Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybersecurity Approaches for Safeguarding Gis and Iot Systems in Smart Cities

Ahmed Anwer AL Jumili[1], Kifah Tout[2], Zaid F. Makki st[3]

[1] *Designation, Lebanese University doctoral school of science and technology, Beirut, Lebanon,*
[2] *Designation, Lebanese University doctoral school of science and technology, Beirut, Lebanon,*
[3] *Alshaab university, Iraq*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Introduction: With the increasing growth of smart cities and the use of Geographic Information System (GIS) and Internet of Thinks (IoT) to enhance urban services, there is an urgent need for cybersecurity. The interconnected nature of smart city systems has become vulnerable to cyber threats. To secure data, encryption has become an urgent need to secure data at various stages during transmission, at static, and during data processing.

Objectives: This study discusses data encryption and challenges using 2D vector distribution and encryption keys. Sensitive data coming from GIS systems and transmitted through IoT devices can be encrypted.

Methods: In the context of smart cities supported by IoT and GPS, it is essential to maintain data security and integrity of its transmission as well. The information transmitted through the smart city network is of various types, including spatial information, infrastructure locations, sensor readings, and real-time communications such as transportation and environmental monitoring. All data is gathered in one context, which is the digital character, and is transmitted from the source to one of the communication layers, which is the transport layer, and then it takes a preliminary processing path through protocols and is transmitted to the physical layer.

Results: The proposed method has proven its worth through good results in encryption evaluation criteria PSNR=86 dB, MSE=40, and Accuracy= 80%.

Conclusions: The study emphasized the importance of real-time encryption given the rapid increase in smart city data. The study provides a comprehensive overview of how encryption works as a flexible foundation for cybersecurity in smart cities that support GIS and IoT systems, and to ensure data security amidst the acceleration of technological development.

Keywords: *Smart city, Geographic Information System, Internet of Thinks, Cybersecurity, Encryption, Encryption key.*

INTRODUCTION

Cybersecurity challenges are multifaceted and often complex. GIS platforms are vulnerable to hacking through unauthorized access and data manipulation, reducing the accuracy and reliability of data that is the basis for city planning and disrupting effective emergency response. IoT security measures are often inadequate, facilitating network intrusions to transmit information. The consequences of cyber-attacks on such systems are disastrous and have serious consequences, including disruption of services, loss of public confidence and financial losses. Many of the basic solutions and supports provided by GIS and the Internet of Things to the smart city, and other services in this field are still widespread. It is expected that the information sources that rely on GIS and the Internet of Things and the number of devices will increase to nearly 40 billion by 2028 [1]. The use of the Internet of Things in modern cars has increased by 36% in the last two years, so the devices that operate with GIS and the Internet of Things are increasing and have the largest role in building smart cities. According to the World Economic Forum, the Internet of Things has contributed to achieving the 17 sustainable goals [2]. The superior ability to communicate and provide information via the Internet contributes to building smart cities, but cybersecurity threats are also increasing [3]. Among the attacks that may occur in smart cities are:

- Traffic light control: Attackers or unauthorized persons can cause traffic congestion and jams, and because wireless networks have been exploited and attacked. [4]
- Attacks against smart vehicles: These attacks cause misdirection of vehicles and wrong paths that cause collisions[5]
- Power grid collapse: Attacks can include power stations and cause catastrophic outages [6]
- Water sources: Attacks can include tampering with chemicals added to water and cause health problems [7]
- Surveillance cameras: Attacks can lead to spying on people and accessing personal data [8].

Smart cities have been the target of many security attacks in many countries around the world for several years. For example, in 2015, the city of Kiev (Ukraine) experienced a complete power outage due to a cyber attack, the electricity was cut off for an entire hour [9]. In 2019, the city of Baltimore (USA) was attacked by a ransomware program and demanded 13 Bitcoins for encrypted files [10]. Cyber attacks paralyze the joints of life and negatively affect people's lives. Also in 2024, there were cyber attacks of a different kind on the communications devices of the Lebanese Hezbollah. In some cases, people prefer not to use technology to avoid such attacks. A study by Letras [11] identified seven factors and their percentages related to citizens' interests in adopting smart cities and concerns, which are as follows: security and protection 45%, privacy of personal data 25%, transparency in services 8%, and finally other concerns 5%.

A. *GIS and IoT in Smart City*

Over the past years, GIS has evolved from a traditional science of managing geographic maps to a fast-paced technology that is a source of the most important information that has contributed to the sustainability of smart cities. The GPS system works to obtain data from various sectors and stores and analyzes it with the help of other technologies and applications to improve smart city data [12].

There are many elements that need to be achieved to create smart cities and an integrated approach must be taken to accommodate these elements, including green energy, smart construction, livable housing, sustainable transportation, water resources, risk reduction and more. One of the main elements that this study focused on is GIS, which is the largest source of information and is increasing dramatically, as in the examples of smart cities (Amsterdam and Dubai). Applications from giant companies (IBM, Google and Apple) such as software and maps have helped attract users to urban cities, as have smart sensors. Modern technology has helped the rapid development of smart cities, which has been the basis for attracting developers and hobbyists and absorbing their skills in the field of building smart cities [13].

