6G- enabled smart city networking model using lightweight security module

M. M. Kamruzzaman
Department of Computer Science
Jouf University
Sakaka, Al-Jouf, KSA
mmkamruzzaman@ju.edu.sa

Abstract

Smart cities use lightweight security module technologies like sixth-generation (6G) and wireless connections to improve people's quality of life. A smart city can use a networking model to power and monitor many geographically distributed networking models to support various applications like energy and resource management, intelligent transportation systems, and e-health. To manage smart city resources efficiently and intelligently, a significant state architecture must service various technologies due to the enormous development in networking models and the amount of data they generate. This research work presents a smart city networking architecture for smart city environments employing the lightweight security module (SCNM-LSM) in this work in progress article. It first offers a new conceptual framework termed the conventional model for activity off-loading and resource allocation. Second, it enhances the standard model by including off-loading and resource allocation awareness. It expands on the specific research topics to create and study the effectiveness of individual components with the previous models to accommodate technological improvements like the use of Artificial Intelligence (AI) in the sixth generation data transmission technology.

Keyword: 6G, Artificial Intelligence, smart city, lightweight security module, smart city networking

1. Overview of Smart city networking and lightweight security module

Several significant cities worldwide are looking at implementing smart city technologies to improve the existing quality of their citizens and maximize the use of city arrangements and services [1]. Smart services to enhance efficiency and setups in medical, transportations, power, schooling, and several other industries are provided by various modern technologies and methodologies that enable such models [2-3]. At the same time, these services help smart cities save money by lowering operating expenses and reducing resource usage. Internet of Things (IoT), robots, fog computation, data storage, and predictive analysis are examples of these technologies [4]. Smart cities can gain a lot of benefits and services by implementing these technologies. WSNs are used to monitor the state of smart city resources and infrastructures in real-time [5]. The Internet of Things allows actual devices in a municipal network to be integrated more easily. CPS is used in smart cities to let people connect more productively with the online and physical worlds. Unmanned aerial vehicles (UAVs) and robotics provide automation and valuable services [6-7]. Environmental surveillance, traffic conditions, privacy and safety measures, and wireless connectivity are just a few examples of these types of services. It can get lower latency, better movement, streamed, and practical assistance [8-9]. The scalable and cost-effective processing and data storage platform of cloud computing benefit the smart city applications.

These contemporary technologies are utilized to deliver a range of intelligent urban services [10-11]. Smart solutions are exemplary for enhancing road design and city street traffic prevention, offering smart road signals and parks, promoting vehicle safety, and enabling self-driving cars [12-14]. For instance, intelligent energy services might help cities efficiently choose more educated energy and power consumption [15]. Smart power services contribute to the utilization of intelligent networks, intelligent buildings, and sustainable sources. Other intelligent solutions include architectural health surveillance and real-time surveillance of crowds in bridges, pipelines, trains and metro lines, and oil and gas pipelines [16]. Smart monitoring systems and public protection and surveillance solutions are among several options accessible [17].

The main contributions of this article are as follows:

- An architectural design is proposed for smart cities to enhance security using 6G technologies.
- A lightweight security model is designed to reduce the complexity of communication in a smart city environment.
- The mathematical model of the lightweight security model is verified and tested.

The rest of the article is as follows: Section 2 demonstrates the background to the security models in a smart city. The proposed smart city environment employing the lightweight security module (SCNM-LSM) is designed, analyzed, and implemented in section 3. Section 4 illustrates the software analysis and evaluation of the proposed system. The conclusion and future scope are depicted in section 5.

2. Background to the security models in smart city

This section investigated and studied the precise concept of smart cities and their demands and existing information structure conditions. This section also discussed the challenges in urban planning information suggested by Bhat et al. [18]. Simultaneously, the basic notion of the Internet of Things and its specialized application to build digital technologies in smart cities was analyzed and studied precisely in this section.

2.1 Basic concepts and core technologies of the Internet of Things

The IoT-enabled technology continually matured and developed with the ongoing growth and invention of information networks and online technologies. In the US, the Computing technique was initially suggested by Jamil et al. [19]. It first features advanced embedded sensors such as the RFID-enabled system to interconnect physical subjects accessible to the Web to intelligently identify and manage material things.

The IoT devices were mainly defined by the IoT technology, which kept referring to the communications infrastructure technology which shattered the constraints of place and time between people, places, and events in society, and realized the above three links to be able at all times and somewhere to interact with one another [20].

The Internet of Things' significance was that virtual individuality and items can at varying moments connected to them using an array of sensors, depending on some standard and coherent communication channels and centered on adaptable, smart interfaces suggested by Lv et al. [21]. That user can access the atmosphere where people live. Web development was a different communication system to carry out information exchange [22].

Regional systematization and complication were the trends towards the Internet of things suggested by Das et al. [23]. As the main trend in urban building and growth, the clever metropolis was the long-term viability of urban planning and governance.

2.2 The core technology of the Internet of Things

The core structure and its associated communication mechanism were leading techniques on the Internet of Things. The IoT-based architecture was separated into three levels: perceptual layer, information, and communication systems. A particular communication technique allowed connectivity between levels [24]. In the analytics platform of smart cities were the Internet of Things (IoT) technologies widely employed.

The following were formulated in the three layers: The essential function of the overall Internet of Things technologies was the perceiving layer suggested by Ismagilova et al. [25]. It mostly communicated with the actual world. Data gathering devices like wireless communication can be the essential elements of the perceptual layer, collecting all types of statical and equations to describe from the objects of interest and then sending the senses to consumers or intelligent terminals with that information. Reality and particular knowledge had varied with computer and mobile smart terminal technologies [26].

The networking layer's major role was to link data obtained by the perceptual layer to the Internet and the web application. The networking layer used broadband Wi-Fi, WiMAX, or other urban wireless network technologies, and a wider variety of 4G and 5G mobile wide-scale communication technologies, such as Zigbee, Bluetooth, and many other wireless networking technologies [27]. The Wireless Local Area Network (WLAN) mentioned technology made it possible, wherever, to upload a huge number of data gathered through the receiver layer.

The application server generally performed the process, storing, evaluating, judging, and reprocessing information according to user demands to give distributed systems and smart services to people in various locations and areas [28]. Multitudes of different sizes were involved in many security problems, and the increased usage of mobile telephones had shown these crowds as an intriguing new data source. Esposito et al. denoted in a high-quality smart city crowd detection system [29]. It collects data from cell devices and social networking sites. It was then analyzed and processed such that an event was identified. Data from the sensing elements can also be collected to achieve knowledge about an occurrence [30]. The results demonstrated 82% accuracy and 61% penetration in identifying messages associated with public safety.

Losavio et al. offered urban areas crowd software solutions related to mobile sensing technologies [31]. Its functions included providing event information via mobile telephones, analyzing the gathered participation sensors data, identifying multicast material, and analyzing the finished event. The technology had been tested at 14 European tournaments. The findings indicated the greatest feature of the scatter diagram.

In certain emergency remedies, cellphones were employed. Yet, these strategies depended on messages, conversations, and social networks for communications reasons. This article offered disaster response architecture to identify and warn emergency centers, including information received via mobile device sensors. A new architecture is needed to overcome all the security issues and system complexity.

3. Proposed smart city environment employing the lightweight security module (SCNM-LSM)

Advanced innovation is driven by several causes, such as cultural transformations, economic problems, and aging populations. The 6G and the intelligent city are in the lead. This section discusses how 6G technology transforms the most significant vertical sectors in IoT and how 6G is a key driver in this shift. Generally speaking, 6G technology implementations might be classed as several industry sectors, such as electricity, medical, production, news and entertainment, automobile, and public transit, in several dimensions. In addition, several apps are available for any vertical company.

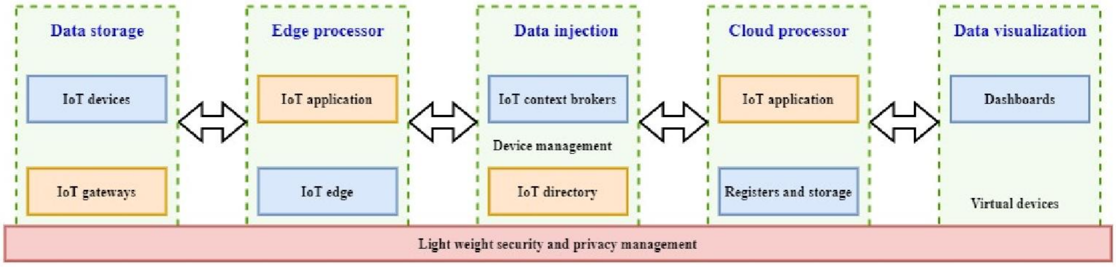

Figure 1. The architecture of the proposed SCNM-LSM system

The architecture of the proposed SCNM-LSM system is depicted in Figure 1. It has data storage, edge processer, data injection, cloud processor, and data visualization modules. It has IoT applications, registers, and dashboards that are used for the connection. Energy production, transportation, and consumption are all changing in the world. Formerly, a large central power plant serviced the end-user need. Therefore, with sustainable sources growing, tiny power stations like solar, wind, and hydroelectric electricity become less dependable. Massive outdated power generators are replacing hundreds of these tiny dispersed power stations. That results in a one-way to a two-way stream of power generation and transmission networks, allowing the company to generate companies. Data and connectivity are needed for the creation of future smart grids. The model provided in this article deals with communication networks and the importance of sensing devices in intelligent meters. They suggest that current services be combined into contemporary information and communication theory platforms to provide online communication for people and energy consumers. The study also looks at contemporary networks and 6G connections for intelligent grids and future frames and barriers.

A messaging system employs different cable and wireless technologies and materials to promote sharing information among two or more network components. Over time, the technological revolution has advanced dramatically, especially digital connectivity. The technical application of a certain standard, which incorporates new techniques and features to distinguish it from previous generations, marks this developmental stage.

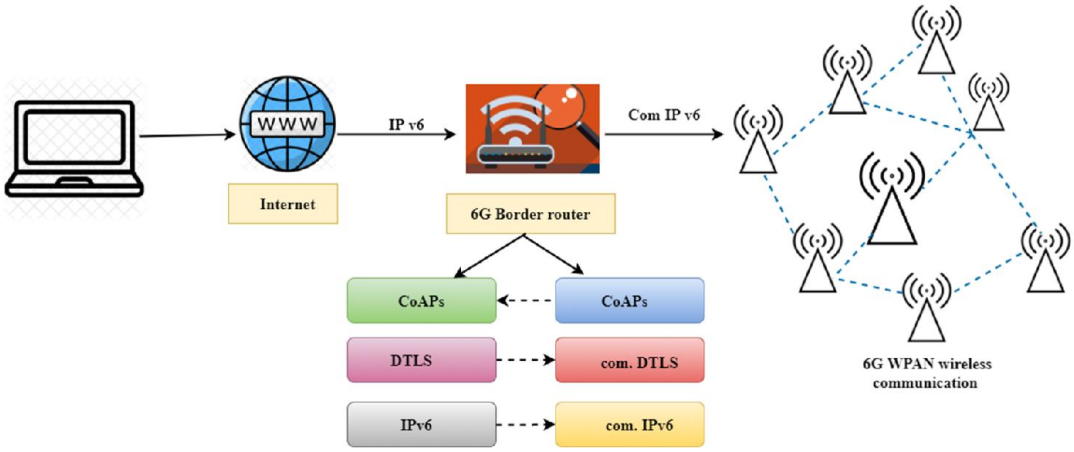

Figure 2. 6G WPAN network lightweight security

Figure 2 shows an IoT configuration with a list of low-energy 6G wireless personal area network (WPAN) network lightweight security solutions and the simple Internet technologies that go with it. Even though communication security protects communications, networks are subject to various assaults targeted at causing network disruption. Intrusion detection systems and firewalls safeguard against such attacks. Because the IoT shares properties with WSNs, Intelligent Data Systems (IDS) could be applied to the IoT.

On the other hand, most of these approaches assume that there is no centralized management and control point, that messages are not encrypted, and that IoT devices are only uniquely recognized within WSNs. The 6G is always accessible to connect 6G WPAN networks to the Internet in the IoTs, and end-to-end (E2E) message security is a must. As a result, creating new IDS for the IoT that takes advantage of these novel capabilities is essential. Despite these advantages, developing IDS for the IoT is challenging because of global accessibility, limited resources, lossy connectivity, and novel IoT protocols.

3.1 An optimized lightweight edge fog algorithm

There are obese and hard to extend the existing pervasive computing network topology overall. This section thus offers small fog computer resources depending on the fog. It illustrates the appropriate model of the Lightweight Fog networks computation proposed. In this concept, terminals device level, fog core networking, and cloud services center are included.

At the fog networking level, geo-position software services are provided in distinct areas. The controlling node performs uniform network administration and computes storing resource development for this hardware level. The control aircraft and data planes are segregated at the fog networking topology. Control nodes set up and maintain network devices evenly by checking data flow via the aircraft. S_{pe} performs awareness and perception, S_{in} indicates signal strength, but others are variables for related core function in Equation (1). R stands for matched dependability.

$$S_{pe,x} = S_{in} t_{pe,x}^{-\delta} s_{pe,x} \quad (1)$$

The signal strength is denoted S_{in}, the performance timing with given degradation factor δ is denoted $t_{pe,x}^{-\delta}$. The computation function $\bar{\bar{\pi}}$ is denoted I Equation (2)

$$\bar{\bar{\pi}} = \arg[\max(R^{\pi}(x))] \quad (2)$$

$R^{\pi}(x)$ relates largely to client computers in the devices endpoint layer and is the source of knowledge for cloud computing data. The fog subnet must supply endpoint devices with network connectivity, data transmission, and computer storage capabilities. Corresponding fundamental function in Equation (3), V is a solid node reliability matched degree, x is a different element-time.

$$R^{\pi}(x) = V_x + \alpha V_{x+1} + \alpha^2 V_{x+2} + \cdots = \sum_{p=0}^{\infty} \alpha^p V_{x+p} \quad (3)$$

The reliability of the node is denoted V_x. The scaling factor is denoted α. In the next five phases, the fog internet protocol primarily follows: Initially, the information transmitting gadget for the different fog networks send queries to the regulation node after reception of the command line information on the connect side, then contacting the work schedules module, assign the physical storage per the real incident and eventually start generating the container packet-switched layer networks.

The fog server then responds to the master control station that provides the particular container data when the containers in the fog layer are accessed. Then they obtain effective modules to the function routing table and articulate the packet transmission rules once the container has received the answer message created. Lastly, the routing table downloading mode sends the data transmission rules devices to the cloud computing layer beneath the routing table. It provides the reply information—the related data processor layer of fog networks displays. The relevant trust mechanism is defined by several communication nodes in the ultra-lightweight method described in this work.

This algorithm demonstrates the appropriate successfulness of communication. SR_{xy} is significant reliability, and it is expressed in Equation (4)

$$SR_{xy} = N_{si} \times \frac{{\delta_{xy}}^{N_{si}}}{{\delta_{xy}}^{N_{it}-N_{si}}} \qquad (4)$$

The number of significant interactions is represented by N_{it}. N_{si} is the maximum number of encounters. δ_{xy} indicates the success rate of interaction. Equation (5) shows the appropriate algorithm of the probability density function.

$$\Pr\left(\delta_{xy}\middle|N_{si}\right) = \frac{\Pr(N_{si}|\delta_{xy})\times\Pr(\delta_{xy})}{\Pr(N_{si})} \qquad (5)$$

The probability of maximum incidence concerning success rate is denoted $\Pr(N_{si}|\delta_{xy})$, the probability of success rate is denoted $\Pr(\delta_{xy})$, and the probability of the maximum incidence is denoted $\Pr(N_{si})$. The appropriate formula is displayed in Equation (6).

$$E_{xy} = P\left(\delta_{xy}\right) = \frac{(N_{si}+1)}{N_{it}+2} \qquad (6)$$

The maximum number of incidence is denoted N_{si}, and the total number of incidence is denoted N_{it}. The functional value of the success rate is denoted $P\left(\delta_{xy}\right)$. The method for calculating overall dependability is indicated in the Solution. The dependability function is denoted in Equation (7)

$$M_{xy} = \frac{(1-\vartheta)M_{xy}(x-v)}{\vartheta E_{xy}} \qquad (7)$$

ϑ denotes credibility, Δm refers for varying points another is coefficient. M indicates temporal differences. The expected value is denoted E_{xy}. The function for determining the dependability of all the other sides is denoted in Equation (8).

$$M_{xy} = \frac{(1-\vartheta)M_{xy}(x-v)}{\vartheta B_{xy}} \qquad (8)$$

ϑ denotes credibility. The dependability function is denoted M_{xy}. The initial biased condition is denoted B_{xy}. The input data is denoted x, and the minimum input value is denoted v.

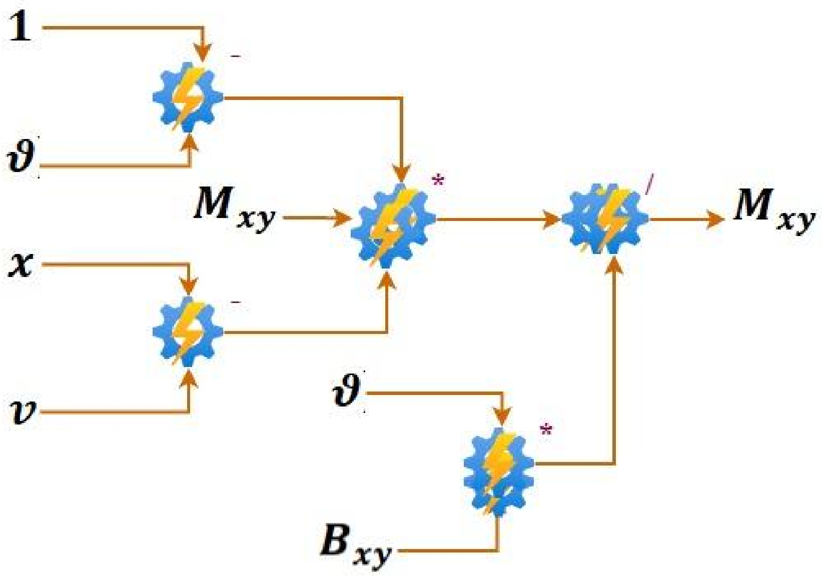

Figure 3. Pictorial representation of dependability

The pictorial representation of dependability is depicted in Figure 3. It uses input from the user, security protocols, biasing conditions at the sender and receiver end, dependability in the previous case. Based on the calculation, it calculates the updated dependability.

3.2 Security of user/machine access and auditing

Several users linked entities, like the Internet of things, IoT - based interfaces, Reporting tools, and data management, have to protect the confidentiality and safety of their IoT stacks. Hence, defining the consumer identification and permission method is necessary before approaching the IoT safety aspects.

The Snap4City platform employs multiple techniques to empower consumers to acquire system resources utilizing security and authorization compliance. A dispersed directory's ability to exchange, depending on the proposed SCNM-LSM, Portable Directory Processing Requirement, and partly maintained, is partly handled by the Member Registration (that are kept synced).

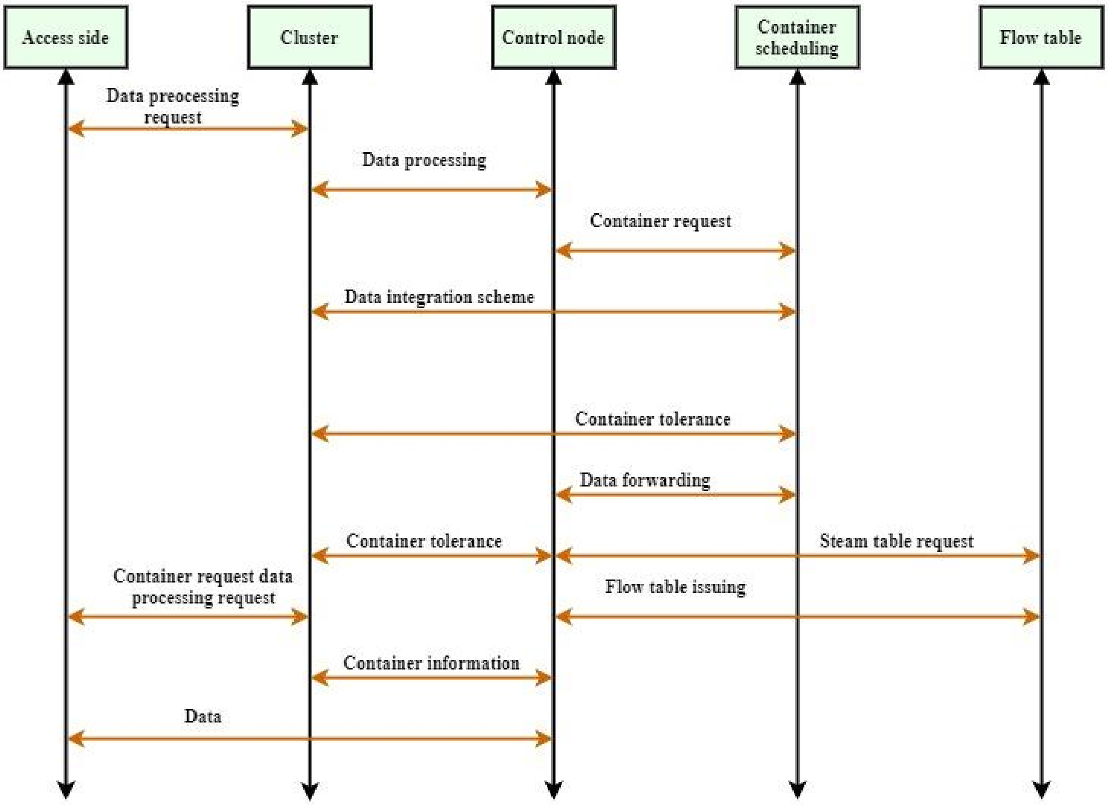

Figure 4. Security interaction model

The security interaction model is denoted in Figure 4. It uses the access side, cluster control node, scheduling node, and flow table. Initially, the data processing request is raised by the end-users. Then the control is sent to the container scheduler. The request is grant-based in the available time slot. The access side sends the data after the flow table issues they grant permission.

The SCNM-LSM component can only be accessed over an unencrypted subnetwork to guard against assaults. Users can check, amend, and finally request their user database to be entirely deleted in compliance with the network on the database. Compulsory Data includes: identities, security flaw hashed versions, e-mails, roles, and memberships for organizations/group groupings.

The login is the key that participants in the Snap4City system are identified by first. These roles are being used to classify individuals regarding the confidence level and give them access to functions Snap4City (Administrator, District Manager, ToolAdmin, RootAdmin) to provide various signals views, allowing more or less data research. In addition, even with restricted features, certain tools can also be played by public/ unknown people.

The data on the organization is utilized as a key in the grouping of people in terms of geography or function and membership (for organizations, e.g., Firenze, Helsinki, Antwerp). Various groups are established for each organization, and each organization denies its own identities, such as programmers, ICT authorities, developers from other parties, consumers, and policymakers.

A simple Sign object (SSO) with Digital Certificates is used to implement the authentication process. It uses the OpenIDConnect standard to enable the authentication process for all components of Snap4City, including the Consumer Resource Management (CRM) based module Drupal and Keycloak for the OpenIDConnect. As OpenIDConnect relies on OAuth 3.0, it is being used to enhance authentications using the identity component of the user.

Following the sequence number provided, demand is sent to SSO Servers to validate if the client is already enrolled into a resource accessible to a Snap4City component. If the client is not logging in, the user must give usernames and passwords to the SSO servers. Where the passwords in the SCNM-LSM client registration match, the client is authorized.

Finally, the asset displayed in the Snap4City component should be permitted based on the different ad hoc applications given by the components to be accessible. In the SSO Regulations, the role of the user-defined in SCNM-LSM is mapped. Hence, in particular, the network manager set the accessibility rule, which allows or prohibits access to specified Snap4City components (specifying grants) to a certain participant's role.

Keycloak passes the users and responsibilities of the Snap4City components accessed during authentification. When any user has access to a certain component, it implements an additional ad hoc permission to certify the HTTP request. To find the organizations and organizations to which it belongs. The component can also access SCNM-LSM. Any interaction between a few Snap4City components is carried out in addition to the standard. Distribution is therefore maintained in confidence, and the SSO Process operates via the various modules using a transitory, secret key scheme in the format of an authenticator.

Suppose such a method is not available or not acceptable (elapsed, flawed, or properly documented) in an engaging environment. In that case, as stated above, the client is routed to the internet login screen. When a link to mobile-to-mobile (M2M) is necessary, for illustration, an entity wishes to share Snap4City. MicroService components, including IoT end devices or IoT software, a regular person needs to supply at minimum for first-time privileges.

The token is opened offline, and the computer does not have to ask for login and use the refreshed token to demand a regular token, as described above. The refreshing offsite token is a lifespan that limits human interference and keeps it safe. Upon proper identity verification and identifying a validated access token return, the token attaches the Snap4City component as its attributes. These are being used to ensure that the consumer can access the desired information/resource sufficiently.

OpenIDConnect system permits consumers to identify access points and communicate between multiple Snap4City components. This setup allows the user experience to be a pleasant while, at the same moment, procedures are put up for thorough user access audits. That is a required infrastructure surveillance need. In the case of leakage or malevolent interference, the problem can be diagnosed, but there is no necessity for a total system redesign. The credentials used by various Snap4City components for strong authentication accessing SSO servers are special to any component.

3.3 IoT applications vs. security

IoT Systems use internet connectivity from storing and connectivity to IoT Systems, database management, and basic distributed systems, as stated in the needs mentioned above and the basic design. Snap4City customers leverage node environments supplemented with many Snap4City units or MicroServices to develop IoT systems with business rules. It is possible to perform IoT cloud services or as IoT network edge.

Therefore, to cover all instances and scenarios, multiple security techniques must be implemented. When an Internet-of-things application runs in the cloud, the program runs on an Apache Mesos & Marathon group in a Docker image. A proxy server setup that follows the various rearrangements of the containers cluster ensures internet connectivity to the node user experience. An ad hoc identification component has been designed to work with the node department of homeland security.

A so-called approach to connect the access permissions control's wisdom into Snap4City architecture has been developed. The node program has been adapted so that people with various roles access it. Whenever a user enters an IoT solution, the login is done the same way as for every other Snap4City component. An update token is obtained from SSO servers, which is always swapped with a certificate for access to every Snap4City component in the IoT platform.

The token is updated to prevent users from logging and thus handling M2M interaction. The system instantly updates in eight seconds because the Internet app runs on clusters and might migrate across many servers over a period. The refreshing token is stored securely in internal memory with unique access to single IoT software.

Consumers cannot independently download additional nodes out from the node framework for security considerations despite the freedom. They need to request the administration to approve and import them. The virtual machine group continually monitors the quantity and motivates and engages on it using the Program and Micro Service Monitoring and Analyst tool.

The user experience is normally only accessed in a direct-wired connection even by the Edge Devices owner if the IoT software is performed at the assumption of IoT end devices. Throughout this case, if it has to access certain Snap4City functions on the cloud (e.g., Micro Services) by the Busty Logical (IoT deployment) authored by user software developers, it can manually process and directly add the credentials into the node stream. The framework transfers these functions for a legitimate recharge token and obeys the circumstance. The proposed SCNM-LSM is designed in this section with low complexity architecture and a high-security model. The performance of the proposed SCNM-LSM is tested and evaluated in the next section.

4. Software analysis and evaluation

Many teams have tested and emphasized the system in more than 150 distinct test situations mentioned on https://www.snap4city.org/108 to verify a Snap4City system. It took about two years for the final verification of the PCP, including various verification forms for technical development companies. ICT authorities for workable and non-prerequisites, City Technicians with scorecards and operating cases, end-users with mobile Applications, and multitudes of customers, including even cloud tests performed and spread penetration testing. Snap4City has competed with over 25 different smart city technologies in the PCP, therefore. Snap4City has won the many IoT Systems for Smart City, and you may view the achievement, the films, the connection to a list of accomplished and verified criteria, and the Select4Cities websites. Furthermore, competitiveness was opposed to the specifications and their successful application and verification through test cases.

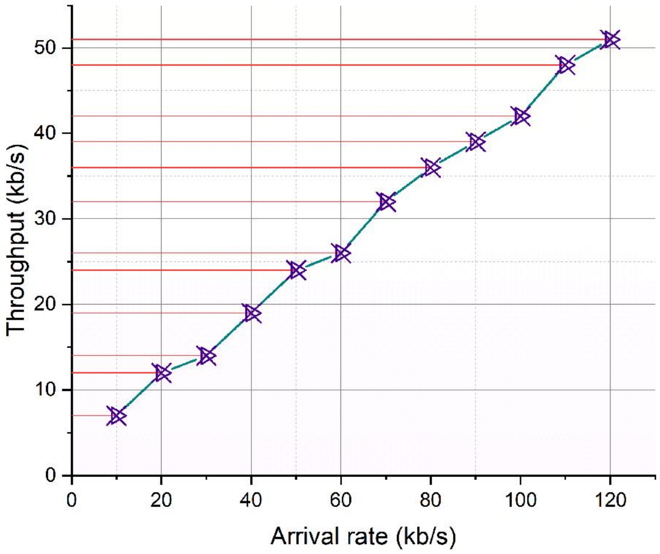

Figure 5(a). Throughput analysis of the existing PCA system

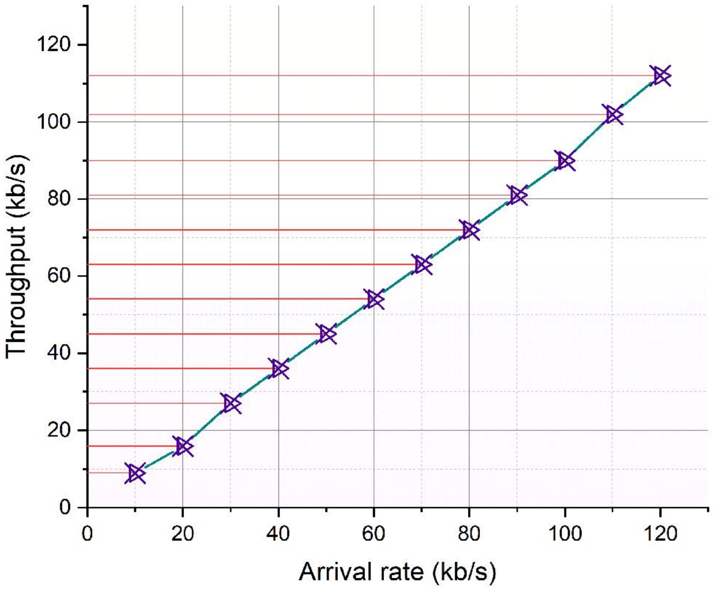

Figure 5(b). Throughput analysis of proposed SCNM-LSM system

Figures 5(a) and 5(b) show the throughput analysis of the existing Principal Component Analysis (PCA) model and the proposed SCNM-LSM system, respectively. The simulation is done by varying the arrival rate from a minimum value to a maximum value, and the respective throughput of the system is analyzed. The throughput is a measure of the number of successful data received at the received end. As the arrival rate increases, the network can process more data and increase the successful data at the receiver. The proposed SCNM-LSM system with 6G technology and resource allocation model enhances the performance.

Table 1. Simulation analysis of the proposed SCNM-LSM system

Task type	Service time (s)	Response period (s)	Reliability (%)	Usability (%)
Transport service system	2.54	1.82	95	85
Supply service system	2.95	1.75	87	67
Warehousing service system	3.84	1.92	92	91

Table 1 shows the simulation analysis of the proposed SCNM-LSM system. The different types of tasks are analyzed, such as transport supply, supply service, and warehousing. The respective outcomes of the proposed SCNM-LSM system, such as service time, response time, reliability, and usability, are analyzed and tabulated. The results show that the proposed SCNM-LSM system has the highest performance with the help of resource allocation methods and lightweight security models.

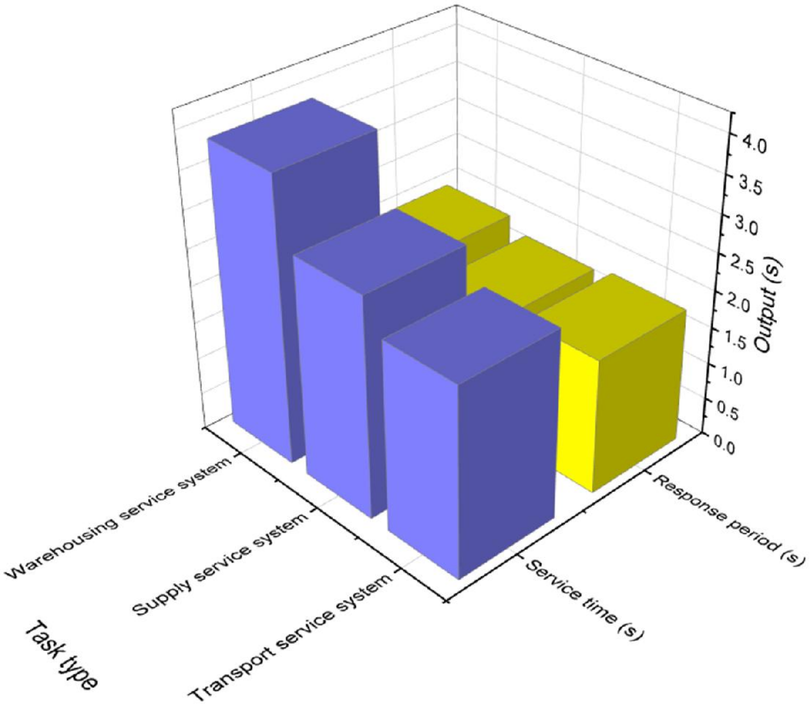

Figure 6(a). Simulation timing analysis of the proposed SCNM-LSM system

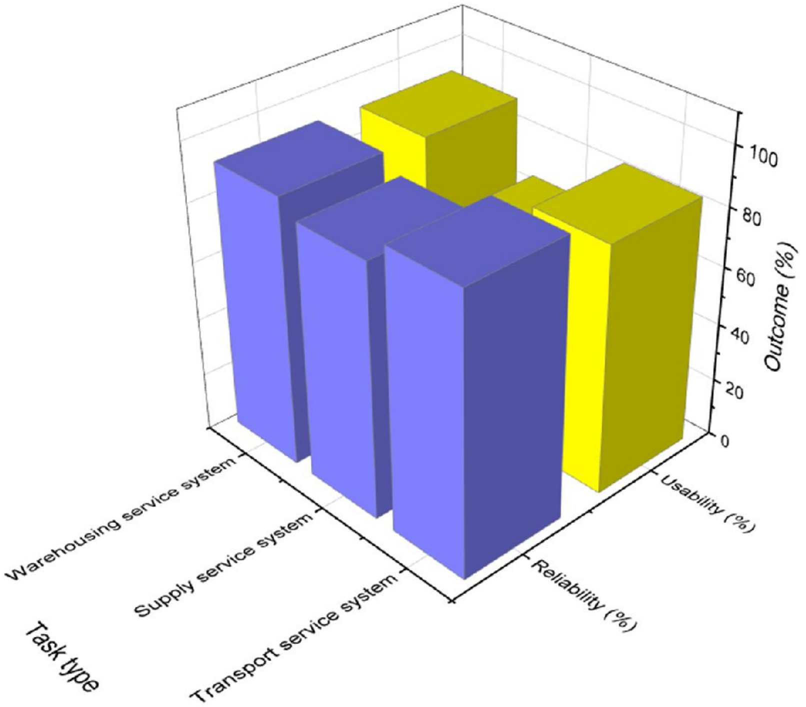

Figure 6(b). Simulation outcome analysis of the proposed SCNM-LSM system

The simulation timing analysis and outcome analysis of the proposed SCNM-LSM system are depicted in Figures 6(a) and 6(b). The simulation is done with the help of a given dataset, and the simulation outcomes of the proposed SCNM-LSM system are analyzed for one month. The simulation outcomes are compared with each other. The proposed SCNM-LSM system with a lightweight security model exhibits lower service and response time, whereas, with the help of 6G technology, it produces higher performance.

Table 2. Software outcome analysis of the proposed SCNM-LSM system

Parameter	PCA (%)	SCNM-LSM (%)
Accuracy	75	91
Precision	64	89
F score	71	96
Recall rate	69	90
Efficiency	48	87

Table 2 shows the software outcome analysis of the proposed SCNM-LSM system. The simulation outcomes such as accuracy, precision, F score, recall rate, and efficiency of the proposed SCNM-LSM system are analyzed and compared with the existing PCA model. The simulation outcomes of the proposed SCNM-LSM system are higher. The proposed model with a lighter security model reduces the system's complexity and enhances the performance with the help of the 6G model.

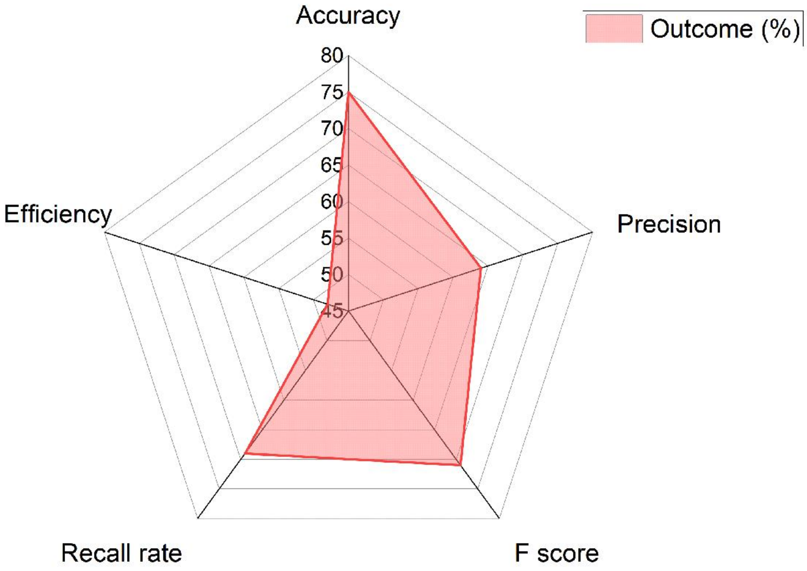

Figure 7(a). Simulation outcome analysis of the existing PCA model

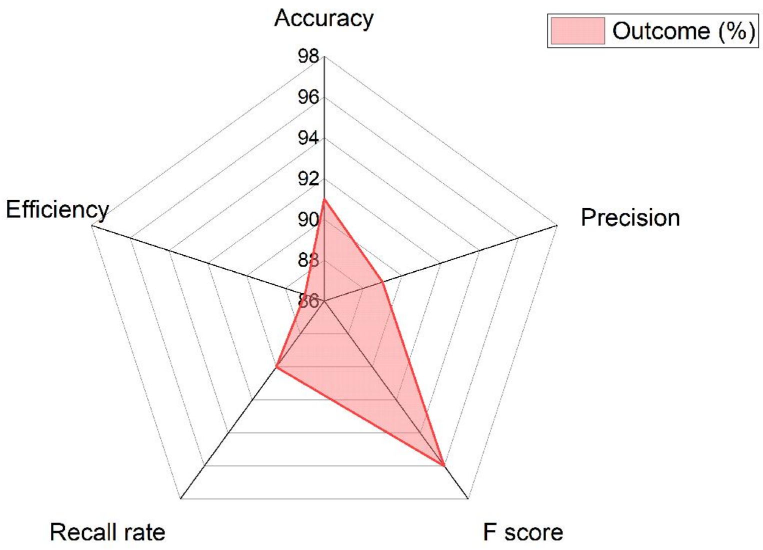

Figure 7(b). Simulation outcome analysis of the proposed SCNM-LSM system

Figures 7(a) and 7(b) show the simulation outcome analysis of the existing PCA model and the proposed SCNM-LSM system, respectively. The simulation outcomes like precision, accuracy, F score, etc., of the proposed SCNM-LSM system are analyzed, and the results are compared with the existing PCA models. The proposed SCNM-LSM system with the lighter security model exhibits lower complexity, and 6G helps to higher connectivity and performance.

The proposed SCNM-LSM system is designed, analyzed, and evaluated in this section. The simulation outcomes, such as accuracy, precision, efficiency, reliability, usability, etc., are analyzed for the proposed SCNM-LSM system, and the results are compared with the existing PCA model. The proposed SCNM-LSM system produces higher results with lower complexity and 6G technologies.

5. Conclusion and future scope

As the growth of intelligent city systems intensifies, expanding security techniques is essential to safeguard them. A smart city environment employing the lightweight security module (SCNM-LSM) is proposed in this article to support the performance in a smart city environment. IoT systems are anticipated to operate with strict minimal latency in a safe and distributed atmosphere so IoT devices may connect with and transfer time-critical data securely and safely. This study provides a new IoT authentication and access control method, which enables safe interaction between gadgets of the same IoT platform and between gadgets of the various IoT systems. The presented method is founded on a system that uses cryptography, distribution character, and fog computing to deal with delay problems. Several IoT applications may be covered by the suggested method. The security standards and an attacking pattern are also specified to evaluate our method and verify its capacity to satisfy these criteria. The next study would build a lightweight compromise mechanism to select miners depending on their trust value to avoid the large volume of power consumption required to be verified by tracking the progress.

6. Conflicts of Interest

The author of this publication declares that there is no conflict of interest associated with this publication.

References

1. Shen, X., Yu, H., Liu, X., Bin, Q., Luhach, A. K., & Saravanan, V. (2021). The optimized energy-efficient sensible edge processing model for the internet of vehicles in smart cities. *Sustainable Energy Technologies and Assessments*, *47*, 101477.

2. Hsu, C. H., Manogaran, G., Srivastava, G., & Chilamkurti, N. (2021). 6G-Enabled Network in Box (NIB) for Industrial Applications and Services. *IEEE Transactions on Industrial Informatics*, 17, 7141 – 7144.
3. Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., & Abd El-Latif, A. A. (2021). Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of Parallel and Distributed Computing*, *153*, 150-160.
4. Shakeel, P. M., Baskar, S., Fouad, H., Manogaran, G., Saravanan, V., & Xin, Q. (2021). Creating collision-free communication in IoT with 6G using multiple machine access learning collision avoidance protocol. *Mobile Networks and Applications*, *26*(3), 969-980.
5. Ramanathan, L., Swarnalatha, P., Ramani, S., Prabakaran, N., Phogat, P. S., & Rajkumar, S. (2020). Secured smart hospital cabin door knocker using internet of things (iot). *Smart healthcare analytics in IoT enabled environment*, 77-89.
6. Banupriya, S., & Kottilingam, K. (2021, May). An Analysis of Privacy Issues and Solutions in Public Blockchain (Bitcoin). In *2021 2nd International Conference for Emerging Technology (INCET)* (pp. 1-7). IEEE.
7. Srivastava, A. K., Grotjahn, R., & Ullrich, P. A. (2019, December). A Multimodel Technique for Estimating Future Changes in Extreme Precipitation. *In AGU Fall Meeting Abstracts* (Vol. 2019, pp. A51Q-2832).
8. Kumar, P. M., & Hong, C. S. (2021). Internet of things for secure surveillance for sewage wastewater treatment systems. *Environmental Research*, 111899.
9. Billah, M. F. R. M., Saoda, N., Gao, J., & Campbell, B. (2021, May). BLE Can See: A Reinforcement Learning Approach for RF-based Indoor Occupancy Detection. *In Proceedings of the 20th International Conference on Information Processing in Sensor Networks (co-located with CPS-IoT Week 2021)* (pp. 132-147).
10. Amudha, G., & Narayanasamy, P. (2018). Distributed location and trust based replica detection in wireless sensor networks. *Wireless Personal Communications,* 102(4), 3303-3321.
11. Zhang, X., Manogaran, G., & Muthu, B. (2021). IoT enabled integrated system for green energy into smart cities. *Sustainable Energy Technologies and Assessments*, *46*, 101208.
12. Manogaran, G., Baabdullah, T., Rawat, D. B., & Shakeel, P. M. (2021). AI Assisted Service Virtualization and Flow Management Framework for 6G-enabled Cloud-Software-Defined Network based IoT. *IEEE Internet of Things Journal*. 1-1.
13. Seyhan, K., Nguyen, T. N., Akleylek, S., & Cengiz, K. (2021). Lattice-based cryptosystems for the security of resource-constrained IoT devices in post-quantum world: a survey. *Cluster Computing*, 1-20.
14. Gheisari, M., Najafabadi, H. E., Alzubi, J. A., Gao, J., Wang, G., Abbasi, A. A., & Castiglione, A. (2021). OBPP: An ontology-based framework for privacy-preserving in IoT-based smart city. *Future Generation Computer Systems*, 123, 1-13.
15. Amudha, G. (2021). Dilated Transaction Access and Retrieval: Improving the Information Retrieval of Blockchain-Assimilated Internet of Things Transactions. *Wireless Personal Communications*, 1-21.
16. Nguyen, T. N., Le, V. V., Chu, S. I., Liu, B. H., & Hsu, Y. C. (2021). Secure Localization Algorithms Against Localization Attacks in Wireless Sensor Networks. *Wireless Personal Communications*, 1-26.
17. Taborda, C. H. C., Vazquez, J. G., Marin, C. E. M., & Garcia, P. G. (2020, October). Decentralized Application for the Classification of Hotels Based on IPFS and Blockchain. In *International Conference on Tourism, Technology and Systems* (pp. 12-24). Springer, Singapore.
18. Bhat, J. R., & Alqahtani, S. A. (2021). 6G Ecosystem: current status and future perspective. *IEEE Access*, *9*, 43134-43167.
19. Jamil, S. U., & Khan, M. A. (2020, December). Edge Computing Enabled Technologies for Secure 6G Smart Environment-An Overview. In *International Conference on Soft Computing and Pattern Recognition* (pp. 934-945). Springer, Cham.
20. Al-Ansi, A., Al-Ansi, A. M., Muthanna, A., Elgendy, I. A., & Koucheryavy, A. (2021). Survey on Intelligence Edge Computing in 6G: Characteristics, Challenges, Potential Use Cases, and Market Drivers. *Future Internet*, 13(5), 118.
21. Lv, Z., Qiao, L., Kumar Singh, A., & Wang, Q. (2021). AI-empowered IoT security for smart cities. *ACM Transactions on Internet Technology*, *21*(4), 1-21.
22. Ahmed, S., Hossain, M., Kaiser, M. S., Noor, M. B. T., Mahmud, M., & Chakraborty, C. (2021). Artificial Intelligence and Machine Learning for Ensuring Security in Smart Cities. In *Data-Driven Mining, Learning and Analytics for Secured Smart Cities* (pp. 23-47). Springer, Cham.
23. Das, A. K., Bera, B., Wazid, M., Jamal, S. S., & Park, Y. (2021). On the Security of a Secure and Lightweight Authentication Scheme for Next-Generation IoT Infrastructure. *IEEE Access*, *9*, 71856-71867.

24. El Tarhuni, M., & Salameh, A. I. (2021, March). Enabling Technologies and Services for 6G Networks. In *The International Conference on Intelligent Systems & Networks* (pp. 33-42). Springer, Singapore.
25. Ismagilova, E., Hughes, L., Rana, N. P., & Dwivedi, Y. K. (2020). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers*, 1-22.
26. Habibzadeh, H., Soyata, T., Kantarci, B., Boukerche, A., & Kaptan, C. (2018). Sensing, communication, and security planes: A new challenge for a smart city system design. *Computer Networks*, *144*, 163-200.
27. Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020). Enhancing cyber-physical systems with hybrid smart city cyber security architecture for the secure public data-smart network. *Future generation computer systems*, *112*, 724-737.
28. Badii, C., Bellini, P., Difino, A., & Nesi, P. (2020). Smart city IoT platform respecting GDPR privacy and security aspects. *IEEE Access*, *8*, 23601-23623.
29. Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 102468.
30. Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., & Han, Z. (2019). Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in a smart city. *IEEE Access*, *7*, 54508-54521.
31. Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal challenges with digital forensics, privacy, and security. *Security and privacy*, *1*(3), e23.