International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Adaptive Security Mechanism for Vehicular Data Networks or Platform using Degree of Privacy

Amol Phatak[1], Dr. V. Srinivasa Rao[2]

Submitted: 17/09/2023 **Revised**: 18/11/2023 **Accepted**: 28/11/2023

Abstract: Vehicular data platforms and networks use IoT devices to provide communication support system and enable the value-added services which generates large amount of vehicular data. The need of hour is to provide security to vehicular data platforms. In this paper, adaptive security mechanism was proposed to secure vehicular data. An adaptive security mechanism allows users to select the degree of privacy they want to use. The privacy degree is divided into low-level, medium level and high level as per the requirement of user. The vehicular data is categorized into vehicle identification & configuration data, running status data, maintenance data, insurance data, driving safety data etc. Different private-key and public-key cryptography algorithms such as DES, AES, RSA are applied on vehicular data of different sizes and suggested the type of suitable algorithm to maintain the degree of privacy and to ensure the requirement of vehicular data category.

Keywords: *Private Key and Public key cryptography algorithms, Security and Privacy, Vehicular data networks.*

1. Introduction

Modern Vehicles are equipped with several electronic devices and are connected through various means of communicating devices which provides a vast amount of useful vehicular data. However, the vehicular data suffers security issues making vehicles unsafe to their users [1] and this lack of security in modern automobiles raises the need of advanced privacy and security mechanism.

The type of privacy to be used is a choice of user, an adaptive privacy protection and security mechanism allows users to select the degree of privacy they want to use. In this paper, the privacy degree is divided into low-level, medium-level and high-level as per the need or demand of the user. The user not focusing much on vehicular data security may choose the low-level privacy degree whereas the Very Important Person (VIP) requires high-level of privacy to protect his/her vehicular data from hackers/intruders.

The standard vehicular data is categorized into Vehicle Identification & configuration data, running status data, Maintenance data, Insurance Data, Driving Safety data etc. The section 2 of this paper provides the details of parameter or fields and its importance from security point of view.

To support the adaptive privacy of such vehicular data, different private key and public key cryptography algorithms are analyzed. In private key cryptography DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are used and analyzed on vehicular data of different sizes. The RSA(Rivest-Shamir-Adleman) algorithm is used under the public key cryptography. The experimental results are shown in Section 3. It analyzes the encryption and decryption time requirement of above algorithms on vehicular data of different file sizes. It also presents the comparison of algorithms at general security level.

2. Vehicular Data Categories

Vehicular data is categorized into Vehicle Identification & configuration data, running status data, Maintenance data, Insurance Data, Driving Safety data etc. [2]

1. **Vehicle Identification & Configuration data:** It provides identification information about a vehicle such as Vehicle Number, Engine number, Type of vehicle (car, van, truck etc.), Size and Shape of Vehicle (width, height, weight etc.), Fuel Configuration information (petrol, diesel, cng or electric), Number of Wheels,
2. **Vehicle Location data:** It is generally used to track the current position of vehicle and provides the information such as Latitude and Longitude as well as the current location on map
3. **Running status data:** It provides the information such as Vehicle Speed (Wheel, Engine speed etc), Light status, Fuel status, Seat belt status and so on
4. **Maintenance data:** This information provides user the different parameters of vehicle maintenance, used for testing the condition of engine and servicing

[1] *[*]Research Scholar, VelTech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India*
Email id: amol1911@gmail.com ORCHID ID: 0009-0007-8905-6658
[2] *Dean School of Computing, VelTech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, India*
Email id: drvsrao9@veltech.edu.in

related fields. It covers the status information of odometer, Transmission Oil, Transmission Clutch, Break Maintenance, Battery status, Tire condition etc.

5. **Driving Safety Data:** This part of information is related to safety mechanisms used for driver and passengers such as Anti-Lock Breaking System, Airbag Status etc. It includes the status information such as Anti-Breaking system, electronic stability control, Top speed limit, Airbag status, Door lock interface, Child safety lock and Seat belt status
6. **Insurance Data:** It contains the information such as Insurance Policy number & Type, Period of insurance, Insured name, Vehicle identification number etc.