The Internet of Things has revolutionized the history of smart cities through interconnected systems to enhance city management. In smart cities, the Internet of Things consists of a network of sensors, cameras, and smart meters that collect and process data in real time. As a result of the applications that accompany the Internet of Things, they work to improve traffic management, energy consumption, and environmental monitoring. Vehicular Ad-Hoc Network (VANET) systems have worked very successfully in smart cities by using GIS information, processing it, and distributing it across Internet of Things networks. In addition, the sensors deployed in smart cities work to monitor weather conditions and air quality, as well as monitoring noise levels and water conditions. Improving safety and monitoring crime are also things that the Internet of Things has excelled in in smart monitoring and rapid emergency response. Although its benefits are very great, its risks are very influential on people's lives, as any data breach has major consequences at the administrative and economic levels.

GIS is the most important source of information gathering and a hub for integrating data from all aspects, such as knowing the sources of problems, the context surrounding its possibilities, what solutions should be designed, and what scenarios can be followed in a dynamic environment. As in Figure 1, which represents geospatial knowledge and its development with the establishment of smart cities and their complexities.

Journal of Information Systems Engineering and Management
2025, 10(42s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

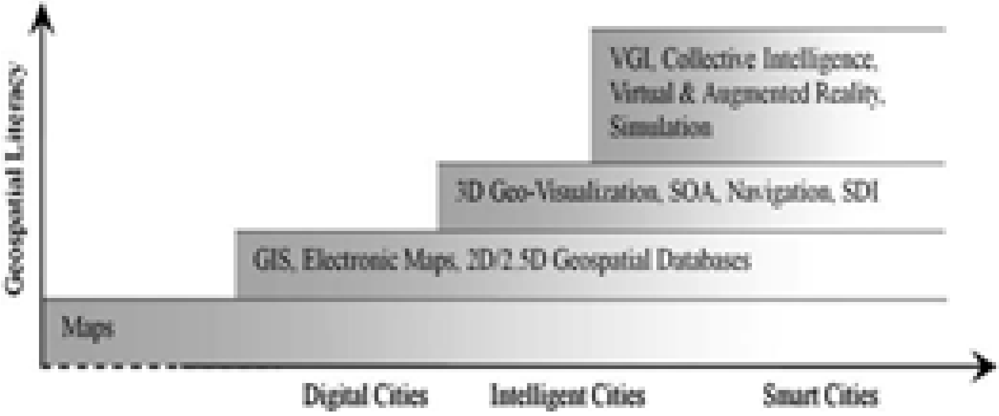

Geospatial Literacy
VGI, Collective Intelligence, Virtual & Augmented Reality, Simulation
3D Geo-Visualization, SOA, Navigation, SDI
GIS, Electronic Maps, 2D/2.5D Geospatial Databases
Maps
Digital Cities
Intelligent Cities
Smart Cities

Figure 1: GIS and related to smart city development [14]

GIS is a technology for data acquisition, analysis and geographic imaging. Through smart cities, these systems help improve the following applications:

- Urban planning, which contributes to the design of cities and lands through maps to develop planning and decision-making for housing
- Transportation and traffic management, which tracks the movement flow of transportation networks to predict appropriate routes and reduce traffic congestion.
- Environmental monitoring in terms of water and air, analysis of climate impacts on the urban environment and prediction of potential disasters.
- Rapid emergency responses to control waste and allocate population resources.

This requires a method that outperforms traditional methods in processing data in real time, and here the need arose to use artificial intelligence technologies and its applications such as machine learning to develop smart cities.

GPS and the Internet of Things are the backbone of smart cities, without which the basics of smart cities cannot be achieved. Through studies on smart cities and the broad landscape that describes these basics of cities, eight areas have been identified (Figure 2). These areas are often used to describe smart cities: governance, mobility and transportation, living and infrastructure, industry and production, economy, healthcare and environment. These classifications are considered comprehensive, but in our study we do not consider them comprehensive, but rather specific to some cases that involve the transfer of data from one source to another, which are vulnerable to cyber-attacks. They may overlap with many applications and contexts.

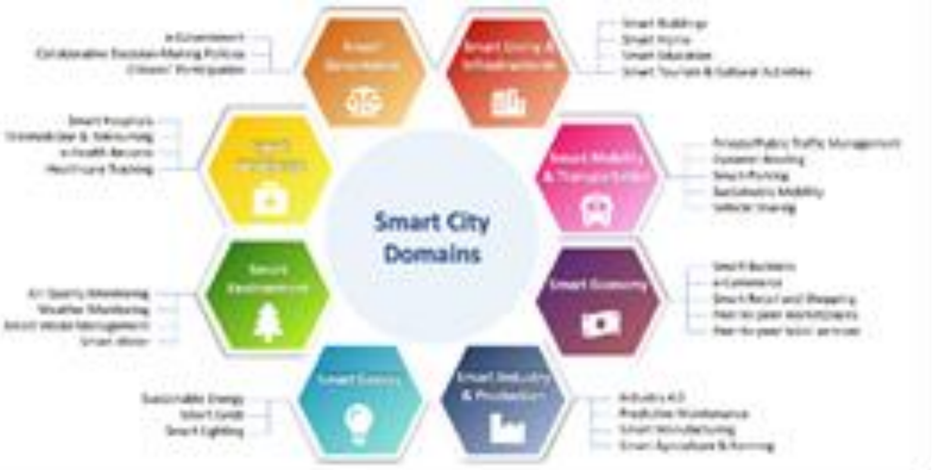


Figure 2: Smart city classification and its applications [15]

B. Challenges of cybersecurity in smart city

Smart cities are described as a model of urban innovation, but technological advances are facing cybersecurity challenges. The integration of computers and their applications in the Internet of Things (IoT) and GIS creates a complex cybersecurity landscape riddled with vulnerabilities and risks. This section delves into the topic of cybersecurity challenges from all aspects in smart cities, starting from the complexity of data acquisition in IoT and GIS to the evolution of major threats. There are several aspects to the cybersecurity challenges in smart cities, and they come from several factors, the first of which is the spread of IoT devices with few security measures and the unsecured data we obtain from GIS or traditional systems with a low level of security, and the nature of interconnection in smart cities [16-17]. IoT devices lack unified security methods, which makes them vulnerable to malicious attacks or the lack of updates to GIS data, which are often old versions that are not secure or their updates are not patched and are also vulnerable to attacks [18-19]. The complexity of interconnection systems in smart cities and their overlap is widely exploited by hackers and allows repeated interference and hacking of a single component, which leads to problems Serious and successive attacks. Sensitive information collected, whether from GPS or any other peripheral device, poses significant concerns regarding the privacy of that data, which makes it an attractive target for cybercriminals to achieve financial gains [20]. Smart cities face a variety of cyber threats, such as ransomware attacks, malware infections, denial-of-service attacks, and insider threats. All of these target critical infrastructure and data from IoT, GIS, data warehouses, and even cloud storage, which harms smart city operating systems [21]. Recent cyber attacks on smart cities, such as the ransomware attack on Atlanta in 2018 and on New Orleans in 2020, confirm the seriousness of cyber threats and their impact on infrastructure [22]. In conclusion, there are significant risks to smart cities posed by cybersecurity challenges to security and safety. In order to counter these attacks, greater efforts must be made by the government and its cooperation with cybersecurity experts and other stakeholders to take security measures, enhance efforts to detect threats and promote a culture of cybersecurity. The risks of threats can be mitigated by proactively responding to these threats.

Smart cities are the next step in the evolution of governments. Therefore, the procedures, requirements and applications may increase in the coming years. To build a strong foundation, we are developing an effective approach to increasing the security of data transferred between these applications, thus facilitating the task of laying the foundation for these cities. In the following section, we will review the most important studies that took into account data security in smart cities and how to eliminate attacks and maintain data security.

One of the major challenges is the integration of IoT and GIS into the field of cybersecurity. This opens the way for extensive research on effective strategies to protect data security in smart cities. Many devices contribute to collecting and transmitting data in real time, whether sensors or data from satellites, so they need protection protocols from malicious attacks. The study [23] highlighted the risks of attacks on IoT systems in smart cities and malware that infect infrastructure and propose encryption as a preventive measure. [24] Emphasizes the importance of encryption for transmission protocols in smart cities to make communication secure and secure sensitive data that has a strong impact on infrastructure and recommends the use of blockchain technology for decentralized storage. [25] Calls for authenticating IoT and GIS devices and authenticating data security during their transmission in smart city networks, especially in real time. One of the challenges facing researchers in Internet security in general and smart cities in particular is the interoperability of devices, as the lack of unified protocols exposes systems to major security vulnerabilities. [26] Proposed special standards for unified communications, integration in the Internet, and the transfer of data obtained from various devices and technologies in smart cities, reducing data breaches, and creating a secure environment in terms of hiding or encrypting interoperable data to thwart hackers. [27] Emphasizes unauthorized access to GIS data and proposes encryption algorithms, even if they are traditional methods for controlling data and role-based access, especially spatial data shared by traffic. [28] Points to another type of risk, which is related to attacks that manipulate data and deceive users, and calls for the use of intrusion detection systems in smart cities to prevent unauthorized access to databases, especially data related to financial affairs. The efforts made in the Internet of Things and GIS in securing data have led to the development of the smart city architecture and thus contributed to the advancement of urban cities. [29] Proposes an approach to using artificial intelligence to detect anomalies in data movement through transmission networks in real time, especially in GIS platforms, to enable early detection of breaches and their immediate processing in advanced security methods. [30] Emphasizes securing the communication layers, especially the physical layer, which plays a role in storing data and has direct contact with users and encrypting it in innovative ways, especially with regard to computers and passwords in bank accounts. [31] Discovered the need for encryption systems in smart cities to address the threats posed by weaknesses in infrastructure and data transmission through data acquisition devices and databases in particular. [32] Emphasizes the importance of developing security policies in terms of governance and working to find solutions within regulatory frameworks for information transmission networks. [33] Pointed to the need for cooperation between the public and private sectors to establish laws for cybersecurity standards, penalties and consequences caused by malicious attacks in smart cities.

Previous studies show a consensus on the need to secure data through encryption and pay attention to the security of protocols used in smart cities and build cybersecurity strategies for the source of information coming from GIS and IoT. Efforts are still being made to address challenges and provide promising solutions such as artificial intelligence and block chain to enhance data security in smart cities, as innovation continues to stand up to future cyber threats.

OBJECTIVES

The goal of a smart city is to improve the standard of living of residents by using the city's resources in the best and most effective way and working to provide a smart ecosystem using modern digital technologies. This is in order to build an innovative data transmission network, provide better water, and optimize energy use, good waste management and easy financial trading [34]. Residents in a smart city are connected to a smart data network to also contribute to decision-making, and for individual privacy and data security, cybersecurity protocols have been developed to ensure the security and confidentiality of smart governance data. Governance data is often more complex and sophisticated and requires electronic security awareness that uses digital technology in the best way. Therefore, the increasing risk to data security represents an endless challenge and mitigating these risks is a priority[35].

