Atomic Spectroscopy

Article

Enhanced Cryptographic Solutions To Protect Messages During Communication In Vehicular Cloud Computing

A. SHEELA RINI, Dr C. MEENA
Research Scholar, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore
Computer Center Incharge, Avinashilingam Institute for Home Science & Higher Education for Women, Coimbatore,.

ABSTRACT: VCC or Vehicular Cloud Computing is a network that combines VANET (Vehicular Adhoc NETwork) and Cloud Computing principles along with wireless concepts to provide services related to safe transportation and traffic management. One important concern during VCC communication is the security of the messages transmitted. In this research work, hybrid cryptographic algorithms that combines layered and combination methods are proposed. The methodology works in two stages. In the first stage, 2 layered and 2 combination algorithms are designed, from which, the best performing method is selected. The selected methods are then hybridized to protect the VCC messages. Experimental results showed that the proposed hybrid cryptographic method is efficient when compared to the existing algorithms.

Keywords: Hybrid Cryptography, Layered Cryptography, Combination Cryptography, Vehicular Cloud Computing, Secure Communication, Message Safety.

INTRODUCTION

The technological breakthroughs in software, hardware and communication has evolved in different types of networks, specially constructed to suit different environments. One such network is VANET (Vehicular Adhoc NETwork). A VANET is a network that uses a set of moving vehicles to form a wireless network that can apply Information Communication Technology (ICT) to provide efficient services related to transportation and traffic management (Kugali and Kadadevar, 2020). The VANET consists of various components to help vehicles to communicate with each other. These components include, Road Side Units (RSUs), GPS (Global Positioning System) devices, cameras, radio transceiver, sensors, moving vehicles and the cloud servers. The huge amount of data sensed from these components need huge storage units along with fast computing devices and methods. As this requirement is difficult to handle by VANET components, VCC (Vehicular Cloud Computing) was introduced. This new technology is a part of Intelligent Transportation system and is designed as a hybrid system that combines the advantages of cloud computing with VANET (Antonio *et al.*, 2020). Currently, VCC has received more attention as it can provide efficient solutions in areas related to vehicle and road safety, improve traffic management, provide efficient entertainment services and provide better utilization of traffic signals. VCC helps to improve communication between vehicles and work to provide a safe and efficient travelling environment.

The main objective of VCC, as mentioned earlier, is to create a safe and efficient travelling environment. However, VCC has several security holes that make the network vulnerable against attacks. Examples of such attacks include jamming (that prevent communication between vehicles), forging or falsifying fake hazard warning messages, message hampering (dropping or altering messages) and privacy violations. Previously, in order to ensure secure vehicular communication, a machine learning-based method was proposed to detect hacked vehicles. However, due to the high mobility characteristics of the vehicles, VCC also faces serious security issues, like authentication, message confidentiality, safety of messages communicated and secure location information.

This paper, focuses on techniques that ensures safety of messages communicated using cryptography. Cryptography is defined as secure communication techniques that allow only the source and the intended destination vehicles to access and view the message content. These algorithms transfer the messages into a hard to decipher form, which can be converted to its original state only by the intended destination vehicles. Cryptographic algorithms have envisaged huge advancements in the past few decades. Initially, the advancements were in the form of mono-alphabetic ciphers, polyalphabetic substitution ciphers, transposition ciphers and block ciphers (Aung *et al.*, 2019). Later on, more advancements were implemented using sophisticated algorithms like AES (Advanced Encryption Standard), DES (Data Encryption Standard), RSA (Rivest–Shamir–Adleman) and SHA (Secure Hash Algorithm). Each of these algorithms have their own merits and demerits.

Recent researches are focused on developing hybrid cryptographic algorithms that can combine their advantages in order to improve its efficiency in protecting messages being transmitted over VCC and thus construct a safe communication environment (Kumar *et al.*, 2021). This work, motivated by the success of hybrid algorithms, also proposes an enhanced 2-level hybrid algorithm that combines the advantages of multiple cryptographic algorithms to provide both vehicle level and message level security. The rest of the paper is organized as follows. Section 2 provides the methodology behind the design of hybrid cryptography algorithm. The algorithms used are BlowFish, RSA, 3DES, AES and MD5 (Message Digest-5).

Section 3 analyses the performance of the proposed hybrid cryptographic algorithms and compare their results with the existing algorithms. Section 4 concludes the work with future research directions.

METHODOLOGY

According to Ekwonwune and Enyinnaya (2020), a hybrid algorithm refers to the usage of two or more cryptographic algorithms with the aim of creating a robust VCC model that can protect messages transmitted. In order to construct a secure communication VCC model, this work proposes a 2-level Hybrid Cryptographic (2-HC) system, where the first level focuses on providing vehicle level security, while second level focuses on message level security.

In general, safety messages are broadcasted every 100 to 300 milliseconds (Liu *et al.*, 2020). At the receiving end, the sender's identity is verified for authenticity. However, as VCC is a high speed network, where even a small delay can cause catastrophic situations, the authentication has to be done in a fast manner. In this paper, to solve this issue, the first level of 2-HC system is focused on correctly identifying valid vehicles by making sure that only registered user's access data. That is, the method allows only vehicles which are part of clusters involved in communication, to access the messages. The rest of the vehicles (that is, public) cannot perform any operation on them. This is implemented using a method that is similar to login, password system commonly used in networks. Here, the vehicle's license plate along with driver's license is used as password to get access to cloud messages.

The second level of 2-HC system focuses on message level security where multiple cryptographic algorithms are used to protect the messages send using cloud systems. In practice, two types of methodology are used to combine cryptographic algorithms (Chakraborty *et al.*, 2020). They are,

Layered Cryptographic Algorithms : These algorithms provide the ability to use different encryption algorithms on different portions of a message. The advantage of this methodology is accessing a single part would not reveal the whole message.

Combination Cryptographic Algorithms : These algorithms apply multiple encryption algorithms on the whole message, thus making it difficult to hack the message as the hacker has to handle two or more encryption algorithms.

This work designs 2 layered and 2 combination algorithms, from which the efficient ones are selected and fused to form a hybrid algorithm. Thus, the proposed hybrid algorithm combines layered and combined algorithm.

The design of layered algorithm uses two popularly used cryptographic method, namely, Blowfish (B) and DES (D). This algorithms performs cryptography in two steps (Figure 1). The first step splits the message into two blocks. While the second method applies, different cryptographic algorithm to each block. During the design of layered algorithms, the order of applying the cryptographic algorithms is critical. In this work, two layered algorithms are proposed, where the first method applies Blowfish to encrypt block 1 and DES to encrypt block 2. The second method, on the other hand, applies DES to encrypt block 1 and blowfish to encrypt block 2. The methods respectively are termed as LC_B+D algorithm and LC_D+B algorithm.

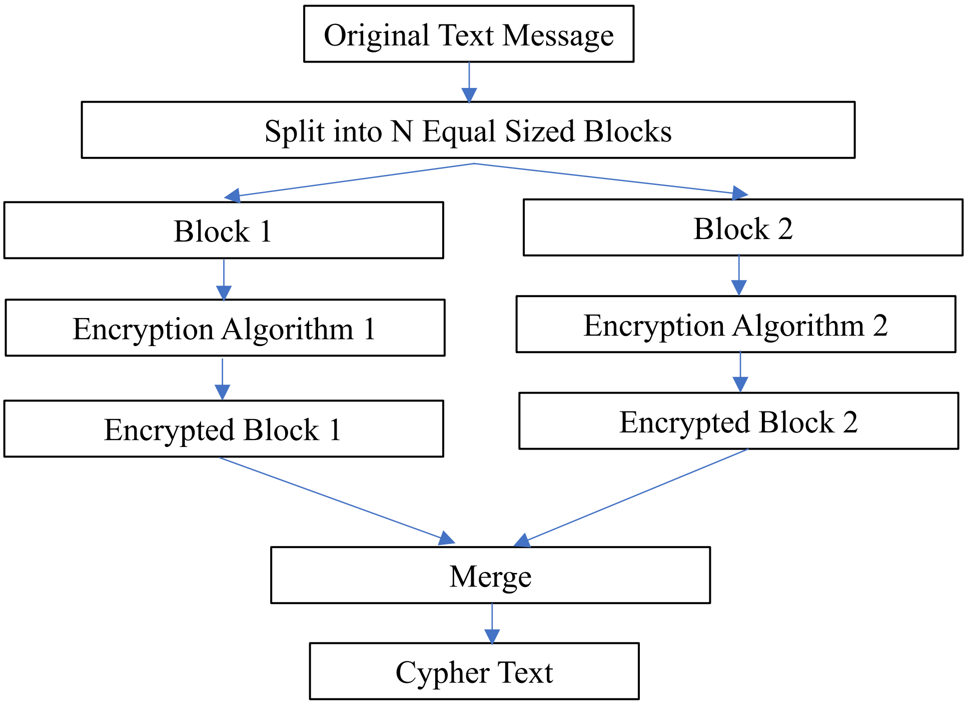


Figure 1 : Layered Cryptographic Algorithm

The design of combination cryptographic uses RSA and AES algorithms. As with layered algorithm, two methods, which differ in the order of applying the RSA and AES algorithms, are proposed. The methods respectively are termed as CC_R+A (RSA is applied first, followed by the application of AES) and CC_A+R (AES is applied first, followed by RSA). The steps involved are presented in Figure 2.

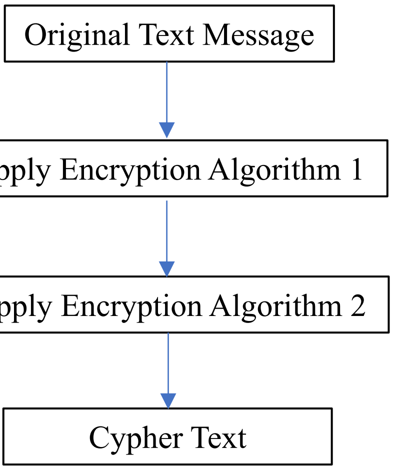
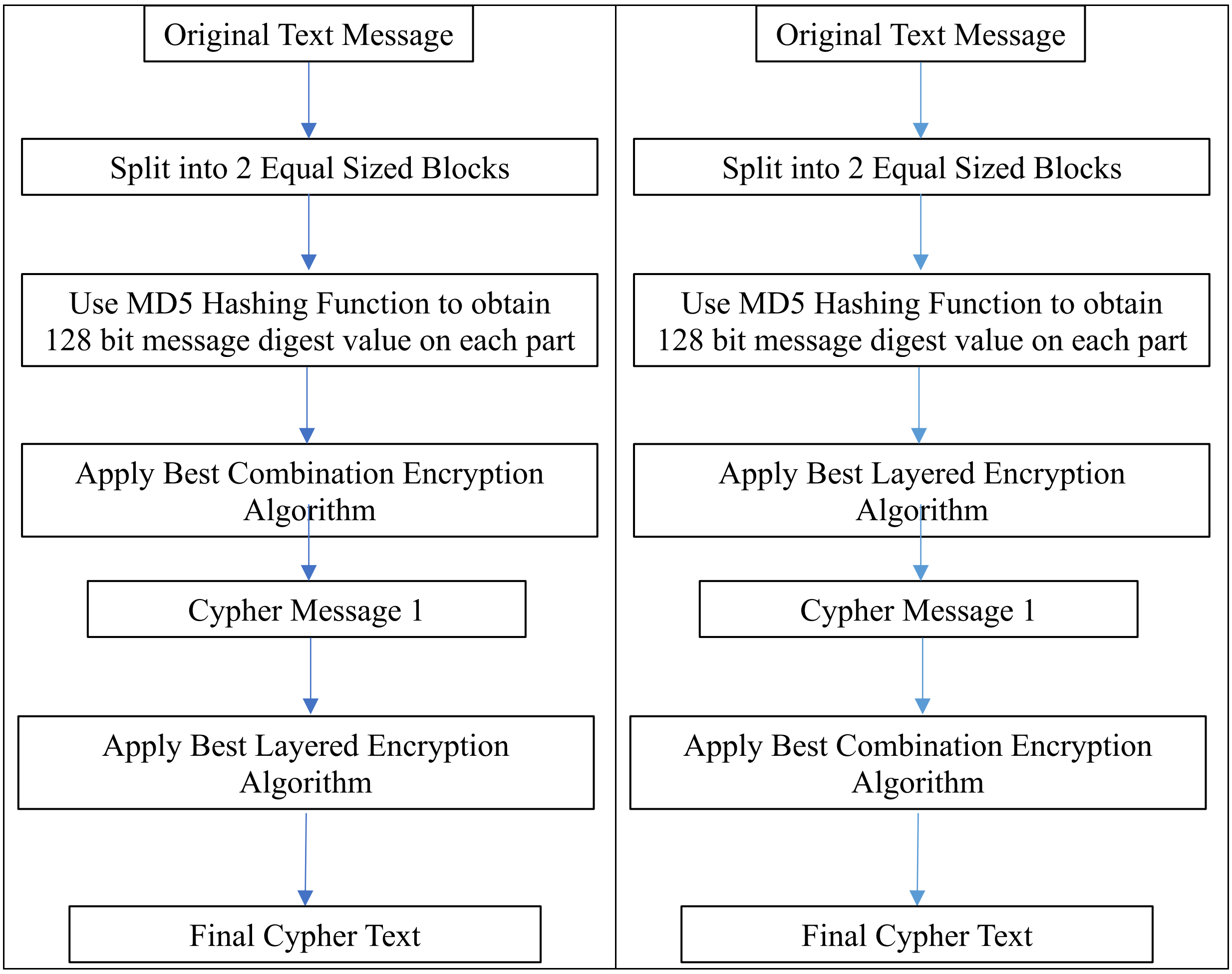


Figure 2 : Combination Cryptographic Algorithm

Performance evaluation of the above four designs showed that both layered and combination methods improve message security and motivated by these results, hybrid algorithms that joined layered and combination methods are proposed. This algorithm is termed as Hybrid cryptographic algorithms. Again, two types of hybridization are designed, which differed in the order of using layered and combination methods. The first applies layered algorithm followed by combination algorithm and is termed as HLC Cryptographic Algorithm. The second applies combination first followed by layered and is termed as HCL Cryptographic Algorithm. The steps involved are respectively shown in Figures 3a and 3b. In both the algorithms, the MD5 algorithm is included to improve integrity.


Original Text Message
Split into 2 Equal Sized Blocks
Use MD5 Hashing Function to obtain 128 bit message digest value on each part
Apply Best Combination Encryption Algorithm
Cypher Message 1
Apply Best Layered Encryption Algorithm
Final Cypher Text
Original Text Message
Split into 2 Equal Sized Blocks
Use MD5 Hashing Function to obtain 128 bit message digest value on each part
Apply Best Layered Encryption Algorithm
Cypher Message 1
Apply Best Combination Encryption Algorithm
Final Cypher Text

(a) HCL	(b) HLC

Figure 3 : Steps in Hybrid Cryptographic Algorithm

Both the fusion algorithms, HCL and HLC, combines the advantages of layered and combination cryptography, thus providing a secure message transmission environment.

EXPERIMENTAL RESULTS

Several experiments were conducted to evaluate the performance of the proposed algorithms. Computation overhead of encryption and decryption algorithms, measured in seconds, were used as performance measure. The coding scheme used is presented in Table 1. Figures 1a,b to 3a,b show the encryption and decryption time taken by the layered, combination and proposed hybrid algorithms respectively..

TABLE 1 : CODING SCHEME

Code	Description
B	BlowFish Algorithm
D	3DES Algorithm
A	AES Algorithm
R	RSA Algorithm
LC_B+D	Layered Cryptographic Algorithm Using Blowfish and DES
LC_D+B	Layered Cryptographic Algorithm Using DES and Blowfish
CC_A+R	Combination Cryptographic Algorithm Using AES and RSA
CC_R+A	Combination Cryptographic Algorithm Using RSA and AES
HLC	Hybrid Layered and Combination Cryptographic Algorithm
HCL	Hybrid Combination and Layered Cryptographic Algorithm

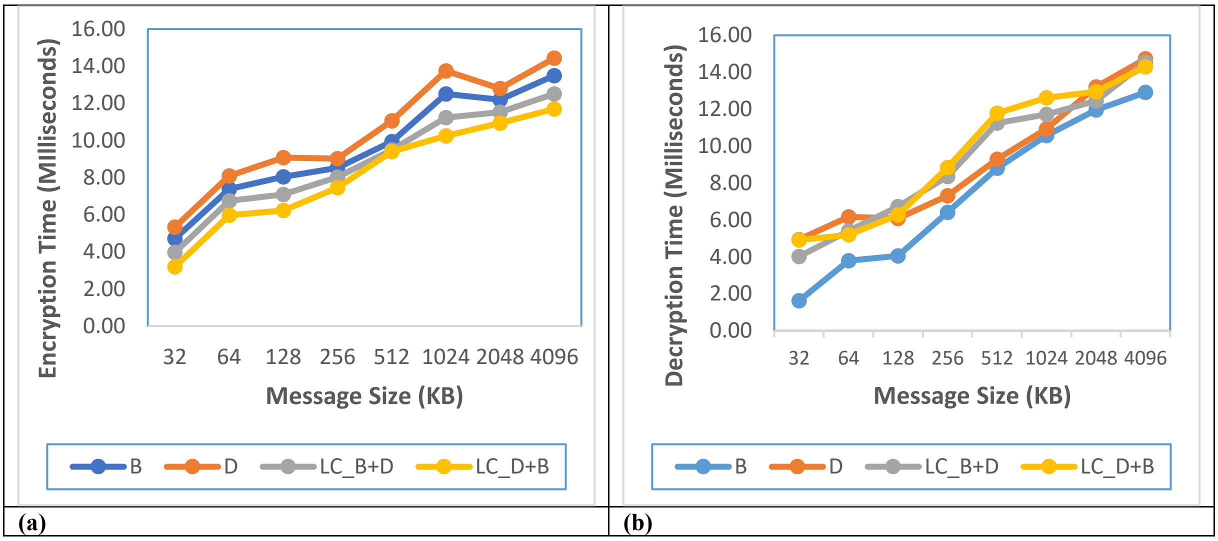
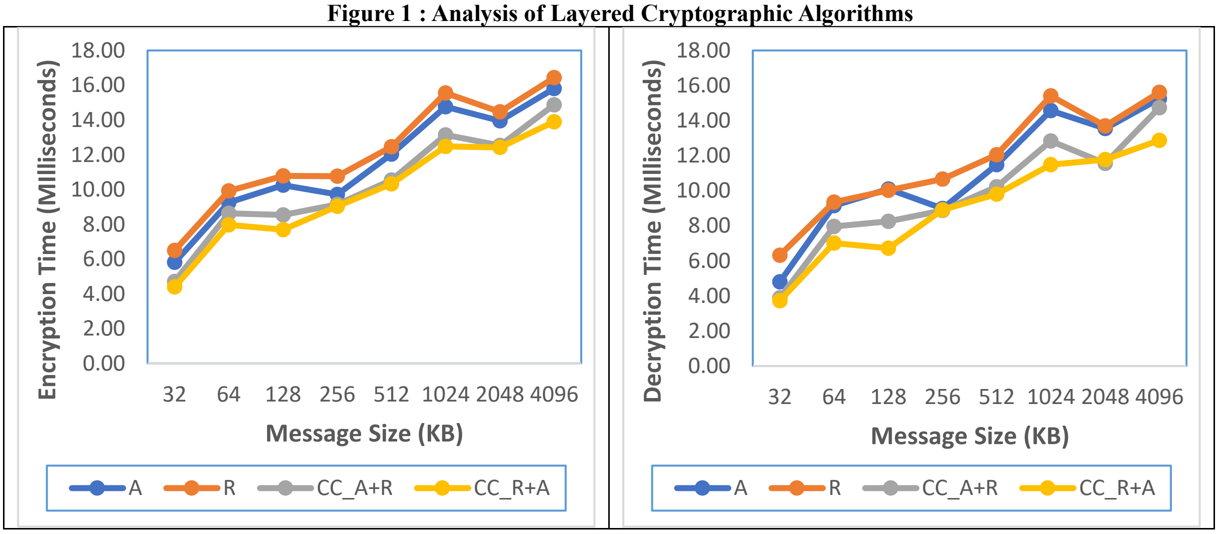
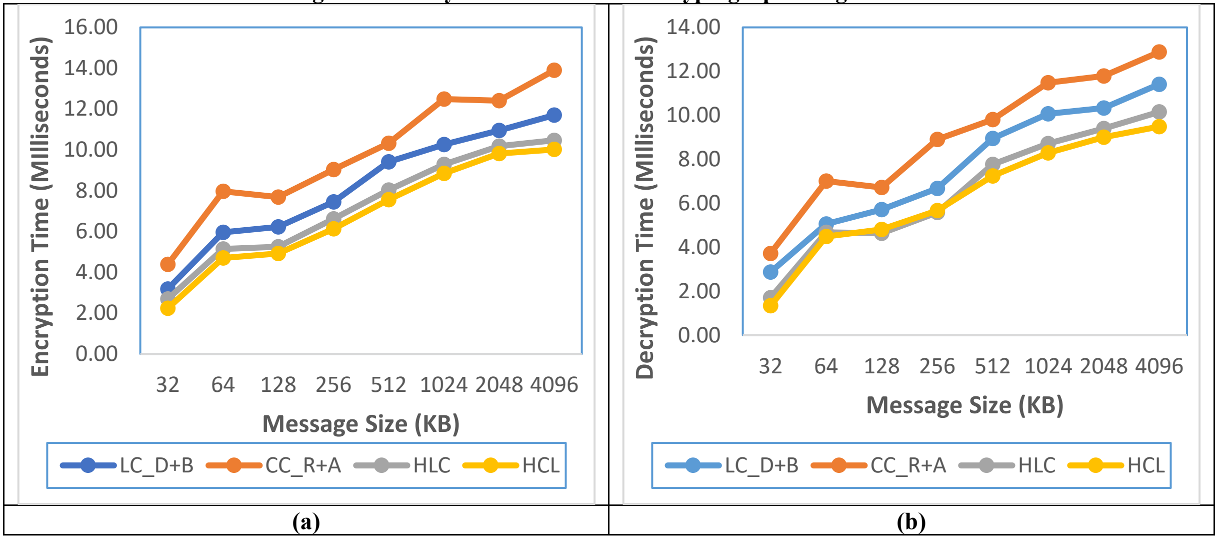


Figure 1 : Analysis of Layered Cryptographic Algorithms



(a) **(b)**

Figure 2 : Analysis of Combination Cryptographic Algorithms



(a) **(b)**

Figure 3 : Analysis of Hybrid Cryptographic Algorithms

From the results, it is understood that the layered algorithms are faster to produce encrypted and decrypted message when compared with combination algorithms. Among the layered algorithms, the algorithm that applied D first and then B had less time complexity. Among the combination algorithms, the algorithm that applied R first followed by A produced results in a fast manner. However, maximum efficiency was produced by the proposed hybrid algorithms with respect to both encryption and decryption time. Among the proposed hybrid algorithms, the algorithm that used layered algorithm on the result of combination algorithm was the fastest.

CONCLUSION

During VCC communication, it is very important to protect the messages being transmitted by the vehicles. In this paper, cryptographic algorithms are proposed to protect the messages. Hybrid cryptographic algorithms that combine layered and communication based methodologies are proposed. For this purpose, a 2-stage algorithm is proposed. In the first stage two layered and two combined algorithms are designed, from which, the best performing algorithm is selected. These algorithms are then combined to form the proposed hybrid method. For this purpose, four algorithms, namely, Blowfish, 3DES, AES and RSA algorithms, are considered. Experiments showed that the method combined 3DES with Blowfish along with the method that combined RSA with AES algorithm, using layered-combination fashion of hybridization produced maximum efficiency. In future, methods that can further protect the messages, like signcryptography, will be analyzed and explored.

REFERENCES

1. Antonio, G., Sameer, S.M., Jun, L. and Wensong, W. (2020)Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey, Article ID 5129620, Vol. 2020, Pp. 1-25.
2. Aung, T.M., Naing, H.H. and Hla, N.N. (2019) Complex Transformation of Monoalphabetic Cipher to Polyalphabetic Cipher : (Vigenère-Affine Cipher), International Journal of Machine Learning and Computing, Vol. 9, No. 3, Pp. 296-303.
3. Chakraborty, R., Bairagi, A. and Bandyopadhyay, S.K. (2020) Design and implementation of two-layer encryption system in cryptography, Vol. 5, Issue 2, Pp. 424-427.
4. Ekwonwune, E. and Enyinnaya, V. (2020) Design and Implementation of End to End Encrypted Short Message Service (SMS) Using Hybrid Cipher Algorithm. Journal of Software Engineering and Applications, 13, 25-40.
5. Kugali, S.N. and Kadadevar, S. (2020) Vehicular ADHOC Network (VANET):-A Brief Knowledge, International Journal of Engineering Research & Technology, Vol. 09, Issue 06, Pp. 1026-1029.
6. Kumar, S., Karnani, G., Gaur, M.S. and Mishra, A. (2021) Cloud Security using Hybrid Cryptography Algorithms, 2nd International Conference on Intelligent Engineering and Managem, Pp. 597-602.
7. Liu, Y., Wang, L. and Chen, H.H. (2015) Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks, IEEE Transactions on Vehicular Technology, Vol. 64, No. 8, Pp. 3697-3710.