Adaptive Security Level:

The above types of vehicular data were further divided into the following types based on importance of the data [3],[10] from security point of view

1. **High Level Security**: Vehicle Location data and Running Status data were required High Level Security and it should not be hacked, so we should use the High level of privacy degree for the same
2. **Medium Level Security:** Vehicle Identification and Configuration data and Driving Safety data are of the medium level risk, so it's better use the medium level of privacy degree and recommended cryptographic algorithms for the same
3. **Low Level Security:** Insurance data and Maintenance data generally required by the insurance companies or RTO so it can be shared for the same. This data is under the category of low risk and a normal or low-level security algorithms can be used for the same

3. Cryptographic Algorithms Applied

3.1 Data Encryption Standard (DES):

The Data Encryption Standard (DES) is adopted as National Standard [4] and IBM team contributed in the development of DES.

The National Bureau of Standard (NBS) has announced the DES as one of the best cryptosystem which is used in the most of the application for information protection. The DES comes under the category of symmetric or single key or private key encryption algorithm.

DES is type of block cipher technique that takes a plaintext bit of fixed-size message string as input and transforms it into another cipher text string of the identical size by applying a series of complex operations. It uses 64 bits size of a block. It makes use of a private-key to customize the transformation, so that the decryption can only be performed by using the same private-key which was used while encrypting the plaintext. The size of the private key is of 64 bits, out of it makes use of only 56 bits during transformation. Remaining 8 bits are used for the purpose of parity checking, and are discarded afterward. Therefore, the effective key length used by DES algorithm is 56 bits. The DES uses 16 identical stages of processing, called as rounds. It also has an IP (Initial Permutation) and FP (Final Permutation). These permutations are inverses of each other. IP and FP have not any cryptographic significance, but were added to provide loading blocks in and out of 8-bit based hardware. In initial step, the block is divided into two 32-bit blocks and both blocks are separately processed. It is called as the Feistel scheme. The Feistel structure assures the similarity between the encryption and decryption process, the major difference is that the sub-keys are applied in the reverse order while decrypting the cipher text.

Now days, the time required for processing the cryptanalysis is reduced a lot, and few hardware techniques were also developed and available. Due this DES can be attacked using different kinds of cryptanalysis techniques. The DES must be stronger than the other cryptosystems in its security [6],[9]

3.2 Advanced Encryption Standard (AES)

AES is an iterated cipher proposed by Joan Daeman and Vincent Rijmen [5]. It supports variable length block and key sizes (e.g., multiple of 32 bits). However, only the 128-bit block size and 128, 192, 256 bits keys are specified as AES standard.

One of the key feature of AES is that its structure does not uses the Feistel network such as its predecessor DES. In Feistel network half of the information block is employed to switch the opposite half of the information block so the halves are swapped.Instead of this scheme, AES is predicted on S-P network within which the complete 128 bits input block is organized as 4 X 4 bytes array called State and is processed in several rounds. Number of rounds to be used rely on the length of the key like, it requires 10 rounds for 128 bit key,192 bit key requires 12 rounds whereas 14 rounds are required for 256 bit key. The State arrayis changed at each round with respect to a round function that defines the following four different byte-oriented transformations.

a) Sub Bytes Transformation

b) Shift Rows Transformation

c) Mix Columns

d) Add Round Keys

In AES, the number be rounds and its functionality each of round which is required to process the encryption and

decryption varies and completely depends on the size of key used.

3.3 RSA: Rivest-Shamir-Adleman (RSA)

RSA algorithm comes under the category of public key cryptography. RSA algorithm, one of the most powerful and popular algorithms which can be used for data encryption as well as digital signatures. The difficulty or hardness in decomposition of large numbers is the security of RSA algorithm. In RSA algorithm, the public key and private key were constructed using two large prime numbers and private key cannot be derived from public key. The cipher text is the decomposition of product of two large prime numbers so it is not possible to guess the plaintext from a public key [8]

RSA algorithm is also used for authentication of users. Diffie-Hellman key exchange algorithm is a key component in the authentication framework. At the start of conversation or key agreement session, participants communicate by using Diffie-Hellman algorithm and create shared keys which will be used for key agreement protocol for next steps followed for conversation.

In RSA plaintext and cipher text are consider as integers between 0 and n-1, where n is that the modulus. The standard size of n is 1024 bits. However, the recommended length of n is 2048 bits now. RSA uses following three sub algorithms:

a) Key Generation algorithm

b) Encryption Algorithm

c) Decryption Algorithm

4. General Comparison of DES, AES and RSA

a. DES was designed to run on hardware, so it is faster in hardware and relatively fast in software. It is having security issues such as it can be broken by brute force attack and fails in front of linear cryptanalysis

b. AES is faster and safer encryption algorithm compared to DES and other symmetric cryptography algorithm. However, it is difficult to write constant time high speed AES software for general purpose computers to prevent timing attacks

c. RSA is considered safe with large key i.e., 2048 bits. Like AES, implementation may introduce some vulnerabilities especially the big number arithmetic operations in Chinese Reminder Theorem (CRT) may introduce some bugs

d. RSA (Asymmetric cryptography) has more functionality whereas DES and AES (Symmetric cryptography) are much faster

4. Result and Discussion

In this section, to evaluate performance of the DES, AES and RSA on vehicular data of different categories as mentioned in section 2.1, the vehicular data of size 10KB, 1MB, 10MB, 50MB and 100MB are considered

Comparison based on Time Requirement:

All the three algorithms are implemented and their encryption time, decryption time and total time (encryption + decryption) were calculated and are listed in below table.

Table 4.1 Comparison based on Encryption time

Algorithm / File Size	**DES**	**AES**	**RSA**
	Encryption Time in ms	Encryption Time in ms	Encryption Time in ms
10 KB	6	600	956
1 MB	115	747	1260
10 MB	993	1083	2120
50 MB	3174	2001	6650
100 MB	6838	4220	26033

The encryption and decryption time calculation is shown in Table 4.1 indicates the analysis as follows:

a. DES is faster for the vehicular data of small size up to 1 MB (takes only 115ms for encryption). Comparatively AES and RSA take more time for encryption almost 6 times slower than DES

b. It is observed that AES is suitable for vehicular data of medium size around 50 MB (takes only 2001 ms) compared to DES (takes 3174ms) and RSA (takes 6650ms) it is recommended to use AES for vehicular data between 10MB to 50MB

c. RSA algorithms' encryption time requirement (around 1000 to 6000ms) is more compared to DES and AES. Even it not suitable for the data of size 100MB as takes much more time (26033ms)

d. One of the interesting analyses for the data of size 50MB is that all DES (993ms), AES (1083ms) and RSA (2120ms) comparatively at same level and not having much more time difference

Table 4.2 Comparison based on Decryption time

Algorithm / File Size	**DES**	**AES**	**RSA**
	Decryption Time in ms	Decryption Time in ms	Decryption Time in ms
10 KB	4	7	25
1 MB	99	116	500
10 MB	775	477	806
50 MB	2762	1550	1200
100 MB	6378	3488	12150

The decryption time calculation shown in Table 4.2 indicates the analysis as follows:

a. If we consider only the decryption time requirement then, for a small size vehicular data up to 1 MB both DES (99ms) and AES (116ms) are suitable compare to RSA (500ms)

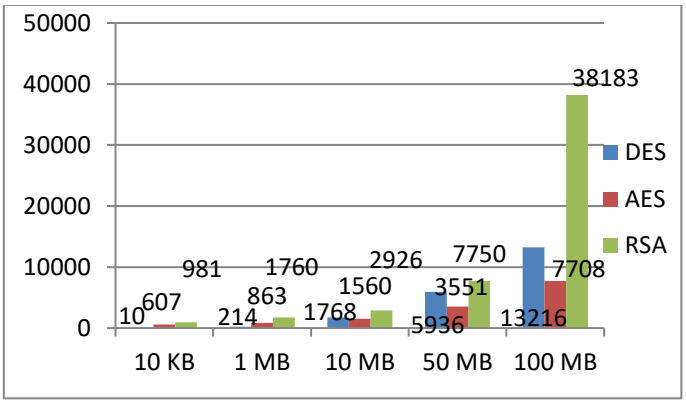
b. AES proved to be more appropriate for the data of size 50MB to 100MB compared to DES and RSA

c. For the vehicular data of size around 10MB, all three algorithms Decryption time requirement is at same level, so it is recommended to use any of the algorithm based on security issues or requirements

Table 4.3 Comparison based on Total Time (E+D)

Algorithm / File Size	**DES**	**AES**	**RSA**
	Total Time in ms	Total Time in ms	Total Time in ms
10 KB	10	607	981
1 MB	214	863	1760
10 MB	1768	1560	2926
50 MB	5936	3551	7750
100 MB	13216	7708	38183

The comparison result is shown below in graph to have a more insight on the use of appropriate algorithm as per the level of degree of privacy needed to protect the user's information



