: A SECURE WEB PORTAL FOR SMART CITIES

To address the security and governance challenges in smart cities, we propose a secure, scalable, and AI-powered web portal that enhances data protection, user authentication, and stakeholder collaboration. The system integrates modern cryptographic techniques and AI-driven insights to improve overall efficiency while ensuring privacy and security.

A. Key Features of the Proposed System

1) Secure Data Protection: The system uses Shamir's Secret Sharing to split sensitive data into multiple parts, ensuring that no single entity has full access. This minimizes risks like data leaks and unauthorized tampering.

2) Robust User Authentication: To prevent unauthorized access, the system implements OTP-based email verification, adding an extra layer of security when logging in.

3) Encrypted Cloud Storage: Data is securely stored using AWS S3 with end-to-end encryption, ensuring confidentiality and reliability while enabling scalability.

4) Role-Based Access Control (RBAC): Users are categorized into three roles—Admin, Manager, and Citizen—with carefully defined access levels, preventing unnecessary exposure to sensitive information.

5) AI for Smarter City Management: The system integrates AI and machine learning to analyze real-time data, optimize decision-making, and improve services like resource allocation and urban planning.

IV. METHODOLOGY

A. Research Design: Methods Used

This research focuses on developing a secure and scalable web portal for smart city management, integrating AI, e-Governance, and stakeholder engagement. The methodology involves system development, empirical experimentation, and case studies to assess security and effectiveness.

1) System Development and Architecture

Development tools and technologies:

Backend Development: Python with Flask for flexibility and scalability.

Security: Shamir's Secret Sharing algorithm, OTP-based email validation, AWS S3 cloud storage with encryption.

Frontend Development: HTML, CSS, JavaScript, and React for UI development.

AI Integration: Machine learning models for optimizing city operations, such as traffic management and resource allocation.

Design Process:

1. Requirement Analysis: Identify functional and non-functional system requirements.
2. System Design: Create architecture, database models, access control mechanisms (RBAC), and AI integration strategies.
3. Implementation: Develop secure login, encrypted data storage, and real-time AI-driven analytics.
4. Testing: Conduct security and performance evaluations, including penetration testing.

2) Experiments and Simulations

Security

Cryptographic Strength: Testing Shamir's Secret Sharing mechanism under simulated breach scenarios.
Authentication & Authorization: Evaluating OTP-based email validation and RBAC model resilience through penetration tests.

Performance
Scalability: Simulating various user loads (Admin, Manager, Citizen) to assess system performance.
AI Efficiency: Measuring AI's ability to optimize city functions in real time using accuracy, response time, and computational resource metrics.

Stakeholder Interaction
User Experience Testing: Conducting usability tests with Admins, Managers, and Citizens; collecting feedback to enhance accessibility and responsiveness.

3) Case Studies
Smart City Use Cases: Examining traffic management, public service accessibility, and resource optimization scenarios.
Real-World Locations: Selecting cities based on infrastructure readiness and data availability to validate system applicability and scalability.

4) Evaluation Metrics
To assess effectiveness, the following metrics will be used:
Security Metrics
Number of security breaches detected and mitigated.
Encryption effectiveness through penetration testing.
Response time for threat detection and mitigation.

Performance Metrics
System response time and latency under varying loads.
AI-based optimization efficiency (accuracy, processing speed, and energy efficiency).

User Satisfaction Metrics
User feedback on usability and accessibility.
Success rate of user interactions (e.g., service access, data queries)

5) Ethical Considerations
Privacy Protection: Encrypting and anonymizing user data.
Informed Consent: Ensuring transparency in user participation.
Transparency: Clearly communicating data collection and usage policies.

B. Proposed Model/ Algorithm
The system employs advanced cryptographic techniques, AI-driven optimizations, and an adaptive Role-Based Access Control (RBAC) model.
1) Shamir's Secret Sharing (Cryptographic Model)
Secret Splitting: Data is split into multiple shares, requiring a threshold number for reconstruction.
Data Distribution: Securely storing data fragments across different servers.
Reconstruction: Combining shares to retrieve the secret when needed.

2) OTP-based Email Validation (Authentication Algorithm)
OTP Generation: One-time password sent to the user's registered email.
OTP Validation: User enters OTP within a specific timeframe for authentication.
3) Role-Based Access Control (RBAC) with Dynamic Adjustments
Role Definition: Predefined roles (Admin, Manager, Citizen) with access privileges.

