International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

Privacy preserving of remote data using iot and encryption for traffic signal optimization

Dr.Henry
Under Graduate Student
Computer Department
JSPM's Rajarshi Shahu College of Engineering
Pune, India

ABSTRACT

Traffic congestion is an ever increasing problem in towns and cities all over the world. Local authorities must continually work to maximize the efficiency of their road networks and to minimize any disruptions caused by accidents and events. In this project we proposed a model for an Adaptive Road Traffic Control system which provides a technique for controlling the traffic in highway network using signals that are automatically controlled by detectors. It coordinates the operation of the traffic signals in entire area (city or town) to give good progression to vehicles through the road network. Whilst coordinating all the signals, the signal timing fluctuates throughout the day, responding intelligently and continuously as per the changes in traffic flow. It removes the dependence of less sophisticated systems on signal plans, which have to be expensively updated. So we Design such system in which vehicle count is collect from sensor and then apply encryption and send to the Control system where all information is get decrypted. All processing is done and send time information to signal system.

Keywords—Security,Encryption, Traffic Congetion, Network, Sensor.

I. INTRODUCTION

Security is major issue in Cloud Computing. Every year 30% data is leak or lost while transferring over the network. Also in the modern era, one of the most exigent issues that our society is facing is vehicular congestion increasing at an exponential rate. Let us take the case study of Pune, one of the major city of Maharashtra, India. Pune has the largest number of vehicles per capita in central Maharashtra. According to Pune RTO Undertaking, more than 45,000 vehicles were registered this year in Pimpri-Chinchwad and Pune making the total count of more than 8 lakhs vehicles on the road. While the number of vehicles are increasing at a fast pace, the infrastructure in the city is not being able to match this growth. Traffic jams during rush hours are becoming a routine affair, especially in the internal sectors where long queues of vehicles can be seen stranded. Therefore, we have tried to address the problem with the help of our project wherein the focus would be to minimize the vehicular congestion. We have achieved this with the help of Sensors on the live field and eventually to deploy a feedback mechanism in the working of the traffic lights where the density of the traffic would also be factored in the decision making process. In the last years, the development of intelligent transport systems (ITS) has increased but they must be efficient to be applicable for the optimization of real-time traffic. For example, optimization tools that use multiple traffic simulations have been defined and also optimization tools based on hybrid traffic flow models are introduced. The traffic density estimation can also be achieved using Cells Transmission Model (CTM). In particular, the CTM-UT is suitable to represent: i) complex flow interactions between neighboring turning movements when entering in the channelized lanes upstream intersection; ii) conflict among crossing flows at complex signalized or un-signalized intersection with the capacity determination for minor flows. We divide the route into specific number of cells, these cells will serve as a method for estimation of traffic density.

In the modern age where technology has become a major part of most of the people due to the conveniences it brings, it also brings with it a possible breach of privacy or confidentiality, such as messages between two parties being intercepted and abused by an outsider. This necessitate a need of an adequate and effective cryptographic

algorithms to secure these kind of data transmissions from an unauthorized user revealing. Although the act of data encryption can be used by private individuals, national security is still the predominant motive for data, encryption. To successfully design & implement security we need to be a step ahead or perhaps think on the same line as the cyber criminals do. Preserving secrecy against outsiders is an issue that has been prevalent in the past, and this is where cryptography plays a part in helping to keep exchanges private messages. Cryptography covers a wide area of techniques, including those such as microdots, merging words with images, and other ingenious ways to hide information from being intercepted by outside parties. It is the process of converting messages from a comprehensive form into an incomprehensive one at one end and which reverses the process at the other end so that the message is unreadable by interceptors or eavesdropper without the secret knowledge. Though in modern times, cryptography is most known or associated with scrambling plaintext, which is the plain message that is going to be sent in transit into cipher text. Of the various ciphers, block ciphers are the type often used in data encryption.

II. RELATED WORK

Congestion in traffic is a serious problem nowadays. Although it seems to pervade everywhere, mega cities are the ones most affected by it. The development of intelligent transport systems is inevitable but they must be efficient to be applicable for the optimization of real-time traffic.