The rapid development of smart cities has transformed urban environments into highly interconnected ecosystems that leverage advanced technologies such as the Internet of Things (IoT) and Geographic Information Systems (GIS). These technologies enable real-time monitoring and efficient management of robust infrastructure, such as environmental resource management, transportation systems, and public safety systems [36]. Due to the increasing interconnectivity of these cities, they are vulnerable to many cyber threats. Therefore, the integrity of information obtained from GIS and IoT is an important priority to maintain the functionality and sustainability of smart cities. GIS information plays an effective role in establishing smart cities by providing spatial data responsible for decision-making and urban planning. The information obtained from GIS, when combined with Internet of Things information such as sensors, environmental sensors, smart meters, and cameras, allows city officials to analyze this data and respond in real time. By working with GIS with the Internet of Things, traffic flow can be improved very intelligently and energy consumption can be managed intelligently. Despite the many benefits, the possibility of attacks on this information by cybercriminals is possible, through this information, operations can be disrupted or physical damage can be caused by stealing secret data [37].

METHODS

In the context of smart cities supported by IoT and GPS, it is essential to maintain data security and integrity of its transmission as well. The information transmitted through the smart city network is of various types, including spatial information, infrastructure locations, sensor readings, and real-time communications such as transportation and environmental monitoring. All data is gathered in one context, which is the digital character, and is transmitted from the source to one of the communication layers, which is the transport layer, and then it takes a preliminary processing path through protocols and is transmitted to the physical layer. This is where it is tampered with and can be preserved through the encryption process as shown in Figure 3. Adopting encryption is a necessary process to ensure that it is not tampered with by unauthorized people, and in the same context, any tampering or infiltration into that data can be detected, thus preserving the security and confidentiality of data in the smart city.

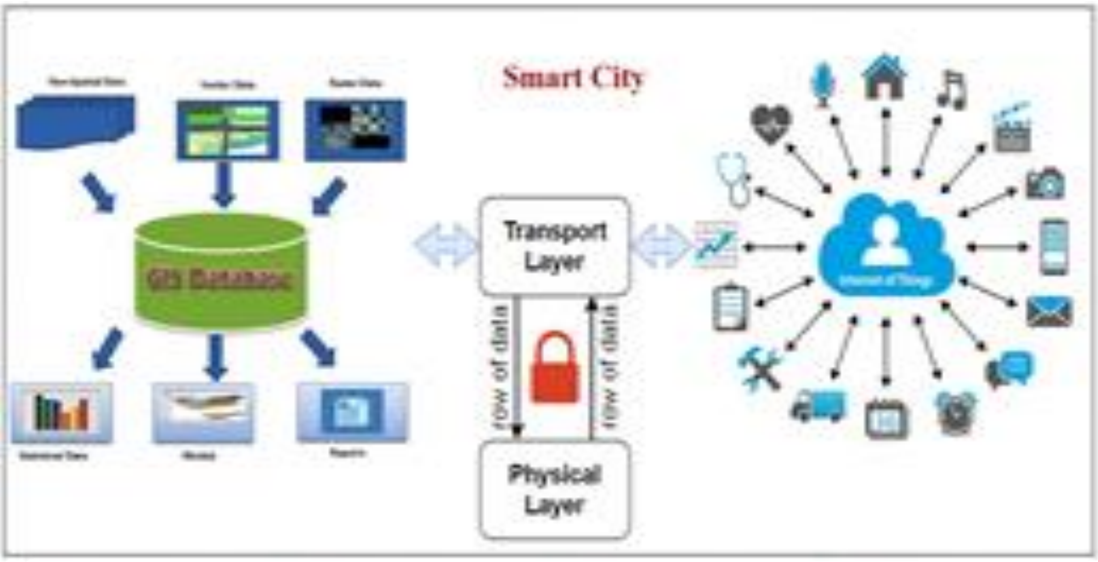


Figure 3: Data flow through smart city

In the context of cybersecurity, data in smart cities is somewhat complex and interconnected. Therefore, data is encrypted and a set of steps are taken as follows:

- Improving resource allocation for security data

Allocating resources such as computing power, transmission bandwidth and financial resources to protect smart city infrastructure is important. This problem can be formulated by covering the security objective and reducing the risks as follows:

$$max \sum_{i=1}^{N} S_i . W_i - \sum_{j=1}^{M} R_j . C_j \qquad (1)$$

Such that: consider as the security level with i component. Represent the weight of the component i, represent the risk and when threat j, N and M consider the total number of components and threat sequentially.

Problem try to find the optimal allocation resource xi that constraints like , when total budget is B.

- Building an Attack Propagation Analysis Model

The problem here is to understand how attacks propagate and their sources through the interconnected structure in order to develop appropriate defense mechanisms. To model the propagation of an attack through the infrastructure using a graph where nodes are IOT devices and GPS servers and their edges are potential paths of the attack as in the following equation:

$$\min_{(i,j)\in E} c_{ij} . x_{ij} \qquad (2)$$

Where E consider the set of connection between components. represent the attack cost (i,j). is the attack indicator which is (i,j) . The objective of this step is to find the cost effective of attack.

- Encryption Key Management for Mobile Data

In the Internet of Things, key management is not an easy task and is a major challenge due to physical constraints. Encryption key management can be modeled in a synthetic way to achieve the goal of minimizing the total communication costs and secure distribution of privileges as follows:

$$min \sum_{i=1}^{N} \sum_{j=1}^{N} E_{ij} . T_{ij} \qquad (3)$$

Where consider energy consumption that can exchange the key between the nodes i and j. while represent the time delay also distributed between node i and j. N is the IoT devices. Here will find the optimal key within the system which is minimized the energy though overhead.

- Real time detection

Any anomalous behavior in the system in real time will detect through IoT devices and GIS structure. That include potential security breaches. In this regard the model that can assume statistical hypothesis to test the system in term of H0 represent null value of normal behavior and H1 represent anomaly one. Then the following equation can illustrate:

$$\min \alpha + \beta \qquad (4)$$

Where represent positive rate false (type I error), and represent negative rate false (type II error). This detection in real time need to use statistical of machine learning to calculate the interval time.

Then we encrypt the data that is transmitted to and from users to be unknown and unauthorized to unauthorized people. Data in its digital form is easier to encrypt and to change its value it must be multiplied by a factor that is known in the encryption key to be returned and decrypted. As in Figure 4.

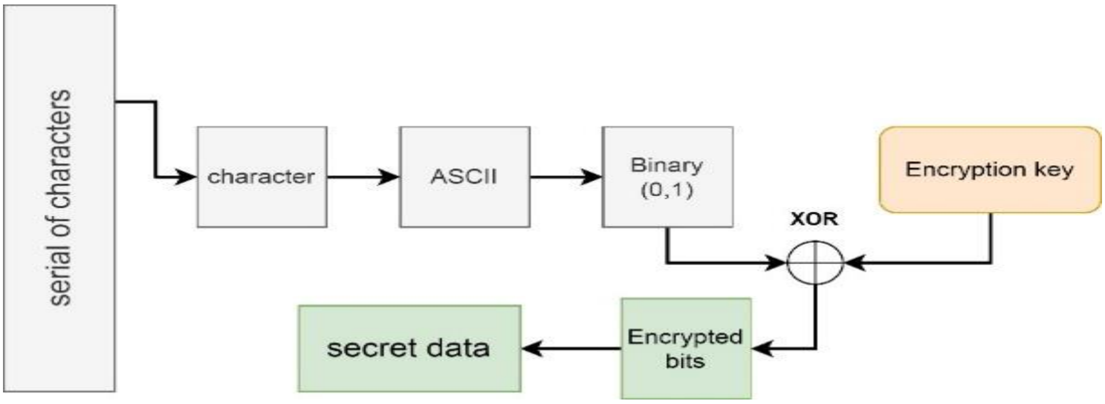


Figure 4: Encryption strategy

In the encryption process, we combine each bit of the transmitted data with the encryption key in the XOR method, and thus its value changes according to the encryption equation so that we can restore the original value of the bits at the other end in the same way by reversing the process, and thus no data can be lost during transmission or encryption. The encryption key is used to be a random variable so that it cannot be detected by intruders or hackers. We use the logistics map to increase the randomness of the encryption key. In each encryption cycle, the encryption equation changes and it becomes impossible to decrypt it by unauthorized persons with the help of the logistics map equation as follows:

$$X_{n+1} = \left(r\mathrm{X_n}(1 - \mathrm{X_n})\right) * \mathrm{K} \bmod 1 \quad (5)$$

Figure 5 shows the changing of randomness with logistic map behavior and for each iteration did not exceed the vale 1, and still changing while it is running during encryption.

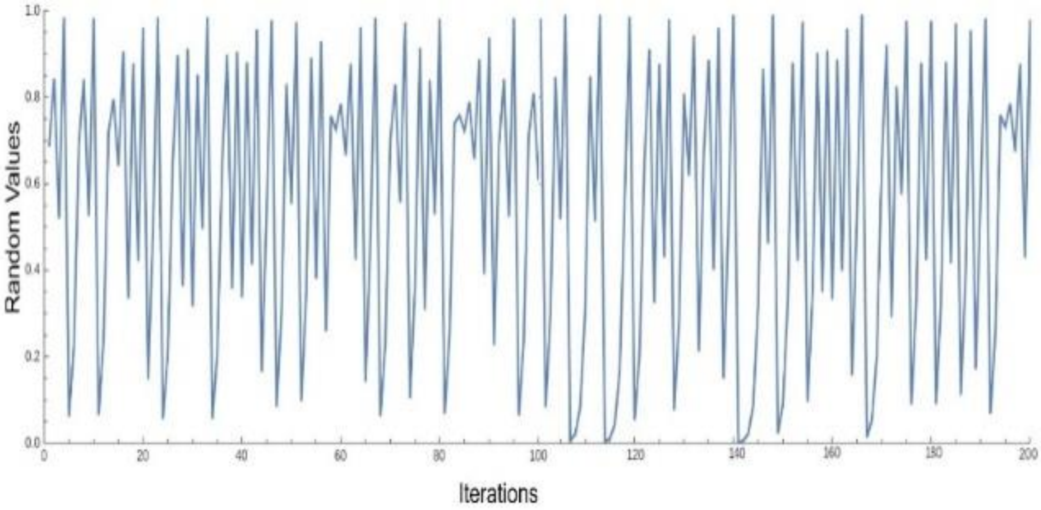


Figure 5: Logistic map behavior within encryption

Algorithms differ in terms of encryption strength, some are difficult and complex, and some are solvable. Therefore, we must check the encryption strength of the proposed algorithm, which depends mainly on the strength of randomness and the difficulty of decoding. In the following paragraph, we will test our proposed algorithm using methods and standards to know the encryption results.

RESULTS

As smart cities become increasingly sophisticated and integrated with GIS and IoT to secure data traffic in smart cities, cybersecurity is of strong strategic importance. The interconnected nature of modern technologies makes them a target for cyberattacks, which in turn impacts infrastructure and private data.

Encryption comes as a defensive solution to secure confidential data through the Internet of Things and information systems platforms. The encryption process takes place through several stages of transmission, processing and response, to protect data from unauthorized access and breaches. Encryption is one of the basic methods to secure communications and data that are transmitted artistically within smart cities. However, encryption provides a secure and robust way to implement smart cities, considering the best performance in terms of power consumption, scalability and accuracy. Due to the large size and rapid expansion of devices, it has become necessary to process data in real time and what encryption protocols require. The results prove the merit of the proposed method in terms of accuracy (80%), PSNR (86 dB) and real-time results.

DISCUSSION

In smart cities, in this study, we encrypt data coming from the Internet of Things or GPS that is transmitted in the city's data network. The data is in the form of data packets in transmission lines, and in order to secure it, we use the data in the encryption keys, which means the length of the data running in the channel. There are certain ratios for segmenting the data and making samples for encryption. First, the data is placed in the form of segments in a special vector called the buffer, and we merge it with the encryption key data, and then a secure data called the security vector is produced. This vector is in the form of a 2D matrix, as in Figure 6.

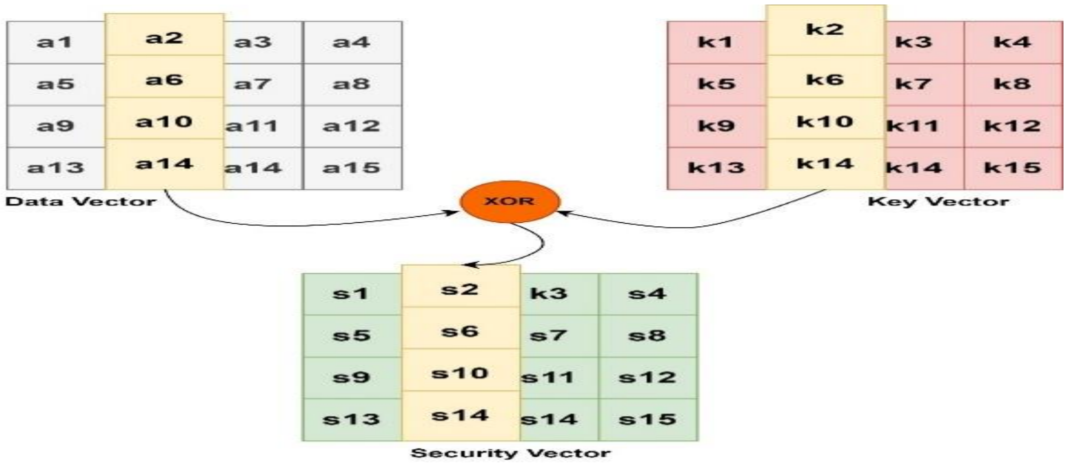


Figure 1: Data stream encryption

Number of criteria included in proposed method each can make effect into sybersecurity illustrated as C1 (Chip area), C2 (Throughput), C3 (Power consumption), C4 (Energy), C5 (Latency), C6 (Program), C7 (RAM), and C8 (Key size). These criteria consider as quantitative due to their nature, then decision making will show in Table 1.

Table 1: Criteria evaluation within normal encryption

iterations	C1 ($A_{Total} = A_{logic} + A_{memory}$)	C2 ($T = \frac{D_{amount}}{T_{time}}$)	C3 ($P = P_{dynamic} + P_{static}$)	C4 ($E = P \times t$)	C5 ($L = \frac{D(Bytes)}{T(Throuput)}$)	C6 ($C(ciper) = E_K(P)$)	C7 ($RAM_T = RAM_D + RAM_K$)	C8 ($Ks = 2^{128}$)
8	0.1213	0.0312	0.1546	0.0216	0.1231	0.2985	0.2973	0.2871
56	0.2635	0.0127	0.2514	0.3625	0.0352	0.3872	0.2418	0.2745
98	0.2933	0.0145	0.3751	0.0617	0.0288	0.0145	0.3857	0.2541
121	0.3527	0.4522	0.2754	0.2061	0.0529	0.3524	0.4625	0.3546
203	0.3743	0.0724	0.2458	0.2815	0.1756	0.0913	0.4821	0.2699

The most important criteria considered here is Peak Signal to Noise Ratio (PSNR) refers to the quality of data after encryption and can calculated as:

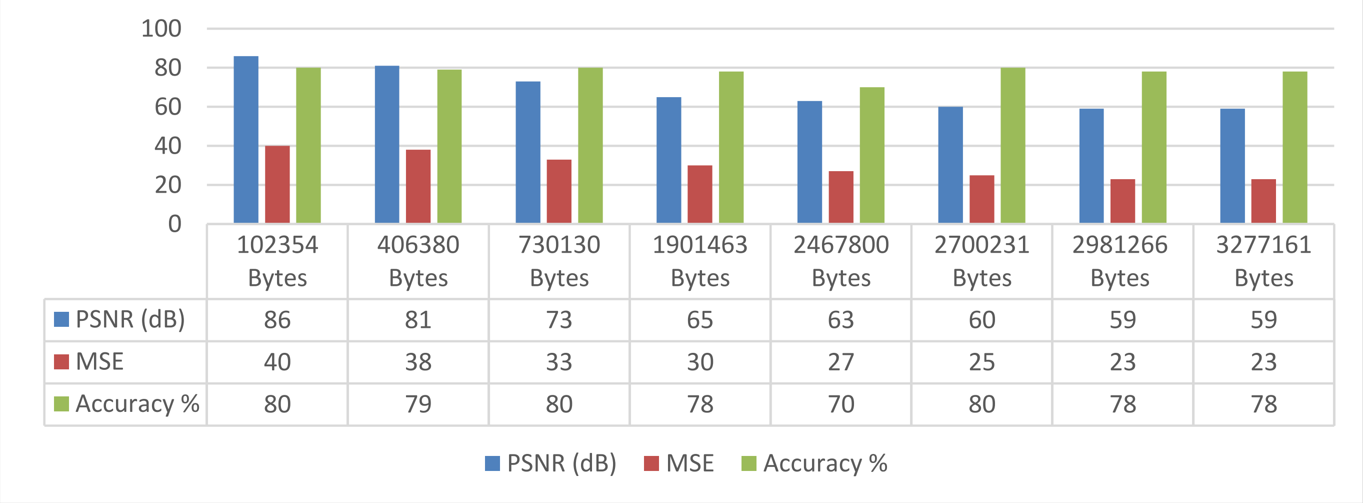
$$PSNR = 10.log_{10}\left(\frac{MAX_1^2}{MSE}\right) \qquad (6)$$

Where MSE is Mean Square Error and can find it by:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (7)$$

Where MAX consider as the maximum data value of m, n dimensions vector and I is original data and K is noisy data (encrypted).

PSNR value is negatively affected by MSE. When data is encrypted data, the data starts to increase its PSNR value. The higher its value, the better, i.e. the data has good quality even with the secret data. Increasing the data encrypted leads to destroy data, so traditional methods compete in the amount of data encrypted in multiple ways. The percentage of encryption varies from one method to another. The percentage can be measured on a scale of 1/8. The method can be tested in multiple proportions and in other ways, as in Figure 1:



	102354 Bytes	406380 Bytes	730130 Bytes	1901463 Bytes	2467800 Bytes	2700231 Bytes	2981266 Bytes	3277161 Bytes
🟦 PSNR (dB)	86	81	73	65	63	60	59	59
🟥 MSE	40	38	33	30	27	25	23	23
🟩 Accuracy %	80	79	80	78	70	80	78	78

Figure 2: Evaluation creteria for encryption in different payload

We notice from the previous figure that the PSNR is inversely proportional to the MSE rate. The PSNR expresses the ability to add strongly and without changing the original text without perceiving that the encrypted text is scattered but the meaning is the same. When the encrypted data increases, the PSNR value begins to stabilize because the algorithm gets used to it as if it was trained on it, and accuracy is a measure of the conformity of the encrypted text with the result of the proposed algorithm, which is considered very good in this context.

The results depend on the ability of the method to interact instantly with encrypted data, perform unconventional methods, and benefit from the weaknesses of previous methods, as will be explained in the next paragraph of the conclusions.

REFRENCES

[1] Tanseer, I., Kanwal, N., Asghar, M. N., Iqbal, A., Tanseer, F., & Fleury, M. (2020). Real-time, content-based communication load reduction in the internet of multimedia things. Applied Sciences, 10(3), 1152.

[2] López-Vargas, A., Fuentes, M., & Vivar, M. (2020). Challenges and opportunities of the internet of things for global development to achieve the United Nations sustainable development goals. IEEE Access, 8, 37202-37213.

[3] Ullah, F., Naeem, H., Jabbar, S., Khalid, S., Latif, M. A., Al-Turjman, F., & Mostarda, L. (2019). Cyber security threats detection in internet of things using deep learning approach. IEEE access, 7, 124379-124389.

[4] Laszka, A., Potteiger, B., Vorobeychik, Y., Amin, S., & Koutsoukos, X. (2016, April). Vulnerability of transportation networks to traffic-signal tampering. In 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS) (pp. 1-10). IEEE.

[5] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. Ieee Access, 8, 54314-54344.

[6] Soltan, S., Yannakakis, M., & Zussman, G. (2018). REACT to cyber attacks on power grids. IEEE Transactions on Network Science and Engineering, 6(3), 459-473.

[7] Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017). Characterizing cyber-physical attacks on water distribution systems. Journal of Water Resources Planning and Management, 143(5), 04017009.

[8] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[9] Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017, April). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In 2017 70th Annual conference for protective relay engineers (CPRE) (pp. 1-8). IEEE.

[10] Ozer, M., Varlioglu, S., Gonen, B., & Bastug, M. (2019, December). A prevention and a traction system for ransomware attacks. In 2019 international conference on computational science and computational intelligence (CSCI) (pp. 150-154). IEEE.

[11] Lytras, M. D., & Visvizi, A. (2018). Who uses smart city services and what to make of it: Toward interdisciplinary smart cities research. Sustainability, 10(6), 1998.

[12] Safari Bazargani, J., Sadeghi-Niaraki, A., & Choi, S. M. (2021). A survey of GIS and IoT integration: Applications and architecture. Applied Sciences, 11(21), 10365.

[13] Lafioune, N., & St-Jacques, M. (2020). Towards the creation of a searchable 3D smart city model. Innovation & Management Review, 17(3), 285-305.

[14] Tao, W. (2013). Interdisciplinary urban GIS for smart cities: advancements and opportunities. Geo-spatial Information Science, 16(1), 25-34.

[15] Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-enabled smart cities: A review of concepts, frameworks and key technologies. Applied Sciences, 12(3), 1607.

[16] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC medical informatics and decision making, 20, 1-10.

[17] Radoglou-Grammatikis, P., Dalamagkas, C., Lagkas, T., Zafeiropoulou, M., Atanasova, M., Zlatev, P., ... & Sarigiannidis, P. (2022, December). False data injection attacks against low voltage distribution systems. In GLOBECOM 2022-2022 IEEE Global Communications Conference (pp. 1856-1861). IEEE.

[18] Auffret, A. G., Rico, Y., Bullock, J. M., Hooftman, D. A., Pakeman, R. J., Soons, M. B., ... & Cousins, S. A. (2017). Plant functional connectivity–integrating landscape structure and effective dispersal. Journal of Ecology, 105(6), 1648-1656.

[19] Oliha, J. S., Biu, P. W., & Obi, O. C. (2024). SECURING THE SMART CITY: A REVIEW OF CYBERSECURITY CHALLENGES AND STRATEGIES. Engineering Science & Technology Journal, 5(2), 496-506.

[20] Fadhil, A. M., Jalo, H. N., & Mohammad, O. F. (2023). Improved Security of a Deep Learning-Based Steganography System with Imperceptibility Preservation. International journal of electrical and computer engineering systems, 14(1), 73-81.

[21] Radoglou-Grammatikis, P., Sarigiannidis, P., Efstathopoulos, G., Lagkas, T., Fragulis, G., & Sarigiannidis, A. (2021, June). A self-learning approach for detecting intrusions in healthcare systems. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[22] Fabian, P. S., Kwon, H. H., Vithanage, M., & Lee, J. H. (2023). Modeling, challenges, and strategies for understanding impacts of climate extremes (droughts and floods) on water quality in Asia: a review. Environmental Research, 225, 115617.

[23] Houichi, M., Jaidi, F., & Bouhoula, A. (2021, April). A systematic approach for IoT cyber-attacks detection in smart cities using machine learning techniques. In International Conference on Advanced Information Networking and Applications (pp. 215-228). Cham: Springer International Publishing.

[24] Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1-10.

[25] Chaturvedi, K., Matheus, A., Nguyen, S. H., & Kolbe, T. H. (2019). Securing spatial data infrastructures for distributed smart city applications and services. Future Generation Computer Systems, 101, 723-736.

[26] Tcholtchev, N., Lämmel, P., Scholz, R., Konitzer, W., & Schieferdecker, I. (2018, December). Enabling the structuring, enhancement and creation of urban ICT through the extension of a standardized smart city reference model. In 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion) (pp. 121-127). IEEE.

[27] Lv, Z., Li, X., Wang, W., Zhang, B., Hu, J., & Feng, S. (2018). Government affairs service platform for smart city. Future Generation Computer Systems, 81, 443-451.

[28] Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. Machines, 9(4), 78.

[29] Luckey, D., Fritz, H., Legatiuk, D., Dragos, K., & Smarsly, K. (2021). Artificial intelligence techniques for smart city applications. In Proceedings of the 18th International Conference on Computing in Civil and Building Engineering: ICCCBE 2020 (pp. 3-15). Springer International Publishing.

[30] Abed, N. K., Shahzad, A., & Mohammedali, A. (2023, October). An improve service quality of mobile banking using deep learning method for customer satisfaction. In AIP Conference Proceedings (Vol. 2746, No. 1). AIP Publishing.

[31] Desai, B., Patil, K., Mehta, I., & Patil, A. (2024). A Secure Communication Framework for Smart City Infrastructure Leveraging Encryption, Intrusion Detection, and Blockchain Technology. Advances in Computer Sciences, 7(1).

[32] Khanna, A., Sah, A., Bolshev, V., Jasinski, M., Vinogradov, A., Leonowicz, Z., & Jasiński, M. (2021). Blockchain: Future of e-governance in smart cities. Sustainability, 13(21), 11840.

[33] Mijwil, M. M., Doshi, R., Hiran, K. K., Al-Mistarehi, A. H., & Gök, M. (2022). Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects. Mesopotamian journal of cybersecurity, 2022, 1-4.

[34] Chen, Z., Gan, W., Wu, J., Lin, H., & Chen, C. M. (2024). Metaverse for smart cities: A surveys. Internet of Things and Cyber-Physical Systems.

[35] Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. The Review of Financial Studies, 36(1), 351-407.

[36] Muravskyi, V., Kundeus, O., Hrytsyshyn, A., & Lutsiv, R. (2023). Accounting in a smart city with the combined use of the Internet of Things and geographic information systems. Herald of Economics, (2), 41-57.

[37] Sharma, R., & Arya, R. (2023). Security threats and measures in the Internet of Things for smart city infrastructure: A state of art. Transactions on Emerging Telecommunications Technologies, 34(11), e4571.