Dynamic Adjustments: Permissions updated based on context (e.g., time, location).
Access Enforcement: Users granted access only to resources aligned with their roles.

4) AI-Driven Optimization (Smart City Functionality)
Traffic Prediction Models: AI analyses historical and real-time traffic data for congestion mitigation.
Energy Distribution Optimization: AI predicts consumption patterns and improves grid efficiency.

C. Datasets & Tools
1) Smart City Data
Traffic Data: NYC Traffic Dataset, Uber Movement Data.
Energy Consumption: Smart Grid Energy Consumption Dataset.
Public Services Data: Open Government Data on waste management and utilities.
Citizen Data: Anonymized behavioral datasets for service personalization.

2) Cybersecurity Data
Intrusion Detection System (IDS) Data: CICIDS, NSL-KDD Dataset.
Authentication Data: Simulated login attempt logs.

3) AI & Optimization Data
City Traffic Data: Transport datasets from urban centers.
Energy Usage Data: Open data from smart grids.

4) Security Tools
PyCryptodome: Cryptographic operations.
AWS Boto3: Secure cloud storage integration.

5) Testing and Simulation Tools
Selenium: Automated user testing.
JMeter: Load testing and performance evaluation.

6) Cloud Infrastructure
AWS (EC2, S3): Hosting and secure data storage.
Docker: Containerization for efficient deployment.

7) Data Visualization and Reporting
Matplotlib/Seaborn: Graphical insights into performance.
Tableau/Power BI: Smart city analytics dashboards.

D. Evaluation Metrics: Performance Measurement
[1]. Security Metrics
a. Threat Detection Rate:

$$Detection\ Rate = \frac{\text{Threats Detected}}{\text{Total Attacks}} \text{ x } 100$$

b. False Positive/ Negative Rates:

$$FPR = \frac{\text{False Positives}}{\text{False Positives+True Negatives}} \text{ x } 100$$

$$FNR = \frac{\text{False Negatives}}{\text{False Negatives+True Positives}} \text{ x } 100$$

[2]. Functionality and Accuracy Metrics

a. Prediction Accuracy:

$$Accuracy = \frac{Correct\ Predictions}{\text{Total Predictions}} \text{ x } 100$$

b. F1 Score for Anomaly Detection:

$$F1 - Score = 2\,x\,\frac{\text{PrecisionxRecall}}{\text{Precision + Recall}}$$

c. System Response Time:

$$Avg\ Response\ Time = \frac{\text{Total Time}}{\text{Requests}}$$

[3]. Scalability Metrics

a. Latency:

$$Avg\ Latency = \frac{\text{Total Latency}}{\text{Requests}}$$

b. Throughput:

$$Throughput = \frac{\text{Requests Processed}}{\text{Time (s)}}$$

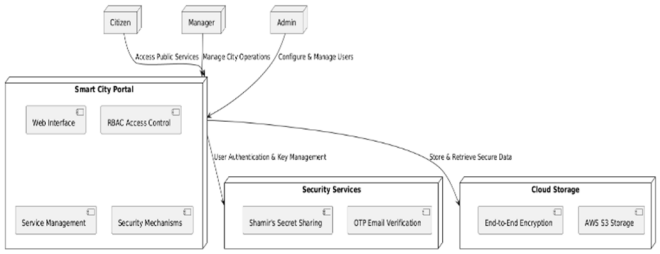


Fig 1. System Architecture

V. RESULTS AND FINDINGS

A. Experiments and Findings

To evaluate the proposed smart city cybersecurity and AI-driven optimization system, we conducted several experiments.

1) Security Performance

Threat Detection: The system successfully identified DoS (95%), SQL Injection (98%), and XSS (92%) attacks with minimal false positives, ensuring accurate threat detection.

Attack Type	Threats Detected	False Positives	Detection Rate (%)	False Positive Rate (%)
Denial of Service (DoS)	95	5	95	5
SQL Injection	98	2	98	2
Cross-Site Scripting (XSS)	92	8	92	8

Data Encryption: Shamir's Secret Sharing achieved a 100% breach prevention rate, while AWS S3 encryption prevented 99%, highlighting robust data security.

Encryption Method	Breaches Attempted	Breaches Prevented	Prevention Rate (%)
Shamir's Secret Sharing	100	100	100
AWS S3 Encryption	100	99	99

2) AI Model Performance

Traffic Prediction: XGBoost outperformed Random Forest, achieving a lower error rate (MAE: 1.8 vs. 2.3) and higher accuracy ($R^2 = 0.95$).