After comparing the Encryption and Decryption time requirement separately, following points are observed based on the Total Time (Encryption + Decryption) calculations shown in Table 4.3 and its respective graph:

a. DES is suitable for Vehicular data of small size i.e., 1KB (only 10ms) to 1MB (214ms) compared to AES (607 to 863ms) and RSA (981 to 1760ms)

b. AES is suitable for vehicular data of size 10MB (1560ms) to 100MB (7708) compared to DES (1768 to 13216ms) and RSA (2926 to 38183ms)

c. RSA algorithms' total time requirement is more compared to DES and AES but, it is recommended for high level security of vehicular data

Comparison based on security issues:

The three algorithms viz DES, AES and RSA which are analyzed in above subsection based only on the time requirement. The section 2.3 also highlights the general comparison of these three algorithms[10] The following observations were based on the security requirement and security issues

a. At low level security or the general security requirement for vehicular data, it is recommended to use the DES algorithm. DES hardware implementation is easy compared to AES and RSA, but it suffers from Brute force attack. The Differential Cryptanalysis (DC), Liner Cryptanalysis (LC) and Davies Attack (DA) are theoretically faster than Brute force attack but not feasible in practice

b. At medium level security the AES is recommended and most suitable algorithm to secure vehicular data. AES is more secure as Brute force Attack is impractical as AES minimum cipher text key is 128 bits that provides 2^{128} possible keys. AES does not suffer from Mathematical Attack; however it is susceptible to Timing Attack.

c. At higher level security, it is recommended to use RSA algorithm to secure vehicular data. RSA algorithm having small size key seems to be vulnerable to Brute force attack but, the issue can be

resolved by using large size key. Mathematical Attack is prevented again by using large key and Timing attack is also prevented using few countermeasures. RSA having more functionalities so it is recommended for the user who want High Level Security by compromising more encryption and decryption time requirement

5. Conclusion and Future Scope

This paper focuses on the use of different cryptographic algorithms on vehicular data. The three important cryptography algorithms viz. DES, AES and RSA are applied on types of vehicular data. It also focuses on the use of adaptive security which allows user to select the security level he/she want to use like low-level, medium-level and high-level security. The experimental results shows that DES should be used for low-level security of vehicular data like insurance data, maintenance data etc. whereas AES is useful to provide medium-level security for vehicular data of type Vehicle identification and configuration data, driving safety data etc. The vehicle data of high importance such as vehicle's location and running status data should be encrypted using RSA algorithm as it is having more functionality compared to DES and AES but, user has to bear the more processing time.

In this paper, only DES, AES and RSA cryptographic algorithms are considered but, the work can be extended for other algorithms like 3DES, MD5, ECC, Blowfish etc. The vehicular data categories other than suggested above can be used to have more insight on the further types of vehicular data.

References

[1] Ahmer khan jadoon, Lincheng Wang, Tong Li, "Lightweight Cryptographic Techniques for Automotive Cyber security" volume 2018,

[2] Specification defines the standard for vehicle data "https://www.w3.org/TR/vehicle-data"

[3] C. Kaiser , A. Stocker1 , G. Viscusi , A. Festl , P. Mörtl , M. Glitzne,Virtual Vehicle Research Center, "Quantified Cars An exploration of the position of ICT start-ups vs. car manufacturers towards digital car services and sustainable business models",

[4] D. Coopersmith, "The Data Encryption Standard and its strength against attacks", IBM J RES, Vol 38 no. 3 1994

[5] Seung-Jo Han, Heang-Soo Oh, "The improved Data Encryption Standard (DES) Algorithm", Jongan Park IEEE Transaction 1996

[6] "Data Encryption Standard for IoT Applications based on Catalan objects and Two combinatorial structure", IEEE Transaction 2020

[7] Muzafer H, Mohamed Elhoseny, Mahmoud Mohamed Selim, and K. Shankar, "The comparative study of the performance and security issues of AES and RSA Cryptography" Abdullah Al Hasib and Abul Ahsan Md. Mahmudul Haque, 978-0-7695-3407-7/08, 2008 IEEE, DOI 10.1109/ICCIT.2008.179

[8] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for

Encryption and Decryption", IEEE 6th International Forum on Strategic Technology 2011

[9] Miles e. smld and dennis k. branstad, "The Data Encryption Standard: Past and Future", ,proceedings of the ieee, vol. 76, no. 5, may 1988

[10] "Adaptive security provisioning for vehicular safety applications", January 2017 International Journal of Space-Based and Situated Computing 7(1):16, DOI: 10.1504/IJSSC.2017.084120