III. PROPOSED SYSTEM

The proposed system is as follows

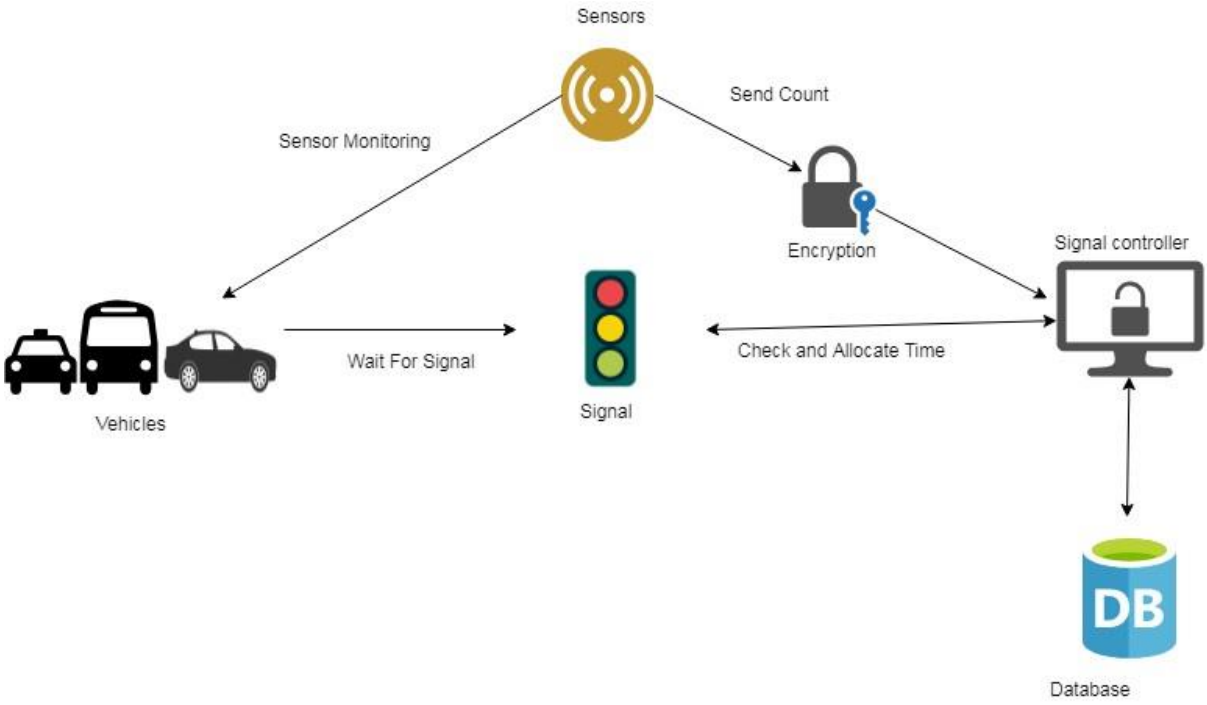

Fig.1 System Architecture

In above architecture we display signal system which is working on the basis of Signal control system. Sensors play vital role in our application. From every direction sensor collect data (i.e. Vehicle Count) and the using Blowfish algorithm all data get encrypted and send to Signal control system. Control system decrypt data received form sensor and process it. Control system finally calculate time for every direction of road side and pass back to signal system.

Blowfish Algorithm

Blowfish is a keyed, symmetric cryptographic block cipher designed by Bruce Schneier in 1993 and placed in the public domain. Blowfish is included in a large number of cipher suites and encryption products, including SplashID. Blowfish's security has been extensively tested and proven. As a public domain cipher, Blowfish has been subject to a significant amount of cryptanalysis, and full Blowfish encryption has never been broken. Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like SplashID that functions on a wide variety of processors found in mobile phones as well as in notebook and desktop computers. Schneier designed Blowfish as a general-purpose algorithm, intended as a replacement for the aging DES and free of the problems associated with other algorithms. Notable features of the design include key-dependent Sboxes and a highly complex key schedule.

IV. CONCLUSION AND FUTURE SCOPE

Urban signal timing is a non-convex problem and finding an optimal solution for not very small and simple networks may take long time, wherever possible. For this reason, we propose the surrogate method to solve this problem. A classification method of the traffic lights is proposed to simplify the problem reducing the complexity of the network. Given the sub-network a Surrogate Method is applied to solve the Traffic Signal Synchronization problem. This decomposition gives comforting results, and other indexes for the imposition are under study. This work is at the beginning and we are studying the possibility to introduce particular characteristics of the routes in the decomposition phase.

V. ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, I wish to thank all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. S. B. Javheri for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Adacher L., Cassandras C.G., Lot size optimization i, manufacturing systems: the surrogate method.International Journal of Production Economics,Volume 155, September 2014, Pages 418-426, ISSN 0925-5273,

[2] Adacher L, A global optimization approach to solve the traffic signal synchronization problem . Procedia: Social Behavioral Sciences,2012.

[3] Adacher L. and Cipriani E., A surrogate approach for the global optimization of signal settings and traffic assignment problem. IntelligentTransportation Systems (ITSC), 2010 13th International IEEE Conferenceon , vol., no., pp.60,65, 19-22 Sept. 2010.

[4] Adacher L., Cipriani E., Gemma A., The global optimization of signal settings and traffic assignment combined problem: a comparison between algorithms. Advances in Transportation Studies.Issue 36, pp35-48, 2015.

[5] L. Adacher and C. Meloni, An agent based approach to the real time air traffic control, IFAC 2005 Traffic Control, vol. 16, no. 1, pp. 2043 2043,2005.

[6] L Adacher, A Gemma, Gabriele Oliva, Decentralized Spatial Decomposition for Traffic Signal Synchronization, Transportation Research Procedia,Volume 3, 2014, Pages 992-1001, ISSN 2352-1465.

[7] L. Adacher, M. Tiriolo, A new node model based on CTM-UT with capacity determination, Transportation Research Procedia, Volume 10,2015, Pages 21 - 30, 2015.