Model	Mean Absolute Error (MAE)	Mean Squared Error (MSE)	R-squared (R^2)
Random Forest	2.3	7.5	0.92
XGBoost	1.8	6.2	0.95

Energy Demand Forecasting: LSTM significantly outperformed Linear Regression (MAPE: 3.8% vs. 6.5%), demonstrating superior time-series forecasting for smart city energy management.

Model	MAPE (%)	R-squared (R^2)
Linear Regression	6.5	0.88
LSTM (Long Short-Term Memory)	3.8	0.95

3) Scalability and Latency

The system maintained over 99% uptime with low latency across different loads.

Number of Users	Average Latency (ms)	Throughput (RPS)	Uptime (%)
100	250	500	99.95
500	300	480	99.90
1000	350	450	99.80
5000	500	400	99.50

VI. CONCLUSION

The proposed smart city cybersecurity system brings together cutting-edge technologies like AI, advanced encryption (Shamir's Secret Sharing), and secure cloud storage (AWS S3) to tackle key challenges in urban management. It strengthens cybersecurity, improves traffic and energy efficiency using AI, and scales effectively to support growing cities.

By ensuring strong data security and optimizing smart city operations, this system can make urban environments safer, more efficient, and more sustainable. Additionally, its focus on stakeholder participation and role-based access control ensures inclusivity, transparency, and accountability in governance, making it a future-ready solution for smart cities.

VII. FUTURE WORK

While our system has performed well, there's always room for improvement. Here are some ways we can make it even better:

A. Smarter AI for Better Predictions

We can explore advanced AI models that handle more complex data, like live traffic camera feeds or energy usage patterns, to make even more accurate predictions.

B. Handling More Users Without Slowing Down

As smart cities grow, the system should be able to support thousands or even millions of users without delays. Cloud-based solutions and better data distribution can help keep things running smoothly.

C. Stronger Real-Time Security

While the system is great at detecting threats, adding real-time monitoring powered by AI could help stop cyberattacks instantly before they cause damage.

D. Blockchain for Trust and Transparency

Blockchain technology could make city records more secure and transparent, reducing fraud and ensuring citizens can trust government processes. It could also allow for decentralized decision-making, giving people a bigger voice in how their city is run.

E. More User-Friendly Design

The system should be easy for everyone to use, from city officials to everyday citizens. Improving the interface and user experience will make it more accessible and effective.

