# Internet of Things based 5G Infrastructure for Securing Transportation Facilities in Smart Cities

Vijey Thayananthan
Department of Computer Science
King Abdulaziz University
Jeddah, KSA

Abdullah Algarni
Department of Computer Science
King Abdulaziz University
Jeddah, KSA

## ABSTRACT

The fifth generation (5G) is going to dominate in the smart cities where 5G provides all the facilities with maximum security and safety. Regarding transportation services, unnecessary accidents rates are increasing with cyber attacks and threats. All security issues for 5G based infrastructure will be facing many challenges such as secure transportation services which is one of the 2030 initiatives in many countries. Despite many security solutions, developing energy-efficient cryptographic algorithms are recommended to secure the future transport systems which not only improve the security but also reduce the cost. The main aim of this strategic research is to develop a secure transportation system using efficient security solutions which not only reduce the exorbitant accident rates but also increase safety system that enhances the livability of smart cities. Employing secure multi-level IoT and 5G based infrastructure used within the transportation systems will be an efficient method. In this system, appropriate applied cryptographic algorithms will be employed to improve transportation services. According to the research idea of this project, the proposed model of the future transportation system will be delivered with better security solutions. In expected results, the dynamic security solutions will be considered. They are vital requirements to minimize accidents and secure smart cities. This research will be leading us to implement an effective security solution for future transport systems. Therefore, each passenger who is driving or using driverless vehicles will be protected from the evolving attacks within the smart cities.

## General Terms

In this paper, the security of the transport service as a general term is considered. Throughout this research, security issues of IoT based 5G are considered to improve the security solutions of transportation facilities

## Keywords

Security; IoT; 5G based infrastructure; Smart cities; Transportation

## 1. INTRODUCTION

Improving secure transportation environments in popular cities is one of the 2030 visions considered by the current governments around the world. In these environments, transportation services will be improved with the efficient use of technologies providing to enhance the facilities and techniques which reduce accidental rate. Instead of improving technological capabilities, security issues should be applied to protect the current transportation system as well as the future technologies used within the smart cities. The accident may happen in many different ways such as drivers' attitude, conditions of the roads, etc. When drivers' attitudes are interrupted by these threats, the driver's behavior is affected, and it creates the uncontrollable situation during driving. Infotainments created through the vehicular communication for useful purposes and planning to continue the driving toward the destination, but wrong information is also sent to the driver by problem makers, unauthorized people, and system. Environmental conditions should be monitor accurately because drivers should prepare the driving according to the situation.

Future wireless systems such as the 5th, generation (5G) of wireless and mobile networks support to design transportation services. Here, the infrastructure of 5G is being developed to reduce the cyber threats which cause an unnecessary accident around the modern cities. Despite the basic level of the infrastructure in the transportation systems, 5G introduces many novel approaches to improve traffic monitoring facilities through intelligent transport systems [1-2].

As far as paper [3] is concerned, IoT for smart city introduced many challenges and solutions future developments including transportation, services via a Software-Defined Network (SDN), etc. Although future mobile communication influenced transportation systems, security challenges, Radio Access Network (RAN), IoT, etc. will be considered to design the secure infrastructure [4, 5]. Further, technological advances such as machine to machine communication, non-orthogonal modulation, ultra-dense cells, SDN, etc. are also applicable to control the traffic services. In this research, the following strategic approaches are essential and motivating to design an effective security solution.

Application layer handles many different transportation applications with variable factors such as time, rate, etc. through the accessing facilities. Therefore, access control which protects the application layer should be secured. Despite many security algorithms, security issues of access control should be considered to improve transportation management services. Despite these facts, threats and motivations are increasing within the transportation services because most of the vehicles are wirelessly linked. It means that cyber-attacks such as Internet-borne malware can create the most significant accident risks and financial loss within the transportation organizations. To secure transportation services, some motivations influenced by the threats should be considered. They are malicious and nonspecific (malware, hacking, etc.), deliberate and planned (terrorism, criminals, etc.), etc. As the strategic plan of 2030 vision, transportation services should be motivated by the efficient security issues of IoT based 5G infrastructure without affecting the legacy of transportation architecture. Before users or service providers consider the security issues, IoT, 5G, and legacy mobile technologies should be analyzed as in [6-8]. Although these approaches motivate to explore this selected research, all designs of these approaches provide efficient security framework which enhances the overall security solutions with low-cost computation algorithms. Although some of the 2030 objectives (improvements in the legislative environment of the transportation sector, the efficiency of transportation infrastructure and usage of public transportation) are important and recommended by the unnecessary expense but also heavy traffic and accidents. Following actions may be possible to improve the transportation policies around the transportation environments.

Another important point is that understanding the environmental disasters such as global warming and pollutions created from the heavy use of vehicles.

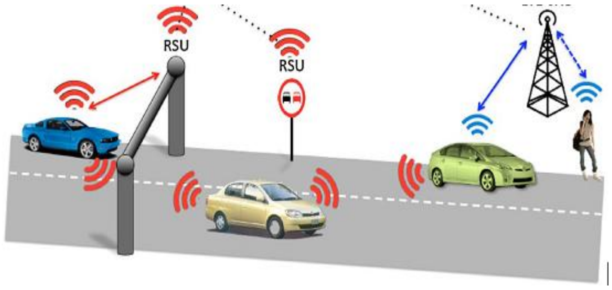

**Fig 1: Secure communication with RSU**

As shown in Figure 1, secure communication channels and links maintain the current transportation system in smart cities. However, insecure transportation services increase accident rates, fatality, cost, and unnecessary traffic.

## 1.1 Research contribution and advantages

Although many challenges and possible implementations are urgent to consider in these contributions, the research has focused on security issues and a few points related to securing the current transportation systems through the following contributions.

Studying and investigating the existing security issues for smart transportation services (RSU, traffic lights, roads, IT-based 5G network, and communication) and systems in all environmental conditions around the new and busy cities

Based on the study and investigation of current IoT scheme, the theoretical model of the secure multi-level IoT based 5G infrastructure is established. Existing or collected accident details (data) from RSU and traffic light cameras, may be used to compare the accident rate. Using conventional and new techniques used in the theoretical model, processing time such as encryption and decryption is considered to compare the security issues. In this comparison, IoT based 5G infrastructure allows us to design security solutions.

Designing possible security protocols using group-based authentication influenced by energy-efficient cryptographic algorithms and developing security solutions using suitable simulation tools for improving the overall transportation systems are considered.

Based on the theoretical model, processing time of security issues, evaluation mechanism which measures the accident rate influenced by cyber attacks within the transportation systems is analyzed.

As shown in Figure 2, IoT influences with many services which include smart transportation. Smart lights on the smart roads use framework depended on the vehicular network and communication. Here, smart road service unit (RSU) plays an essentail role in controlling the traffics. Despite many frameworks, the efficiency of V2V and V2I communication need to be analyzed with evolving threats.

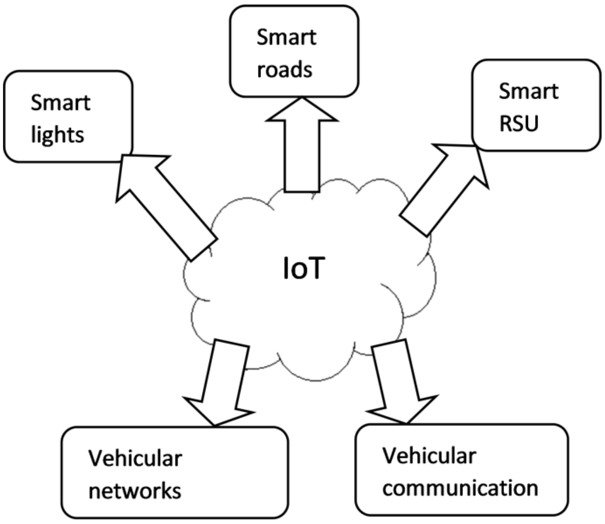

**Fig 2: Smart transportation services with IoT capabilities**

## 1.2 Organization

The rest of the paper is organized as follows. Section 2 focuses on the literature review, and related work includes current security issues and techniques, mitigation, and IoT issues based on 5G networks. Section 3 provides security issues of IoT based 5G infrastructure which include the theoretical model of the secure transportation system as a proposed model. Section 4 explains the details of securing transportation services with results and analysis. Further, the accident rate influenced by the processing time of communication services used in the future transportation system is mentioned briefly in tabulated form. In Section 5; overall conclusions are written based on the theoretical analysis and results.

# 2. LITERATURE REVIEW

According to [9], IoT-based cognitive edge framework for sharing economy services provides some benefits to improve the facilities of the smart cities. Despite many services, authors briefly considered about the transportation facilities through Blockchain concepts. In the context of transportation services, Blockchain approach reduces the accidents rates, cyber attacks of the transportation services and maintains the security issues of the other services considered in the smart cities. In their framework, the authors claimed that the integration of cognitive computing and Blockchain could reduce the scalability of IoT devices. Also, this integration provides the management facilities to handle the IoT based transportation services in the smart cities and intelligent system.

As mentioned in [10], low-cost encryption and decryption techniques provide less time complexity. As far as existing security issue “Ciphertext-policy attribute-based encryption (CP-ABE)” is concerned, designing security protocols for IoT applications used in transportation systems will increase the cost. The IoT emerges with many devices connected to the Internet which provides quick access to maintain the transport services. The everyday transportation activities are to encompass everything from IoT based services which include the security [11].

According to [12], smart cities in India need secure network grids which allow the communities to manage their daily life peacefully. Despite the overall performance of Modern Network Grids, the transportation system needs extra protection with the critical success factors. To improve the reliability of the smart cities, principal component analysis allow us to use its 16 critical factors. Figure 3 shows the possible transportation facilities with three different IoT approaches. They are basic, massive (mIoT) and vehicular (vIoT).

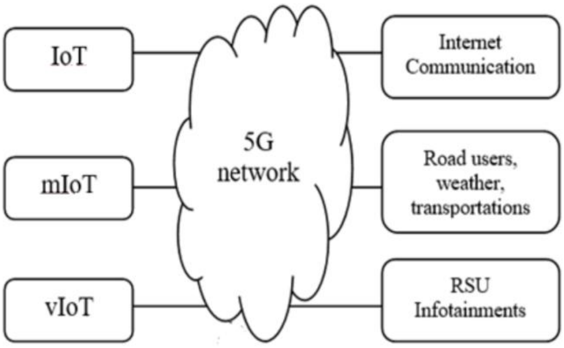

**Fig 3: Transportation facilities with IoT based 5G network**

In [13] ultra-lightweight mutual authentication approach has been proposed. Here, two bitwise operations adopted for authentication purpose which ensures low computational and storage cost. The proposed approach resists against a different type of attacks such as; DoS, tracking, replay, etc.

According to [14] authors discussed how wireless sensor nodes would protect the future of smart cities and their hierarchical security framework prevent the attacks.

As in the article [15], different communication protocols, security, privacy, etc. in managing IoT are considered as critical challenges to improving the security of massive connectivity without breaching privacy. Although IoT brings significant advantages over traditional communication technologies for smart transport and smart city applications, IoT based smart transport services and architecture have not been implemented properly yet.

Different authentications schemes explain about the future solutions of the reply attacks in the IoT environment [16]. Despite many authentication algorithms, authors have proposed a lightweight mutual authentication scheme which may help us to secure the IoT based 5G infrastructure. However, IoT security depends on end-point identity authentication and another security mechanism such as access control for transportation services [17].

Despite the many security issues considered in the current transportation services, papers [18, 19] provide relevant security concepts which may be possible to improve the future transportations services with maximum security.

According to [20, 21], green data storage expected to use in future transportation environments, is considered with the novel security solutions based on Li-Fi and quantum cryptography. Through this approach, big data used in smart transportation systems could be secured with energy-efficient security protocols. In order to improve the data traffic performance, network traffic analysis [22-24] is one of the evaluation mechanisms used for securing data communication within the smart transport of the new smart cities.

Communications protocol design for 5G vehicular networking architecture [25, 26], allows us to improve the communication services of the transportation systems linked with the internal and external signals. To standardize the future transportation systems with new facilities such as security issues, integrated infrastructure based on the interworking of heterogeneous technologies may be implemented within the modern cities.

As shown in Table 1, Vehicular Communication Functions (VCF) needs to be handled securely through the appropriate security. Here, the IoT based 5G system provides us to design secure transport.

**Table 1. Security issues**

| 5G for transportation | Related security |
|---|---|
| IoT environments for core and VCF | VCF security (for central and distributed IoT environments) |
| Software Defined Mobile Network Control (SDMC) | SDN security for VCF, transport services, SDMC, etc. |
| Mobile network based on multi-level IoT | IoT security, network slicing security |
| Transport service awareness<br>Adaptive allocation of functions, joint optimization of VCF and core | Flexible security approach, e.g., choice of cryptographic algorithms<br>Applied cryptography approach, e.g., support for flexible allocation of security functions |

According to [27, 28], the proliferation of IoT in 5G applications dominates the current communication systems. Despite many security solutions, the multi-level security model is included in the 5G network due to IoT proliferation in vehicular communication. Here, this model not only protects the data and resources but also prevents unauthorized accessing.

Papers [29, 30], provides the necessary information on security solutions on IoT to develop automated and adaptive traffic management. Regarding smart transport services, the smart city focuses on many IoT applications. Instead of securing other services in smart cities, energy management and cruise control for public transportation were focused on additional security.

Environmental based security issues such as polluted roads should create security warning to vehicle users before entering that particular road. In these situations, IoT can provide RSU to support for improving not only security issues influenced by V2V (vehicular-to-vehicular) network. As far as V2V and IoT are concerned, V2I (vehicular-to-infrastructure) is the part of the transport communication systems and services. Regarding the environmental-based traffic accidents, trust model of improving secure communication between the vehicles offers many facilities in the transportation services. These specific improvements depend on vehicle contexts, drivers' attitude, etc. reduce unnecessary accidents [31, 32].

Regarding the IoT, vIoT, and mIoT are the good features of the future IoT schemes in transportation systems. When each vehicle considered as a sensor, sending and receiving messages or communication between the vehicles need a secure sensors network connected with IoT. Therefore, creating efficient, secure vIoT using appropriate encryption and decryption algorithm will improve the future transportation services. In this research, the AES (advanced encryption standard) algorithm with IoT based 5G infrastructure is considered [33].

In transportation monitoring, large-scale high-dense IoT devices provide the necessary facilities to improve the smart traffic services. Despite the IoT devices considered as nodes in the IoT scenario, the sensor nodes need some protections because when they operate together, some nodes get wrong information which not only wastes the money but also it creates the complex situations calling all emergency such as ambulance and police. This wrong message creates extra traffic to the public within the urban cities. All warning systems incorporated with IoT devices and RSU must ensure that transportation services exchange the correct data between the vehicles, which monitor the fire detection, vehicle accident, etc. as emergency and rescue operations.

# 3. SECURITY ISSUES OF IOT

IoT based security solutions can be used to improve static and dynamic security issues in smart cities. Static security issues are useful to manage home security. In this section, dynamic security issues are considered for improving the security levels of transportation services.

## 3.1 Security Issues of IoT based 5G

The IoT based 5G schemes are growing among the services used within the transportation and smart cities. This scheme needs a secure infrastructure which allows the transport service provider to monitor and solve the transportation facilities quickly and dynamically. In the IoT based 5G network, gateway router and IoT based devices need to be protected using secure routing algorithms, protocols, and policies. Gateway routers support to provide secure filtering to the autonomous system used in the transportation services.

In the transportation system, IoT based 5G gateways provide many security issues. They are a secure boot, system security influenced by the runtime, security updates, etc.

- Secure boot protects the software involved in IoT based 5G systems through the verifications. Here, the integrity and authenticity of IoT based systems are verified.
- System security influenced by runtime allows us to protect transportation services without signature updates.
- Security updates ensure the application of the transportation services through the secure channels trusted within the smart cities.

Above concepts allow us to enhance the security levels of the potential security solutions in transportation services.

Secure transportation system considered has been employed to future IoT based 5G infrastructure which allows improving the vehicular communications. Here, the proposed system ensures that IoT based 5G infrastructure provides better security messages between the RSUs, vehicles and vulnerable road users (VRUs) than the conventional approaches. This secure information guarantees the transportation services with high quality, speed, etc. it also can be used for prioritized traffic which improves the transportation services with additional security and privacy. Although IoT based 5G services provide excellent facilities, vehicles should be able to send and receive secure communication with other vehicles/users/RSUs.

Using IoT, vehicles are communicating with each other and establishing the connection with the nearest RSU through the Internet. With secure transportation platforms developed from the IoT based 5G infrastructure, drivers can reduce the accident rate. As shown in figure 4, the proposed model represents the simple illustration of the secure transportation system. In this model, each layer provides secure transportation facilities. Details of each layer will be in the following subsection.

## 3.2 Proposed Theoretical Model

As shown in figure 4, this paper has proposed the theoretical model. In this model, layers between the smart transportation and monitoring devices increase the security levels through secure IoT based 5G infrastructure.

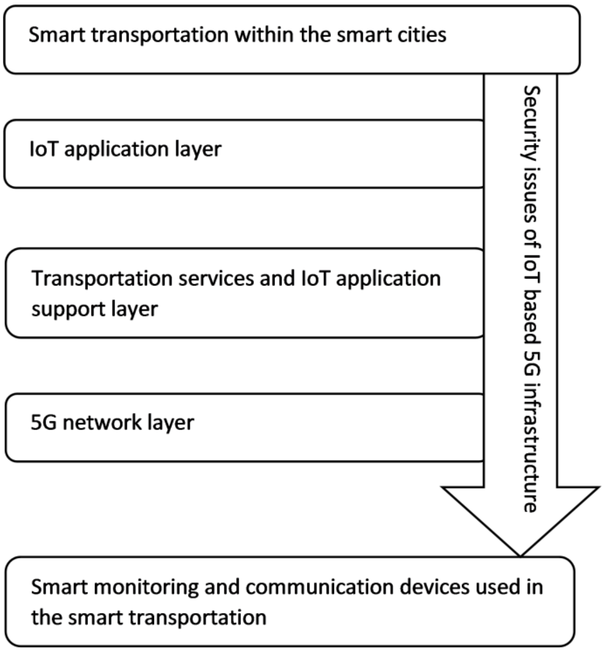
Smart transportation within the smart cities
IoT application layer
Transportation services and IoT application support layer
5G network layer
Smart monitoring and communication devices used in the smart transportation
Security issues of IoT based 5G infrastructure

**Fig 4: Theoretical model of secure multi-level IoT based 5G infrastructure**

In this theoretical model, multi-level IoT based security is considered. Security solution of multi-level IoT not only protects the data and resources but also prevents unauthorized accessing in transportation services.

The IoT application layer collects the necessary data from the smart transportation within the smart cities and handles many different transportation applications according to the external conditions. The transportation services and IoT application support layer provides a secure path between the IoT application layer and 5G network layer. Secure path supports the information exchange between multiple subnetworks within the IoT based 5G infrastructure. The 5G network layer enhances the competing requirements to improve the security level of services used in the transportation system. Here, IoT needs to be secured from possible threats; they are eavesdropping, impersonation, relay, replay attacks, etc.

## 3.3 IoT based 5G infrastructure for efficient transportation

Transportation systems in smart cities should have efficient V2V and V2I. Despite many Internet connections within the transportation systems, efficient design of IoT based 5G infrastructure will connect and handle millions of users through the 5G network. Here, communications between V2V and V2I face many challenges; they are secure traffic communication, safety regulations, handling emergencies and finding secure parking locations. Table 2 shows the current requirements as system details and technologies used in transportation services. Thus, infotainment is considered as an example of the transportation services, which is one of the problems in V2V and V2I. Further, system details can allow us to implement the IoT based 5G infrastructure for future transportation.

**Table 2. IoT based infrastructure for transportation**

| **System details** | **The technology used in infotainment transportation** | | |
|---|---|---|---|
| | ***Wi-Fi*** | ***3G*** | ***5G (LTE)*** |
| Operating frequency | 2.4 GHz - 5GHz | 850MHz | 700 to 2500MHz |
| Data rate | 54Mb/s<br>6.75Gb/s | 3Mb/s | 1Gb/s<br>500Mb/s |
| Coverage | 140m<br>100m | 5 to 30 km | 5 to 30km |
| Latency | 46ms | 100ms | 5ms |
| Power usage | Medium | high | high |

Vehicle performance is one of the measurements involved in transportation systems. Regarding the security issues, energy management and lifetime are important points to maintain secure transportation services. Especially electric vehicles should have the following security issues.

1) Enough energy to maintain all the basic electronic devices which not only provide secure services during the journey but also protect the resources fit into the vehicles.

2) Energy saving management which provides the safety warning to enjoy the entire trip and available solutions to charge the electric vehicles.

In electric vehicles, IoT devices are enriched by the sensors used around the vehicles. Energy consumption of each IoT device may vary according to the security levels. Although IoT devices work with low energy consumption, energy harvesting and saving will be possible through the IoT/EoT technologies. Also, IoT based 5G will encourage us to charge the batteries of the electric vehicles wirelessly. An IoT/IoE architecture is considered to enhance the smart city mobility and transportation services [34]. The pervasiveness of IoT devices in the inside and the outside of the vehicles create a secure communication network and wireless connections between the real and virtual worlds.

This paper examines an IoT based 5G infrastructure for securing transportation services. Hence, the performance of the 5G network should be considered for evaluating the performance of selected symmetric encryption of various algorithms. Although securing transportation services considered with best encryption algorithms is important, employing IoT based 5G enhances the security levels in the transportation service.

## 4. SECURING TRANSPORTATION

Although many security challenges considered in the current transportation services, few of the security solutions are successfully implemented within the transportation services. In the dashboard, the status of safety while the vehicle is moving can be displayed through the IoT based 5G communication channel. The IoT devices can send secure data related to transportation services to the dashboard directly. Efficient security solution can be maintained through a secure IoT network.

### 4.1 Security Solutions in Transportation

Despite many solutions implemented in the transportation services, employing secure multi-level IoT based 5G infrastructure, efficiently applied the cryptographic algorithm, and secure interfaces within the proposed theoretical model will provide necessary security solutions. Implementing such a security solution within the transportation systems will be an efficient method to improve the current and future security problems. Evolving threats and cyber attacks are the potential security issues which need dynamic solutions during the manuring. However, the security solution should increase the reliability and robustness of the future transportation system within the smart cities.

### 4.2 Results and Analysis

According to the proposed model, security issues of IoT base 5G infrastructure depends on the quick processing to facilitate the current transportation systems. Therefore, testing the time for encryption and decryption with the conventional approach is important. As shown in figure 5, IoT based 5G infrastructure performs better during the decryption rather than the encryption. In this basic testing of the encryption, when the data size is increased, time for encryption performs better.

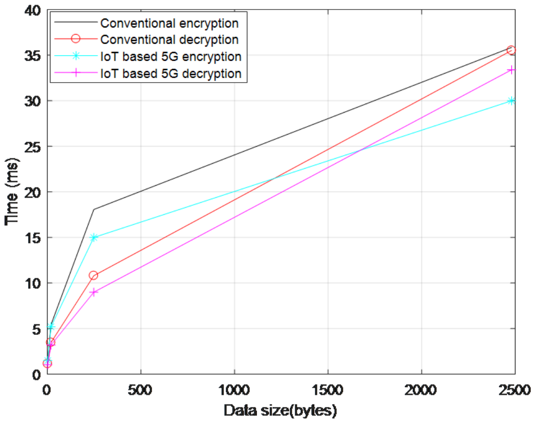

**Fig 5: Comparison of conventional and IoT based 5G infrastructure**

In these results, data size against the processing time for encryption and decryption is analyzed with existing and proposed infrastructures. Regarding the data size, different vehicle performance is one of the measurements involved in transportation systems. Although the same encryption and decryption algorithms are employed in the conventional and IoT based 5G infrastructures, the overall performance of processing time not only depends on the encryption and decryption but also secure IoT based 5G infrastructure. In the analysis of testing time, execution time is considered with the data size. Further, an efficient technique of encryption and decryption algorithms reduces the processing and execution time. Table 3 shows, the execution time of the existing encryption and decryption techniques when conventional infrastructure uses the advanced encryption schemes (AES) and data encryption standard (DES) [36]. Also, it shows that the execution time obtained during the encryption and decryption varies with the data size.

**Table 3. Execution time (in milliseconds) of selected encryption and decryption**

| Data size (in Kbytes) | Encryption | | Decryption | |
|---|---|---|---|---|
| | AES | DES | AES | DES |
| 49 | 56 | 29 | 63 | 50 |
| 59 | 38 | 33 | 58 | 42 |
| 100 | 90 | 49 | 60 | 57 |
| 247 | 112 | 47 | 76 | 72 |
| 321 | 164 | 82 | 149 | 74 |
| 694 | 210 | 144 | 142 | 120 |
| 899 | 258 | 240 | 171 | 152 |
| 963 | 208 | 250 | 164 | 157 |
| 5346 | 1237 | 1296 | 655 | 783 |
| 7310 | 1366 | 1695 | 882 | 953 |
| Average Time | 374 | 389 | 242 | 246 |
| Through put | 4.174 | 4.01 | 6.452 | 6.347 |

Although much-existing encryptions and decryption techniques are mentioned in [36 & 37], this research focuses on the AES algorithm for securing transportation facilities. Analyzing execution time allows the service providers to enhance the transportation facilities. In this time analysis, IoT based 5G infrastructure not only reduce the execution and processing time but improve the security issues in the transportation services. The throughput of the encryption or decryption scheme can be calculated from encryption time which is the processing used for converting plain text to encrypted text.

## 4.3 Accident rate monitoring

Due to the insecure transportation services and complexity of V2V communication networks, the accident rate was increasing. Further, traditional security mechanisms such as authentication may not be possible in the future IoT based 5G services. However, authentication used in the theoretical model allows us to improve the security issues in V2Is influenced by IoT. Table 4 shows the security issues of the IoT based 5G infrastructure for different approaches to transportation.

**Table 4. Security issues of IoT based 5G infrastructure**

| | **Approaches in transportation** | | |
|---|---|---|---|
| | **Infrastructure** | **Services** | **Monitoring** |
| Security parameter | Authentication | Authentication and authorization | Authentication of smart transportation |
| 5G Network | Ad hoe and grid approach | Ad hoe and communication approach | Generic and IoT communication approach |
| Description | Block all ports of the IoT based 5G channels | Collect all IP address of the devices & their services, and authenticate | Ensuring secure access and authorizing in transportation services |
| Limitations | Theoretical transportation system | Scalability based on vIoT and mIoT | Encryption and decryption time for IoT based 5G system |

In future smart cities, IoT enables us to lay some smart sensors on the roads which provides facilities as smart services in smart transportation. These sensors not only encourage future autonomous vehicles but also secure the public transportation services within the smart cities. Equipping vehicles, roads, other objects and services between these need flexible, energy-efficient and secure sensor network and communication. Thus, the intelligent approach of the transportation services will not only protect traffic accidents but also improve traffic congestion.

# 5. CONCLUSIONS AND FUTURE WORK

We have studied the IoT based 5G concept considered in the transportation of smart cities a multi-layer framework that addresses security issues. In this research, the current and future security problems within the transportation services have been explored. Hence, this research will be leading us to implement an effective security solution for the transport systems. As an early solution, this paper introduced the theoretical model which will not only secure the transportation services but also it will protect the smart city. According to the result mentioned in subsection 4.2, IoT based 5G architecture has reached a quick response time which indicates that IoT based 5G architecture can provide better security performance than the conventional design. As far as this theoretical model is concerned, whenever or wherever vehicles move within the smart cities, it will provide maximum protection from the evolving attacks. In the future work, as given in [35], IoT based 5G-enabled hierarchical architecture can be developed using the proposed theoretical model for improving the security issues of transportation facilities through a software-defined intelligent transportation system.

## 6. ACKNOWLEDGMENTS

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks, DSR technical and financial support.

## 7. REFERENCES

[1] Menouar, Hamid, Ismail Guvenc, Kemal Akkaya, A. Selcuk Uluagac, Abdullah Kadri, and Adem Tuncer. "UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges." IEEE Communications Magazine 55, no. 3 (2017): 22-28.

[2] Camacho, Fernando, César Cárdenas, and David Muñoz. "Emerging technologies and research challenges for intelligent transportation systems: 5G, HetNets, and SDN." International Journal of Interactive Design and Manufacturing (IJIDeM) (2017): 1-9.

[3] Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of the Internet of Things for smart home: Challenges and solutions." Journal of Cleaner Production 140 (2017): 1454-1464.

[4] Sfar, Arabia Riahi, Enrico Natalizio, Yacine Challal, and Zied Chtourou. "A Roadmap for Security Challenges in the Internet of Things." Digital Communications and Networks (2017).

[5] Samaila, Musa G., Miguel Neto, Diogo AB Fernandes, Mário M. Freire, and Pedro RM Inácio. "Security Challenges of the Internet of Things." In Beyond the Internet of Things, Springer International Publishing, 2017, pp. 53-82.

[6] Gavrilovska, Liljana, Valentin Rakovic, and Vladimir Atanasovski. "Visions towards 5G: Technical requirements and potential enablers." Wireless Personal Communications 87, no. 3 (2016): 731-757.

[7] Amaral, Leonardo Albernaz, Everton de Matos, Ramão Tiago Tiburski, Fabiano Hessel, Willian Tessaro Lunardi, and Sabrina Marczak. "Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G." In

[8] Internet of Things (IoT) in 5G Mobile Technologies, Springer International Publishing, 2016, pp. 333-367.

[9] Rahman, Md Abdur, Md Mamunur Rashid, M. Shamim Hossain, Elham Hassanain, Mohammed F. Alhamid, and Mohsen Guizani. "Blockchain and IoT-based Cognitive Edge Framework for Sharing Economy Services in a Smart City." IEEE Access (2019).

[10] Jo, Minho, Vanga Odelu, Ashok Kumar Das, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. "Expressive CP-ABE Scheme for Mobile Devices in IoT satisfying Constant-size Keys and Ciphertexts." IEEE Access (2017).

[11] Mozzaquatro, Bruno A., Ricardo Jardim-Goncalves, and Carlos Agostinho. "Towards a reference ontology for security in the Internet of Things." In Measurements & Networking (M&N), 2015 IEEE International Workshop on, IEEE, 2015, pp. 1-6.

[12] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. "Critical Success Factors to Establish 5G Network in Smart Cities: Inputs for Security and Privacy." Journal of Global Information Management (JGIM) 25, no. 2 (2017): 15-37.

[13] Tewari, Aakanksha, and B. B. Gupta. "Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags." The Journal of Supercomputing (2016): 1-18.

[14] Wu, Jun, Kaoru Ota, Mianxiong Dong, and Chunxiao Li. "A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities." IEEE Access 4 (2016): 416-424.

[15] Sukant K. Mohapatra, Jay N. Bhuyan, Pankaj Asundi, and Anand Singh A Solution Framework For Managing Internet Of Things, A Solution Framework For Managing Internet Of Things, International Journal of Computer Networks & Communications (IJCNC) Vol.8, No.6, November 2016.

[16] Jan, Mian Ahmad, Fazlullah Khan, Muhammad Alam, and Muhammad Usman. "A payload-based mutual authentication scheme for the Internet of Things." Future Generation Computer Systems (2017).

[17] Kim, Jin Ho. "A Survey of IoT Security: Risks, Requirements, Trends, and Key Technologies." Journal of Industrial Integration and Management (2017): 1750008.

[18] Vijey Thayananthan, Ahmed Alzahrani, and Muhammad Shuaib Qureshi, "Efficient techniques for key management and quantum cryptography in RFID networks," SECURITY AND COMMUNICATION NETWORKS, USA, 2014.

[19] Riaz Ahmed Shaikh and Vijey Thayananthan," Hop-by-Hop Trust Evaluation Algorithm for Identity Anonymous Wireless Sensor Networks," SECURITY AND COMMUNICATION NETWORKS, USA, 2014.

[20] Vijey Thayananthan, Omar Abdul Kader, Kamal Jambi, and Alwi Bamhdi, “Analysis of Cybersecurity based on Li-Fi in green data storage and cloud computing for industrial networking,” IEEE CSCloud/SSC 2017.

[21] Vijey Thayananthan and Aiiad Albeshri, “Big data security issues based on quantum cryptography and privacy with authentication for the mobile data center ” 2nd International Symposium on Big Data and Cloud Computing (ISBCC’15) Elsevier, India, 2015.

[22] Alam, Furqan, Vijey Thayananthan, and Iyad Katib. "Analysis of round-robin load-balancing algorithm with adaptive and predictive approaches." In Control (CONTROL), 2016 UKACC 11th International Conference on, IEEE, 2016, pp. 1-7.

[23] AA Hadi, OA Abdulkader, S Al-ardhi, V Thayananthan, “Analytical Model of Enhancing Traffic Performance based on Weighted Nodes,” IEEE “2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation, UK 2016, University of Cambridge”. DOI 10.1109/UKSim.2016.28, pp. 337-342.

[24] Ejaz, Waleed, and Alagan Anpalagan. Internet of Things for Smart Cities: Technologies, Big Data, and Security. Springer, 2019.

[25] Katsaros, Konstantinos, and Mehrdad Dianati. "A Conceptual 5G Vehicular Networking Architecture." In 5G Mobile Communications, Springer International Publishing, 2017, pp. 595-623.

[26] Chiti, Francesco, Romano Fantacci, Dino Giuli, Federica Paganelli, and Giovanni Rigazzi. "Communications Protocol Design for 5G Vehicular Networks." In 5G Mobile Communications, Springer International Publishing, 2017, pp. 625-649.

[27] Salman, Ola, Ayman Kayssi, Ali Chehab, and Imad Elhajj. "Multi-level security for the 5G/IoT ubiquitous network." In Fog and Mobile Edge Computing (FMEC), 2017 Second International Conference on, pp. 188-193. IEEE, 2017.

[28] D'Angelo, Gabriele, Stefano Ferretti, and Vittorio Ghini. "Multi-level simulation of the Internet of Things on smart territories." Simulation Modelling Practice and Theory 73 (2017): 3-21.

[29] Saha, Himadri Nath, Supratim Auddy, Avimita Chatterjee, Subrata Pal, Susmit Sarkar, Rocky Singh, Amrendra Kumar Singh et al. "IoT solutions for smart cities." In Industrial Automation and Electromechanical Engineering Conference (IEMECON), 2017 8th Annual, pp. 74-80. IEEE, 2017.

[30] Suo H et al. (2012) Security on the internet of things: a review. In: International conference on computer science and electronics engineering (ICCSEE '12), vol. 3, pp 648–651 IEEE, 23 Mar 2012.

[31] V Thayananthan, RA Shaikh, "Contextual Risk-based Decision Modeling for Vehicular Networks," International Journal of Computer Network & Information Security 8 (9), 2016.

[32] Hasrouny, Hamssa, Carole Bassil, Abed Ellatif Samhat, and Anis Laouiti. "Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET." In Vehicular Ad-Hoc Networks for Smart Cities, pp. 71-83. Springer, Singapore, 2017.

[33] Kaufman, C., Perlman, R., Speciner, M.: Network Security: Private Communication in a Public World. Prentice Hall Press (2002).

[34] Badii, Claudio, Pierfrancesco Bellini, Angelo Difino, and Paolo Nesi. "Sii-Mobility: An IoT/IoE architecture to enhance smart city mobility and transportation services." Sensors 19, no. 1 (2019).

[35] Din, Sadia, Anand Paul, and Abdul Rehman. "5G-enabled Hierarchical architecture for the software-defined intelligent transportation system." Computer Networks 150 (2019): 81-89.

[36] Elminaam, Diaa Salama Abdul, Hatem Mohamed Abdul Kader, and Mohie Mohamed Hadhoud. "Performance evaluation of symmetric encryption algorithms." *IJCSNS International Journal of Computer Science and Network Security* 8, no. 12 (2008): 280-286.

[37] Wang, Zhu, Yan Yao, Xiaojun Tong, Qinghua Luo, and Xiangyu Chen. "Dynamically Reconfigurable Encryption and Decryption System Design for the Internet of Things Information Security." *Sensors* 19, no. 1 (2019): 143.