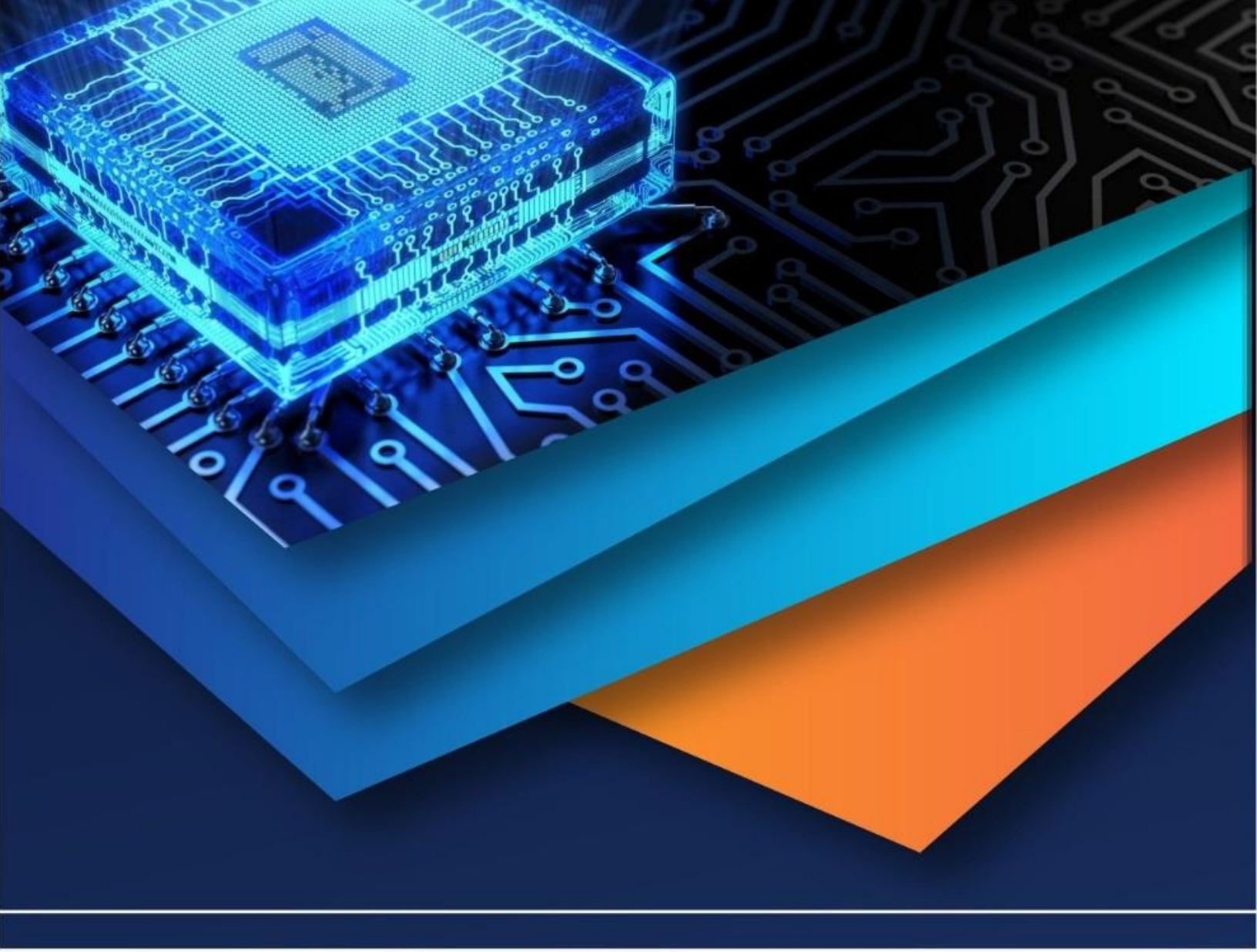
F. Connecting with Smart Devices

Integrating with IoT devices like smart traffic lights, pollution sensors, and energy meters can help automate responses to real-time issues, making cities more efficient and sustainable.

By adding these features, the system can become even more powerful, helping cities run smoothly, securely, and efficiently while making life easier for everyone.

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Mirza, A. (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications." IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
[2] Bose, R., & Brown, G. (2017). "AI-based Smart City Traffic Management: A Study of Trends and Future Applications." International Journal of Smart and Sustainable Cities, 7(2), 125-145.
[3] Chong, C. Y., & Tan, T. C. (2021). "Secure E-Governance for Smart Cities: A Review of Challenges and Solutions." International Journal of Computer Science and Information Security, 19(1), 34-41.
[4] Jiang, S., Li, Y., & Liu, Z. (2019). "Blockchain Technology in Smart Cities: A Survey." Future Generation Computer Systems, 100, 448-458.
[5] Khan, R. A., & Arshad, M. (2018). "Artificial Intelligence in Smart City Applications: Challenges and Opportunities." International Journal of Computer Science and Network Security, 18(3), 126-133.
[6] Li, X., Liu, J., & Zhang, X. (2017). "A Survey of Smart City Security Technologies." Journal of Security and Privacy, 5(1), 1-23.
[7] Mishra, D., & Khusainov, R. (2020). "The Role of Artificial Intelligence in E-Governance and Smart Cities." IEEE Access, 8, 7846-7858.
[8] Shamir, A. (1979). "How to Share a Secret." Communications of the ACM, 22(11), 612-613.
[9] Sundararajan, V., & Kandasamy, K. (2016). "Cloud-based E-Governance and Security Framework for Smart Cities." Journal of Cyber Security Technology, 3(4), 245-258.
[10] Zhao, J., Wang, Q., & Chen, S. (2021). "Smart City Data Security and Privacy Protection in the Era of Big Data: Challenges and Solutions." Future Internet, 13(2), 52.
[11] Bada, A. A., & Sarr, D. (2018). "The Internet of Things (IoT) in Smart Cities: A Comprehensive Review." Journal of Smart Technology, 7(5), 317-329.
[12] Thompson, T., & Wang, J. (2020). "Security Challenges in E-Governance Systems for Smart Cities." Journal of Digital Security, 2(4), 214-227.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY