I.J. Information Technology and Computer Science, **2022, 2, 17-30**
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2022.02.02

Dual Layer Encryption for IoT based Vehicle Systems over 5G Communication

Sajid Bin-Faisal
American International University - Bangladesh, Dhaka, 1229, Bangladesh
E-mail: sajidfaisal80@gmail.com

Dip Nandi, Mashiour Rahman
Department of Computer Science, American International University - Bangladesh, Dhaka, 1229, Bangladesh
E-mail: {dip.nandi, mashiour}@aiub.edu

Received: 21 August 2021; Revised: 11 October 2021; Accepted: 06 November 2021; Published: 08 April 2022

Abstract: In modern communication scenario of the 5G era, the service quality is the greatest concern for the users. Also, the concept of security can't be neglected in this case. In the IoT oriented services like vehicle and VANET systems, the security in the presentation layer of the network is required. This work is over the security mechanism of the service storage and fetching the files for service. A new scheme of multi layered file and content encryption has been produced in order to strengthen the security of the file and data to maintain integrity and confidentiality of the IoT enabled services implemented in 5G. The encryption scheme is designed for the password encryption through asymmetric key cryptography (RSA) along with an enhanced concern of internal content or data security with symmetric key (AES-128) cryptography. This encryption system of double layer for a file makes the study unique and differentiable than other security schemes.

Index Terms: Communication, VANET, Security, Scheme, IoT, Integrity, Confidentiality, Encryption, Symmetric.

1. Introduction

Internet of Things (IoT) is the service platform which is capable of bringing the things such as people, machines and services under the supervision of an internet-based platform. The services are growing rapidly from the last decade. The current state of the IoT industry is based on the power efficiency, service efficiency, integration and security to gain reliability of services to achieve Quality of Services (QoS). The Consumers rights and security of the data is a must in IoT arena. A consumer will never consider any kinds of security issues or failures of confidentiality occurred in the system. They should be provided the enhanced and strong form of access control mechanisms, integrity and authentication as per the requirement of safety [1]. Various probable attacks need to be analyzed in the particular services and network architectures. The device and system maintaining considerations should be briefly summarized and demonstrated for both side of the parties. The industrial IoT or the IIoT needs the well-structured usage of the security protocols and maintenance of the system. Otherwise, it will never be accepted globally for industrial purpose. The security vulnerabilities and drawbacks can be similar in both IoT and IIoT though in some cases IIoT may have more issues and problems regarding organizational data security [2]. As organizational data contains tons of personal data for the users which should be kept secret by agreement and never be leaked either intentionally or unintentionally due to the failure of the security protocols.

The focus is on the security assurance and trust management of the smart vehicle service on V2V services of 5G communication for IoT Systems. The study aims to provide both the data security and Confidentiality of the vehicle users in the operation. There should be categorization for the IoT for its Connectivity, Industry, location, device, user, and technology [3]. The next few years from now on should be the era of 5G telecommunication technology. The 5G is capable of covering an astonishing amount of data passage around the integrated services. Also, the intercommunication among the systems is highly required in a vehicle service. The implementation of 5G communication has been on trial in the developed countries like South Korea, China, USA and also in some countries of Europe [4]. The spectrum frequency and bandwidth coverage capabilities are way beyond what it was in 4G communication system. The IoT applicability and usage should be higher in 5G communication as these demands very good amount of network coverage. The bandwidth size is 2 times greater than what it was in 4G. The 5G network is focused over several services and industrial intercommunications. As the number of platforms are increasing the service gets exposed to possible other third-party organizations and stakeholders. Thus, network segmentation of multiple services into mini slices can be a solution in this scenario. As the 5G network mostly works for coverage and bandwidth capabilities, it has

to depend over some important security concerns like confidentiality, authentication, and data integrity to the other communication systems. A huge number of vehicles and machines are coming into the network in the next few years of evolutionary communication generation of 5G. These machine to machine, vehicle to vehicle services in the industrial factors need to be monitored by central data service and software systems. Thus, the probability of data leakage is very high. So, that is why the security in 5G service is the target point of the research.

Security is going to the next burning topic in the future days of global communication. There has been a number of 2 billion users of devices in just the year 2011 and it was nearly 10 years before back. It is predicted that this number will grow faster than ever in the rate before the end of the half for this 21st century. Security in this work does not mean to be only the prevention of theft and antisocial activities in the vehicle system. It should also produce the matter of confidentiality and user data leakage management in the service. The car/vehicle or the devices are connected to it in the vision to make the service better. Hence, as a number of user properties, personal data and devices are interconnected it should not be easy for an intruder to access all the devices and information of a user or organization by the help of snatching a single vehicle. That should be considered as a security loophole. The confidential data is not expected to be lost or violated just because the theft or unauthorized access to a vehicle. Various security ensuring measures are being taken to facilitate security of the vehicles. Thus, the concern is authenticating the verified users and also being confidential about the leakage of the user-oriented data for their properties/ smart vehicles. Key management and authentication protocols along with the cryptographic technology are the basis of these type of security infrastructure in the application, presentation and network layer [5,6]. The GPS modules are used to locate the approximate location of the vehicle and the continuous tracking of the vehicle on service while running. The assurance in security is also provided in the past while the car is in a parking space by the help sensors, RFID chips and Person detection mechanisms. GSM are focused more on the communication throughput on the system, and this needs a satisfactory data integrity for the reliance of the service being provided in IoT. The things which are being focused on this security scheme is the IPv6 based surveillance camera, Authentication procedures, Low energy consuming chipset and modules, detection systems for verification, V2V (Vehicle to Vehicle) secured communication.

The objective of this research is to provide a double layered approach of encryption which will be serving the privacy and security requirements for both the file and the content inside the file for the services. The security tools like Boxcryptor, nCrypted, Sharedsafe, Cloudfogger and Ensafer are mostly being used though the security mechanism which are only based on the authentication of access and file encryption. This study indicates the need of both the file and file content security of a service platform in IoT through encryption. The experimental methodology is also shown in this article to prove the efficiency and feasibility of both the RSA encryption of password and content or data encryption by AES-128 of the data rows for the service platform. The linearity of the encryption scheme is proved at the end of the experiment through graph visualization.

Therefore, the contribution of this article is to provide a security assuring encryption system of dual layer that is integrated with both symmetric and asymmetric key cryptography to secure the files and the data contents in the files for a particular IoT service as the Internet of Vehicles or IoV. The paper also shows that the passwords can be made highly secure by encrypting through public key infrastructure RSA with process description. Then the rows can be encrypted in the data files with AES-128 algorithm efficiently by the conventional approach. Thus, the proposed model of “Dual Layer Encryption” of files by password protection and digital content security scheme are discussed in the later portions of the paper especially in portion 4. The result and the system structure verification and demonstration will be found on section 5.

2. Related Work

This portion discusses about the demand of security and the measures or protections to be taken to get rid of the suspected attacks. The state of the research regarding protection mechanism in the vehicle service provided in IoT. The current research scheme, the existing security products for the file and data level security and the working scope from the literatures would be guided.

At, first the research requirement in the vehicle systems implemented over 5G communication via IoT must be discussed before going to the depth of the study. Fifth Generation and its aspects in the future world will be arrived soon. It is still in the infant stages of its age. The World-Wide Wireless Web is the functional requirement that is needed in terms of ensuring the technological scheme. Wi-Max communication protocol that focuses on the modern world of Artificial Intelligence, Cognitive Science, Machine Learning and Data sciences to establish unlimited access and usage of the resources around the nations. The speed is beyond 1 Gbps that has to match the power consumption capabilities and architectural, systematic design of the technologies [7]. Current era of massive capacity management through Cloud Computing and storage services through the internet is the major challenge to manage. Yet, Security should be a major issue in the 5G telecommunication and if it is served successfully with proper CIA (confidentiality, Integrity & Authentication) then the services of business, education, agriculture, research, transportation, and medical systems will be a revolution through internet.

There should be categorization for the IoT for its Connectivity, Industry, location, device, user, and technology [3]. A model of acceptance in a specific framework is strongly required for technology enhancement in the industry.

Secured and manageable data framework is also a matter for concern for this study of security architecture. There is a system architecture for the safe city in the article "SafeCity: Toward Safe and Secured Data Management Design for IoT-Enabled Smart City Planning". There needs to be a security protocol of data processing and authentication purpose in a specific service of IoT. Number of vehicles in the track, water and other fuel dissipation are also analyzed in the particular article as these will be worthy enough to facilitate a smart city design [8]. So, some targeted points need to be indicated for that particular service to enhance in the security scheme in a vehicle service around the city in IoT. After that the overall performance should also be verified under the test operations. There should be a security platform for various levels of things in the IoT service. The fault in the things such as the small sensors and their energy consumption, routing protocol and device power management with overall service network of Wireless sensors [9]. Thus, the service can move towards a more secured solution scheme. The next page has the table 1 which contains the information of things or technologies used in the IoT service industries of vehicles for a secured communication protocol management. The interconnection of the things devices and sensors needs to be well structured and well equipped. The smart applications and services in IoT require the knowledge of every involved technology and the working mechanism [10]. The things are considered as the devices and technologies which are used to implement a service in IoT. The focused platform here is IoT based vehicle services. So, the usage and the reason of inclusion in the system are shown in table 1. There are 10 existing and most notable technologies used in the vehicle services of IoT to serve the system purpose. The list of things will be used in the IoT service scheme are provided:

Table 1. List of measures and technologies used for IoT vehicle service security.

SL	Technologies / Things	Usage
1	Wi-Fi	Basic LAN for the wireless service
2	RFID	For user and driver authentication
3	Vehicle	Bus, Truck, Cars etc around the service range
4	Android devices	For connecting a registered user in the service
5	Cloud	For data storage in the system
6	Encryption (AES)	Data security in the application layer of network
7	GSM	Global mobile intercommunication, data, voice and video transfer and roaming service around the globe.
8	GPS	Positioning of the vehicles
9	Cellular Tower	Base stations for power relaying in the network range. Basically, the antenna for radio Access network
10	Finger Print	Unique Biometric identifier of a person

The password system is a very reliable authentication process of user authentication in any sort of system verification. The password creation policy should be applied by a user in an intelligent manner. The password creating schemes can be found in the article [11] by Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider according to the services on the internet or offline. These are subjected to be made as a protection against brute force and dictionary attacks in the network.

Password System Oriented Attacks

Brute Force attack is the process that enables the permutations of the words in the dictionary to be tried out to break through the password security system. Yet, the attack can work at a faster rate and still it can take years to break in to the password system. In the article [12] "A study of passwords and methods used in brute-force SSH attacks", the authors Owens & Matthews have produced the manners of creating passwords to be lengthy, stronger and as less meaningful as possible to prevent the brute force attacks in the password protected services. The process of password authentication and development measures are directed as per the length of the key and error prone user attempts by Konark Truptiben Dave [13]. Also, a study regarding this brute force and dictionary attack to be conducted as a hybrid attack can break the password systems by a simple powered processors about 90% or more if these are meaningful or closest to a meaningful word [14]. The study on Slovenia establishes that the strong passwords remain mostly unbreakable while using strong processors to break the passwords. So brute force attacks on passwords can be prevented with strong and less meaningful passwords according to this instance.

Security through Encryption

Encryption is a process that helps to get rid of attacks like side channel attacks and fault attacks against the proposal produced by Fumaroli and Vigilant. The researchers Chong Hee Kim and Jean-Jacques Quisquater [15] have shown the effectivity of the measures taken to protect against these types of attacks within low power consumption. A hybrid authentication system with the AES and Elliptic Curve Cryptosystem has been produced in the health-based applications from the researchers Shailja Dahiya and Manoj Bohra by slightly modified ECC system with key expansion scheme of AES [16] which produces better performance and efficiency by time (in seconds) than the existing scheme of ECC, AES. The AES algorithm has been implemented in the same health-based application by using the

method of parallel processing by using GPU and CPU by spitting the task between these two-unit processors. The task has been divided by 5 consecutives by the authors Narayanan Manikandan and Srinivasan Subha [17] through text conversion to binary, process in local memory and combination of the cipher text which is forwarded to the CPU.

Cloud based Existing encryption applications' Observation

Cloud storage-based security assuring software like the Boxcryptor, Cryptomator and nCrypted are quite similar in the actions yet, the security standard is not 100% verified according to the ISO/IEC 25010 protocol as authenticity and service integrity are not satisfactory [18]. Desktop based encryption software like AxCrypt, and AESCrypt use the random key for encryption which misses in VeraCrypt and Diskcryptor [19]. The DiskCryptor and VeraCrypt attempts to secure the local disk storage and file-folder. These two uses layered encryption with the hardware and partition in the disk where the AxCrypt is secure as it uses AES-128 for file security and RSA-4096 for the security of the key with proper password management system [20]. Among all the client-side encryption software, the mathematical analysis over the encryption and adjustment has shown that Cloudfogger performs better than BoxCryptor, Ensafer, SafeMonk and SharedSafe [21]. However, Dropbox allows the use of BoxCryptor and TrueCrypt yet BoxCryptor tool encrypts one after another and on the way of transmission [22]. Where TrueCyptor encrypts the files altogether. Yet BoxCryptor is suitable for mobile communications with each end security [23]. Cloudfogger has the best performance using the AES-256 [24] encryption system but, it does not provide global level file layer security and authentication due to its accessibility. Most interesting fact is that only the Cryptomator tool performs better than boxCryptor and it works with AES-256 encryption for its file name and file layer [25] security while transmitting via cloud. Applications like 7zip [26] uses only the AES-256 encryption for securing just the file and the password does not remain safe at all. As it focuses more on compression and less on the file and its internal content security. So, the focus is only found over the authentication and file encryption process. However, the concern of making the password stronger to break through, by encrypting the password with a strong asymmetric key cryptography while observing the file content security with conventional approach of AES-128 for the Internet oriented services such as the vehicle platform of IoT.

The authors Repu Daman and Manish M Tripathi [27] have shown the difficulty of encryption from the client side in cloud-oriented health data security. They claimed the use of client-side encryption for serving the integrity of health data and the unreliability from the server portion. The researchers aimed to enhance the complexity of decryption, in order to facilitate the customers. Since it is an issue of confidentiality of the client side, the data needs to be properly and strongly encrypted by the authorized body. The use of the cloud platform is increasing day to day, yet this has been proved to be insecure at some instances especially from client side mentioned in article [28]. It has mentioned the importance of security in the physical level of cloud services. The mixture model of private and public cloud is also a matter to get more focus.

Thus, being inspired by the schemes, this research also proposes a way of both client and server-side oriented Dual Layer Encryption in Vehicle service data in IoT which comprises in the cloud Databases or storages. The security of the schemes is considered mostly focused over the authentication process, local storage security, access control and file encryption. So, it can be said that there is a lack of focus over the approach of both the file security and its data content security through different encryption standard. Also, it should be added that the performance is not more important than the purpose of digital data security. So, the industrially used tools need to be focusing more and more over the purpose of security and strengthening the encryption systems. The encryption system of RSA can also be used for password encryption along with digital verification of accesses. The password itself is a data which is used for the security purpose. However, the password itself can be encrypted as well. It is just like securing the thing or the technology which itself provides the security.

So, it can be seen that the vehicle services in IoT can be made secured in terms of data by using a dual level approach of encryption for both file and content encryption with different protocols, both symmetric and asymmetric. Some of the tools focuses over efficiency and speed and some focus on the step of process. Where some of the tools are based on a single approach of encryption. If the password itself is secured with a strong asymmetric encryption along with the conventional or existing digital verification process, then the security will be more satisfying for both the client and service providers' side in IoT. The systems like AxCrypt and Veracrypt can only perform in local devices and drives yet the security protocols can be adopted to the cloud services. Most of the systems do not consider about the internal content encryption. All of the work is actually over the security of the file through password. The files internal content can be easily decrypted by just providing the security. Which should not be allowed as this will provide only one layer security and that is through password and file encryption. This study is now using the similar but modified and enhanced concept of file and file content security by different approach of encryption. Here, the experiment is partitioned into 2 parts. The first part is over the password encryption process and test through RSA cryptosystem. The next one is the row of the files' data to be encrypted with AES-128 encryption. Thus, the file layer gets the focus of stronger security and encryption along with password-oriented authentication. The file data layer gets the dynamic process of encryption. Yet the content inside the file is itself encrypted with another layer of security. That is why this proposed scheme should be a bit modified and advanced than that of Boxcryptor and cloudfogger etc. Because, these tools only work on file encryption mostly along with password protection. Basically, these gives the encryption for one

single place of the service repository. The concept of data rows of the services like IoT based vehicle, needs the rows of data to be to be encrypted with suitable and faster encryption technique.

3. System Observation

The 5G is being implemented on various platforms in the global trade. The machine to machine and vehicle to vehicle communication is produced in 5G more efficiently. The upcoming and most futuristic form of digital wireless communication is this 5th generation. Almost most of the countries have already started the use of this generation as 5G core network and 5G new radio access network. The figure below demonstrates the architecture of the smart vehicle service security-based design in 5G network for IoT. The Smart vehicles in the IoT ecosystem is getting software based and wireless in its working protocol. Therefore, the need is increased for the security controlling mechanisms and tracking systems through GSM, GPS, cloud storage, smart machines, mobile communication access point etc. The smart systems are highly dependent over a security framework integrated in the IoT service to the users and drivers to locate, track, authenticate through the system architecture [29].

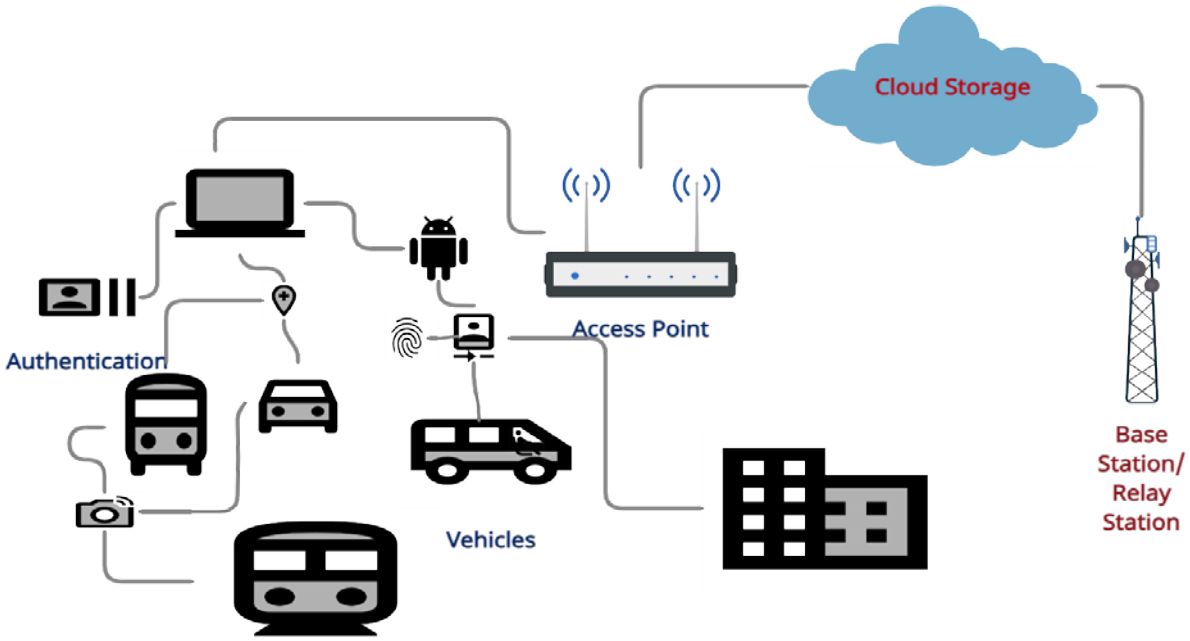

Fig.1. The smart-secured vehicle Service in IoT for 5G network. **"©Sajid Bin Faisal"**

The framework here integrates the vehicles like bus, train, cars in a specific service in a wireless system where the connectors are considered as the connection between the components but not the wires. A base station will be backhauled to an access point of the network slice where there are a number of users, machines of authentication and controlling platforms. The system will use the fingerprint scanning protocol to authenticate a user and the users' devices will be registered to the vehicles of the service platform. The GPS location tracking service and strong encryption system will be used to keep the data less attack prone. The continuous supervision through the surveillance camera may keep the unauthorized activities in the system. This may provide both theft protection and data security in the service. The cloud system will be used as data storage. The relay station may relay the information somewhere else other than the service.

The focus in this work is the data and file security through encryption process. The Asymmetric and Symmetric key encryptions both can be used in the security of the content and the file contains these vulnerable data. The type of the file and the data are analyzed later in this portion right after the general encryption process description. The responsible network layer for the encryption will be introduced.

The data format is shown as demo in the table below:

Table 2. Demo Data for the vehicle service in IoT platforms.

Vehicle_License	user_Email	Fuel_Percentage	speed (avg)15 min	last_Location(15 min)	Current_Destination	phone	Blood pressure
L-354	user23@gmail.com	85%	45 kmph	Mirpur2	Mirpur10	178939	120/80
L-356	user25@gmail	94%	52 kmph	Dhanmondi27	Mirpur10	168945	130/90
L-402	user79@gmail.com	59%	57kmph	Mirpur11	Asadgate	139087	110/70

The file name along with password will be protected via RSA encryption system. Among all the 7 layers of OSI (Open System Interconnection) model Presentation layer is one. This layer is the layer that comes after application layer and responsible for data security through encryption. The applications and the services are performed to be presentable to the Application interface. So, for any kind of protection that have done to protect the data rather than the physical system and network layer, is the presentation layer of OSI model. The encryption like the AES, RSA and DES are performed through specific algorithms to mathematically encrypt the data for making it unreadable and hard to detect for any further occurrences through the usage of the data. Thus, the cipher text generation through a specific algorithm and key management is done in the presentation layer. The presentation layer molds the data in to the presentable syntax independent form to the application layer. Thus, encryption is also a choice of data formation before going to the application layer. Thus, it can provide a contribution towards data security [30]. The content is kept secured by the cipher text form generated in this layer.

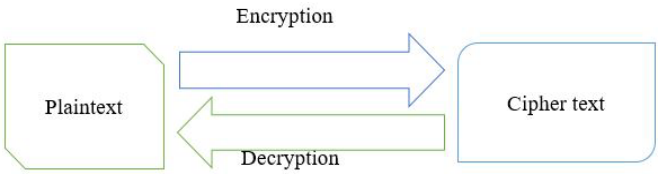

Fig.2. The flow of cipher text and plaintext generation through encryption and decryption.

Encryption Process RSA and AES-128

The private key of RSA is capable of decrypting the message to an end and no other keys can decrypt the message in this process. Thus, the security through RSA encryption is stronger as it uses 2 key-based encryption and it is not easy for the intruder to get the private keys to decrypt message from one end. Also, there are different private keys used to decrypt the message for each end. So, this is why the RSA asymmetric encryption is very hard to decrypt. The RSA asymmetric cryptography works for securing data by key generation, encryption and decryption. Thus, the data is transmitted after certain process of request [31]. The scenario can be described as followed:

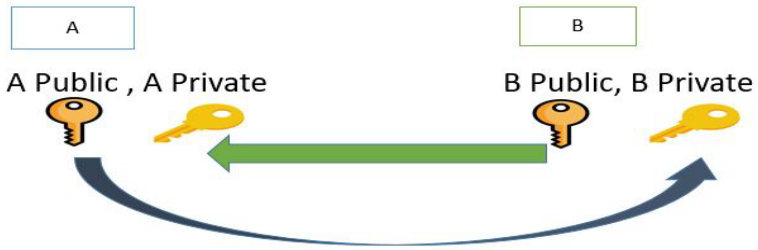

Fig.3. Visual representation RSA encryption Public-Private keys' task.

AES-128 is a symmetric or single key-based encryption system which works through consecutive operations of AddRoundkey, SubBytes, Shiftrows into 10 consecutive iterations [32,33] and Mixcolumns (only on the last iteration) [34]. The industrial data is mostly seen to be encrypted by this process of encryption.

4. Proposed Scheme of Security

The concept of the work is focused over these 2-encryption process. The reason behind using two different encryptions for data security of the vehicle service users or drivers of a system of IoT industry in 5G communication will be demonstrated in the next portion. RSA and AES are both used for different purpose of the security protocol derived in this study. The security measures in the presentation layer, RSA and AES encryption process and the vision of data security through a new approach of encryption are briefly discussed below. In the end the reason behind this approach will be theoretically justified for the 5G communication technology in IoT environment.

The data is secured in the vehicle service through encryption process in the presentation layer. This layer is concerned about the data modification and tampering through unwanted access to the data of the service. For this reason, the data should not be neither disclosed nor modifiable to the invaders of the system service in IoT. If a scenario is considered as follows:

The data is stored in the specific cloud storage or service database. One person wants to break through the assistance in the physical layer of hardware level or through the port related mismanagement in the network layer. The poor performance of the intruder detection mechanism of the network layer can also be responsible for this kind of access of the intruder. The intrusion into the system may still save the data from being polluted of stolen. The data should be encrypted in such a manner that it would be almost quite impossible for the intruder to use, read, fabricate,

modify or run the data that is the confidential property of the users. Suppose if he/she gets the data then it needs to be decrypted to read out in a short possible time. The message, file and the data in the file are 3 different vulnerable contents in an IoT service. The intruder first needs to locate the file, next the system access must be done by any type of session hijacking. If these are possible then the first dilemma the intruder may face is that he/she may find the file of the data is password protected and the password is strongly encrypted by Asymmetric key cryptography. It is going to be really hard for the attacker to break through the encrypted password of the data containing File. Then, even if the attacker or the bot has successfully opened the file; the data inside the file may be found encrypted as well. So now the attacker needs to decrypt the data in the database or any CSV file by a single key symmetric encryption. Thus, it can be seen that the file and data are being encrypted by 2 different encryption processes and the attacker needs to be faced with 2 layers of encryption in terms of opening the file and disclosing the data inside it. It can be said that the scheme is able to provide double layer encryption process for the sake of data security from the unwanted accesses and attackers. Two different type of decryption performance should be executed by the attacker and that makes the data strongly protected from the attacks.

The Scheme of security through dual encryption:

- File is secured with password (******…*) and that is encrypted with RSA algorithm.
- Only the person who has the private key of the password cipher can access after decrypting to that end.
- The data rows in the file are encrypted with AES-128. The entry iterations are encrypted with same key at the same instance and different key generated for different entry of the instances.
- User file is both passwords secured with encryption with internal content encryption.

##The data is encrypted in the file (AES-128). Also, this file itself is password protected through RSA encryption. So, first it needs a secured and strong encryption to break for **opening** the file. Next, the content inside the file needs to be decrypted to read/write.

Fig.4. Security Scheme for data through double layer encryption and password protection.

The experiment is based over both the RSA password encryption and file row data encryption by AES-128. The python version 3.9.1 has been used to see whether the string or character length of the password that needs to be encrypted is linear or not in terms of space. The number of data rows have been gradually increamented in order to check the capability of taking load for AES-128 encryption. Thus, the experimental process has conducted the test for the various length password to be encrypted with RSA and the linearity of the AES-128 cipher process through python based pycryptodome package. The advanced and enhanced procedure of password encryption via RSA algorithm is also considered as the part of the study.

RSA for password encryption

Basically, the RSA algorithm is used for key encryption for both ends. In this work the password characters will be considered as a string of alphanumeric values. The password will be encrypted with asymmetric RSA Public Key encryption (PKI). Suppose, the password is actually provided with the requirement from the service agencies. This password is encrypted with the public key and the desired and authenticated person has the private key to decrypt the password of the file. The reason for encrypting the file password with asymmetric encryption that is because it is hard to break and provides reasonable security and authentication through the key policy.

The password may contain at least of 8 characters and at least one numeric character with at least one capital and minimum 1 special symbol. So, for the sake of understanding the process of password encryption, one password is considered for understandability of the context. The password is considered as "**Filt@150"**.

Before encrypting the password, the values entered by the user must be converted to the UTF-8 corresponding values except the numerals. The process of numeral encryption is different in this case. As the RSA encryption works with key exchange but in this extent, the values are not numerals. So, these must be converted to the corresponding decimals. As RSA can only be calculated with decimals.

The password is: F (70) i(105) l(108) t(116) @(64) **150**

The Process of numeral encoding is different the values are contextually changed by the 2's complement method and thus 150 will be changed to other kind of value and then this value will be encrypted with the public key.

1→ 001
001 is inverted as 110. So, adding +1 to 110 is 111. So, 111 is the decimal value of 7
5→101
101 is inverted as 010. Adding +1 to 010 is 011. As 011 is the decimal value 3
0→ 000
inverted as 111 and adding +1 with it may have carry so it is not changed, and the decimal is 7 considered in this case.
So, the numerals like 70,105,108,116,64, 7,3 and 7 will be encrypted at each instance to generate the cipher text.
The Key Policy

There will be a pair of keys for RSA, and it will be changed by the service authorized after 3/4 days of interval. As it is known that the RSA algorithm as 2 important key parameters p and q. So, these values will be updated in Random after an interval of the time by the admin. here, the concept is the values like 70,105,108,116,64,7,3 and 7. So each of the values are considered as m1, m2….m_n=m_8

Here the value of n is calculated as,

$$n = p * q. \tag{1}$$

Public Key for encrypting (e,n) and private key for decrypting (d,n). e is relatively prime to (p-1*q-1) and has no common factor. The remainder will be 1. so, the calculation process of d and e is to be got from,

$$\mathrm{d} * \mathrm{e} \bmod (\mathrm{p}-1) * (\mathrm{n}-1) = 1 \tag{2}$$

The formula for encryption is

$$\text{cipher text} = (\mathrm{m})^{\mathrm{e}} \bmod \mathrm{n} \tag{3}$$

for getting back to plaintext is:

$$(\mathrm{CT})^{\mathrm{d}} \bmod \mathrm{n} \tag{4}$$

m 1 = 70

m2 =105

m3 = 108 and so on

Now the first char as a message is targeted for encryption and it is 70. thus, m1 is 70. The value of p and q are 10 and 17 in this instance. So, n is 10x17=170 and p-1*q-1 = 144, 144x1+1=145, 145 mod 3 = 1 and the divided value is 48. hence, d is 48 and e is 3. Public key (3,170) private key (48,170). RSA Password portions encrypted via the PKI equations:

Table 3. conversion of the message portions of the passwords to cipher text

Message Portion	Value of portion	(m)^e mod n (encryption)	Corresponding ASCII char	Cipher Text
m 1	70	(70) ^ 3 mod 170 = 110	“n”	**“n_12~43273”**
m 2	105	(105) ^ 3 mod 170 = 95	“_”	
m 3	108	(108) ^ 3 mod 170 = 12	“12”	
m 4	116	(116) ^ 3 mod 170 =126	“ ~ ”	
m 5	64	(64) ^ 3 mod 170 = 4	“4”	
m 6	7	(7) ^ 3 mod 170 = 3	“3”	
m 7	3	(3) ^ 3 mod 170 = 27	“27”	
m 8	7	(7) ^ 3 mod 170 = 3	“3”	

So, the encrypted string to RSA is “n_12~43273 “the cipher text = “n_12~43273”.

The Decryption process (Cipher text to Plain text)

Table 4. Reverting back to the plain text from the cipher potions obtained in the cipher text part.

Cipher Portion	Value of Cipher	(CT)^d mod n (decryption)	Binary value to reverse 2's complement (for numeral portions)	Corresponding ASCII char	Plain text
c 1	n	(110) ^ 48 mod 170 = 70	-	"F"	"**Filt@150"**
c 2	_	(95) ^ 48 mod 170 = 105	-	"i"	
c 3	12	(12) ^ 48 mod 170 = 108	-	"l"	
c 4	~	(126) ^ 48 mod 170 = 116	-	"t"	
c 5	4	(4) ^4 8 mod 170 = 64	-	"@"	
c 6	3	(3) ^ 48 mod 170 = 7	111 binary and 2's complement is (000+1) =001	"1"	
c 7	27	(27) ^ 48 mod 170 = 3	011 binary and 2's complement is (100+1) =101	"5"	
c 8	3	(3) ^ 48 mod 170 = 7	111 binary and inverted as 000	"0"	

So, the plaintext of the password string is "**Filt@150**".

RSA Padding and Process of Password encryption for the File

Let's consider the password is of 8-character inputs of the string. Then it is easy to take all the characters as the sequential array content for m1, m2, m3, m4, m5, m6, m7 and m8. Then the questions come as what if the password is of 12 characters or maybe more than that as 16, 20 or maybe 21. This process of padding technique can be described in this portion. The target is to make the string input of password to make consisting of 8 sequent portions. The table below shows the number of characters to be dealt for padding to put them in the encryption formula as numeric. The size of the string and character padding process is shown for the portioning of the message into 8 sequential parts.

Table 5. The Padding chart for the password to be encrypted with RSA for 8 portions.

String Size	Padded sequence	Message Portion division into 8
8 chars	1,1,1,1,1,1,1,1	Each character as mn (1-8)
10 chars	2,2,1,1,1,1,1,1	First 2 portions m1 and m2 takes two chars and rest 6 portions takes 1 each
12 chars	2,2,2,2,1,1,1,1	First 4 portions m1, m2, m3 and m4 takes two chars and rest 4 portions takes 1 each
15 chars	2,2,2,2,2,2,2,1	First 7 portions take 2 each and the last one takes 1 character
16 chars	2,2,2,2,2,2,2,2	All the portions take 2 character each
17 chars	3,2,2,2,2,2,2,2	All the portion takes 2 characters when the first one alone takes 3 characters.
18 chars	3,3,2,2,2,2,2,2	First 2 portions take 3 characters and the last 6 take 2 characters each.
19 chars	3,3,3,2,2,2,2,2	First 3 portions take 3 characters and the last 5 take 2 characters each.
20 chars	3,3,3,3,2,2,2,2	First 4 portions take 3 characters and the last 4 take 2 characters each.
21 chars	3,3,3,3,3,2,2,2	First 5 portions take 3 characters and the last 3 take 2 characters each.
22 chars	3,3,3,3,3,3,2,2	First 6 portions take 3 characters and the last 2 take 2 characters each.
. . . .	.. ..	… … … …
40 chars	5,5,5,5,5,5,5,5	All of the portions take 5 characters each.

The process of padded characters to calculate the numeric digits for passing forward to the encryption process focuses on the specific criteria. Let's consider that the password is "**Wint#Efs**". Then all the 8 characters are represented one by one as their ascii numeric values for RSA calculation. After padding is done the characters are going to be m1= 87, m2= 105, m3=110, m4= 116, m5=35, m6=69, m7=102 and m8=115. The concern is if the padded character is more than one in each portion of the string then the process enables the addition of the numeric values of each portion after padding. Then the additional value goes to the RSA encryption operation as the substring m1, m2, m3 and so on. When the password is of 12 characters then as per the rule, the first 4 portions take 3 characters and the last 4 takes 2 characters each. The character in each portion needs to be added up to through as a message substring for the password encryption in to the equation. When the password is "**vERnerNinh@A**", then the process of padding will be m1= vE, m2=Rn, m3=er, m4=Ni, m5=n, m6=h, m7=@ and m8=A.

Hence, m1= 118+69= 187, m2= 82+110=192, m3=101+114=215, m4=78+105=183, m5=110, m6= 104, m7= 64 and m8=65. So, the values 187,192,215,183,110, 104, 64 and 65 will go sequentially to the formula 'm^e mod n' for encryption. Then each of the corresponding value of the formulae will be generated as the encrypted cipher text of the

password with RSA. Now same thing happens for the password of 40 characters. The additional value of the 5 each character will be considered as the 8 consecutive message portions to be passed to the RSA encryption basic formula to obtain the cipher text. The characters in each portion of the string are added, no matter what the value is. It can be any number that can be used to put in as the number of the certain part for RSA encryption.

5. Result Analysis and Discussion

This portion describes about the complexity of the process and technical demo with data to be encrypted. The security assurance of the asymmetric RSA cryptography is far stronger than the symmetric fast cryptographic system. It is slower in some cases and the industry just want the processes to be faster as possible. So before implementing the RSA cryptosystem the designers of the cloud platform need to be aware of the efficiency and security performance of the algorithm. As the asymmetric RSA cryptography works with 2 different keys which enables the encryption with the public key and the decryption with the private key [35]. The RSA algorithm has the Big O or the worst-case scenario of O (n^2) that is in terms of polynomial case of efficiency. The algorithm is exponential according to the increase in the size of the key from 64, 128, 256, 512, 1024 and 2048 [36].

Mathematical Justification

If one instance of RSA execution requires polynomial of n that is O (n^2). Then the reason of it is using a specific length key with a pair of public and private key. In the proposed system the RSA algorithm needs to be executed for consecutive 8 times for the 8 portions of the password to be encrypted. Here, the same key of size 512 bit will be used as the private and public key of the RSA equations. From the theoretical perspective 1 message is encrypted by RSA with 25053 ticks or 0.002 ticks by the specific pair of p and q value. This time is the addition of the key generation time and the time taken to generate the cipher text [35]. So, it takes 0.00250 seconds to encrypt one message. Hence, it may take 0.00250 x 8 = 0.02 seconds to encrypt a password of 8 sub parts of a text string. So, in every case it will be the time near to 0.02 seconds, more or less.

The complexity of the RSA is O (n^2) normally. If 8 portions needed to be encrypted with the same key pair consecutively then it will be O (n^2+n^2+n^2+n^2+n^2+n^2+n^2+n^2) = O ($8n^2$) = 8 O (n^2). Hence it will be polynomial as usual and the subsequent 8 portions of a password partition may not affect the time complexity cases that much notably. So the RSA encryption process of password encrypting is an efficient approach [37]. So the time complexity is still a polynomial form of constant power 2 which is variable ^{constant}. Hence, the time complexity of RSA process is 8 O (n^2) which is basically polynomial and not exponential.

The Space Complexity

The password in this case has been considered as a sequence of 8 portions of character lists. In this case, the size of string in Python takes the value starting from 57 to beyond. The password has to get least of 8 characters and it can get longer as per the user or the authority requires. The space complexity in this case is dependent upon the size of the password string and the RSA key pair length in bits. It is cleared earlier that the key size in bits is fixed which is 512 bits / 64 bytes each public and private key. So, it can be said that as it is being used for all the 8 sequential portions of the password string, this has not much effect on the complexity variation. Thus, it is clear that the complexity in terms of RSA encryption for space is dependent over the size of the string. The string size is taken in the python version 3.9.1 programing kit for consecutive 8, 16, 24, 32 and 40 character long string as the password. The byte size taken in each instance have been checked from the code in python.

Table 6. The password string size and the memory size.

Password String Size (number of Characters)	Memory size in Bytes
8	57
16	65
24	73
32	82
40	90

However, after plotting the estimated byte size and string character numbers in the graph, a perfect linear relationship has been found in the end. As the size of the password string is the only parameter which works for the variation of the space required for the password encryption in asymmetric system. This can be meaningful to conclude that the RSA password encryption process is linear in terms of space constraint.

So, the space complexity of RSA encryption for password is linear or O (n) as the key length of encryption is fixed here. So, in the straight-line indicates the linearity of RSA process in this approach in terms of space. The RSA algorithm is acceptable in terms of both time and space as it shows efficiency of performance in both cases.

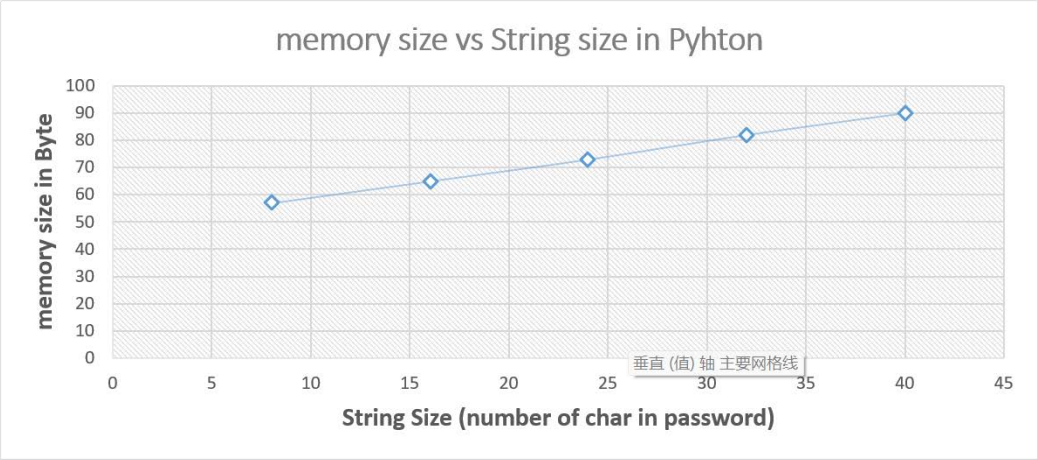

Fig.5. The linearity of the Password string length with memory space.

The AES-128 encryption over the demo data

The demo data has been provided in the system to be encrypted through AES-128 system in Python. Also, the process of cipher text generation and key token generated for the rows instance have been shown to make an image of the scheme. The system uses same key for the entry of the rows inserted in the same time. It uses different key of token to generate cipher text for those rows inserted at different attempts individually in the scheme. That makes the system more secure. Hence, the cipher text, returned plaintext and the conversion in binary code is shown in the verification below. The documentation assistance of the AES-128 work in python pycryptodome is from [38] with special thanks.

```
Microsoft Windows [Version 10.0.19043.1110]
(c) Microsoft Corporation. All rights reserved.

F:\Study materials\sem2\MsCS Thesis\Encryption in Python>python AES128.py
Key token:
<function token_bytes at 0x000001A847BD91F0>
Encrypted to binary format for the row:
0b1011101010110001100100110000000110100010001101010010110001110000011110000101110110011101010010100010010100011011100000
1101110110101111010100111111101010111101011110110010011010001101110100101100010000100110011100000011101011000101000110
0101111110001010100110101110111111001011100000110010110001111001100100111010000111000001100001001110000001000101110100111
1101101011101010101100011111100001000010001110101010010100110101011001000111101100101111111011111111110101001001011110100
0010101110100000
Row cipher text: b'@W\xe8%\xf5\xdf_\xf6\xc8jJu\x84\xf0c\xd5\xb5O\x17\x81\x13\x06\x87N\xe6\xb1\x0c.\xdf5\x15\xbf\x1a\xc5:
p&\xc4\xd2\x8d&{}\xf5\xa7^\xbb\xc1\x8d\x12\xa5\xce.<8\x96\x1a\xd1\x80\xc9X]'
plaintext returned: 54% L-354 user3@gmail 50kmph Kallyanpur Asadgate 179921 90/120
Key token:
<function token_bytes at 0x000001A847BD91F0>
Encrypted to binary format for the row:
0b1101110100001100011011001001100011010011010010010010101100110010010010001011110010111000111001000111111100100100001110
1000100001101000000011100101000101011101011110000001001001110101010011110101011001000010110110000110000111101011011010000
0101111101110110101111101100101110110010011110010000011100010111110100011010100110011110010011101110000101011000101101101
0000011101110110010000110010000001000100100100111011101011101101100110101010000011001010111001100100000000100001101001000
01000100001100110
Row cipher text: b'\xe6\x10!\r\x012W\x06\xd5\xecz\x93\x88\x80\x0c\xd9\x1d\xb4\xc5\nw\xf2L\x8d\xbe8\xc8\x93]\xf6\xb5}\x05
\xddz\x18\xb6\x90\xf5\xd4I\xe0uE9\xa0!:$\x7f\xe4\xb8\xbcH2+I\xd3\x98l\x0c\xdd'
plaintext returned: 61% L-354 user@gmail 53kmph Mirpur11 Kallyanpur 180645 110/160
```

Fig.6. Demo Rows of data encrypted in AES-128 for the storage.

The Execution time for AES encryption for the Rows in the Data File

The number of inputs with respect to the time taken in seconds have been observed in order to see the relationship between the input size and the time of encryption (AES-128) of row data of file. This verification has been verified in the Pycryptodome environment with the system input for number of rows of data in the source code.

Table 7. The increment of rows from 5 to 50000 to see the change in the encryption time. (Observed from the python source code by increasing the rows of input)

Number of Rows (Input)	Encryption Time by AES-128 (seconds)
5	0.0109
50	0.1518
500	1.4750
5000	6.2334
50000	58.8476

The first table (5) is to check the load taking ability for the input bounds of rows. The next one determines the linearity in the simplest of ways to check it with the number of rows along the x axis and the time of execution for AES-128 in seconds along the y axis.

Table 8. Execution time vs Input Rows table chart of observation.

Number of Input Rows	Time of Execution for AES-128 (seconds)
5	0.01562
10	0.01143
15	0.02246
20	0.02696
25	0.03579
30	0.04438

So, it can be determined that the file data is encrypted well efficiently via the AES-128 cryptography. The data related to the IoT vehicle service platform in the 5G era of communication can be served with security along with efficiency of service data fetching and processing. Thus, the principle focus of the 5G is remained along with the security assurance of the service. The RSA is used for password encryption with more than 100 times better security strength than AES-128. The internal data for the file in the cloud location is encrypted in the symmetric key cryptosystem. Thus, it can be claimed that both the file password and the internal content have been provided security via a double layer of encryption to protect the service data from getting compromised.

The execution time and linearity for both the encryption systems have been analyzed in this portion mathematically and theoretically. This scheme should be capable of serving the demanding capability of the security in the services of IoT vehicle applications. Also, other implementations of the IoT protocol in 5G can abide by this scenario such as the medical or health related data services. The interaction among the services in IoT is the main focus nowadays.

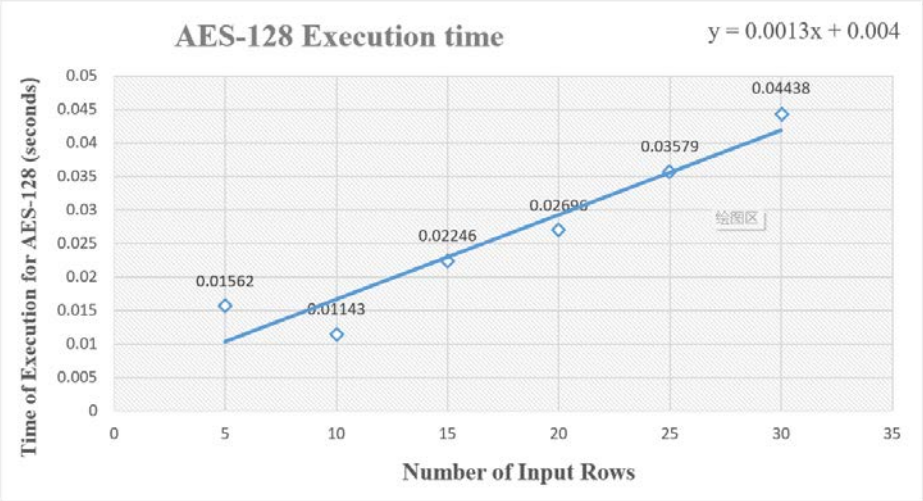

Fig.7. AES-128 execution time vs Input rows graph plotted.

As it can be seen that the graph shows a straight line of y= 0.0013x + 0.004. So, the AES-128 encryption is linear and it is efficient enough to get accepted. The verification is done by increasing the load and observing the execution time in seconds.

The rows inserted at one attempt is encrypted for the file with a similar master key. Even when the rows are inserted in different time uses the different master key that is managed by the service organizations. So, it should be quite complex for the attackers to get in to the file content after breaking the RSA encryption. Then, the attackers must know the sequence of the AES-128 master key of 16 bytes each for the rows entered at each attempt in the storage. Thus, the security protocol gets more efficient and reliable to work with the IoT system. The password of the files has been seen to be encrypted with RSA encryption linearly in terms of memory in figure 5. The figure 6,7 and table 7,8 determines the efficiency and workability of AES-128 cipher process via different load of input data rows.

The security related concerns and dilemma are now hugely focused over the security of cloud platform through the mobile devices [39]. So, the security measures should be more satisfying and stronger in order to maintain a successful communication platform for the customers. The inclusion of mobile devices for the internet-based cloud services for vehicle platform requires the need of convincing security protocols.

6. Conclusion

The study has shown the scheme of a Dual Layer encryption system in IoT vehicle services. The use of both password and content security along with the file security may enhance the security protocols of a service. The password string is aimed to be encrypted via asymmetric key cryptography along with the existing key policy through RSA. Next, the data containing rows on the service platform is internally encrypted as the second layer of encryption. Basically, this study protects the file password with RSA and the content inside of it should be decrypted after accessing the file for anyone. Thus, it would be near to impossible for the intruder to get into the data for facing two layers of encryption. Also, it is easier for the authorized person to access as they have the private key and master key of AES-128. Finally, it can be concluded stating the fact this study was focused to ensure a double encryption system to be undertaken in order to secure a file and its content. Previously, this concept had been missing in the existing data and file security tools and technical framework. In future, this double layer encryption concept with RSA and AES-128 should be tested as a security tool that will be ready to serve the demand of data and file security issues. The final observation of the research can be stated that both the system for file and file data encryption are technically linear. In future, the test cases of the proposed scheme should be analyzed according to the algorithm of prioritization for test cases on specific files in the service and their security-oriented effectiveness.

References

[1] Loi, F., Sivanathan, A., Gharakheili, H. H., Radford, A., & Sivaraman, V. (2017, November). Systematically evaluating security and privacy for consumer IoT devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy* (pp. 1-6).

[2] Yu, X., & Guo, H. (2019, August). A survey on IIoT security. In *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)* (pp. 1-5). IEEE.

[3] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in industry*, *101*, 1-12.

[4] Minoli, D., & Occhiogrosso, B. (2019). Practical aspects for the integration of 5G networks and IoT applications in smart cities environments. *Wireless Communications and Mobile Computing*, *2019*.

[5] Ukil, A., Bandyopadhyay, S., Bhattacharyya, A., & Pal, A. (2013, September). Lightweight security scheme for vehicle tracking system using CoAP. In *Proceedings of the International Workshop on Adaptive Security* (pp. 1-8).

[6] Ukil, A., Bandyopadhyay, S., Bhattacharyya, A., Pal, A., & Bose, T. (2014). Lightweight security scheme for IoT applications using CoAP. *International Journal of Pervasive Computing and Communications*.

[7] Sharma, P. (2013). Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network. *International Journal of Computer Science and Mobile Computing*, *2*(8), 47-53.

[8] Zhang, H., Babar, M., Tariq, M. U., Jan, M. A., Menon, V. G., & Li, X. (2020). SafeCity: Toward safe and secured data management design for IoT-enabled smart city planning. *IEEE Access*, *8*, 145256-145267.

[9] Hwang, Y. H. (2015, April). Iot security & privacy: threats and challenges. In *Proceedings of the 1st ACM workshop on IoT privacy, trust, and security* (pp. 1-1).

[10] Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, *19*(4), 439-444.

[11] Owens, J., & Matthews, J. (2008, March). A study of passwords and methods used in brute-force SSH attacks. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*.

[12] Dave, K. T. (2013). Brute-force attack seeking but distressing. *Int. J. Innov. Eng. Technol. Brute-force*, *2*(3), 75-78.

[13] Bošnjak, L., Sreš, J., & Brumen, B. (2018, May). Brute-force and dictionary attack on hashed real-world passwords. In *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro)* (pp. 1161-1166). IEEE.

[14] Kim, C. H., & Quisquater, J. J. (2007, September). How can we overcome both side channel analysis and fault attacks on RSA-CRT?. In *Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2007)* (pp. 21-29). IEEE.

[15] Dahiya, S., & Bohra, M. (2017, October). Hybrid parallel partial model for robust & secure authentication in healthcare IoT environments. In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)* (pp. 239-243). IEEE.

[16] Manikandan, N., & Subha, S. (2018). Parallel AES algorithm for performance improvement in data analytics security for IoT. *International Journal of Networking and Virtual Organisations*, *18*(2), 112-129.

[17] Ramadhani, E. H., Kabetta, H., & Amiruddin, A. (2020, December). Exploration of the Security of Free Data Encryption Applications for Cloud Storage. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1007, No. 1, p. 012042). IOP Publishing.

[18] Bursać, M., Vulović, R., & Milosavljević, M. Comparative Analysis of the Open Source Tools Intended for Data Encryption.

[19] https://www.axcrypt.net. Available [online]. Accessed: 26 July 2021.

[20] Das, S. K., Hossain, M. A., Sardar, M. A., Biswas, R. K., & Nath, P. D. (2014). Performance Analysis of Client Side Encryption Tools. *International Journal of Advanced Computer Research*, *4*(3), 888.

[21] Latha, S., Raju, K., & Santhi, S. (2014). Overview of dropbox encryption in cloud computing. *Transactions on Engineering and Sciences*, *2*(3), 27-32.

[22] https://www.boxcryptor.com. Available [Online].
[23] https://www.cloudwards.net. Available [Online].
[24] https://cryptomator.org. Available [Online].
[25] https://7ziphelp.com. Available [Online].
[26] Daman, R., & Tripathi, M. M. (2015). Encryption tools for secured health data in public cloud. *International Journal of Innovative Science, Engineering & Technology*, *2*(11), 843-848.
[27] Singh, J. (2017). Study on challenges, opportunities, and predictions in cloud computing. *International Journal of Modern Education and Computer Science*, *9*(3), 17.
[28] Sathiyanarayanan, M., Mahendra, S., & Vasu, R. B. (2018, August). Smart Security System for Vehicles using Internet of Things (IoT). In *2018 Second International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 430-435). IEEE.
[29] Lombardo, A., Merelli, E., & Palazzo, S. (1988, January). Implementation of encryption services in the OSI upper layers. In *1988 Computer Networking Symposium* (pp. 107-108). IEEE Computer Society.
[30] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter.
[31] Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19-22.
[32] Liu, J. J., Huang, Y. L., Leu, F. Y., Pan, X. Y., & Chen, L. R. (2017, October). Generating dynamic box by using an input string. In *International Symposium on Mobile Internet Security* (pp. 17-29). Springer, Singapore.
[33] Bulens, P., Standaert, F. X., Quisquater, J. J., Pellegrin, P., & Rouvroy, G. (2008, June). Implementation of the AES-128 on Virtex-5 FPGAs. In *International Conference on Cryptology in Africa* (pp. 16-26). Springer, Berlin, Heidelberg.
[34] Minni, R., Sultania, K., Mishra, S., & Vincent, D. R. (2013, July). An algorithm to enhance security in RSA. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.
[35] Khatoon, A., & Ikram, A. A. (2014). Performance Evaluation of RSA Algorithm in Cloud Computing Security. *International journal of innovation and scientific research*, *12*(1), 336-345.
[36] Edelsbrunner, Gu, H., 2008. *DESIGN AND ANALYSIS OF ALGORITHMS*. [online] Www2.cs.duke.edu. Available at: < https://www2.cs.duke.edu/courses/fall08/cps230/Book.pdf >
[37] https://pycryptodome.readthedocs.io/ Available [Online].
[38] Rida Qayyum, Hina Ejaz, "Data Security in Mobile Cloud Computing: A State of the Art Review", International Journal of Modern Education and Computer Science, Vol.12, No.2, pp. 30-35, 2020.
[39] Samia Jafrin, Dip Nandi, Sharfuddin Mahmood,"Test Case Prioritization based on Fault Dependency", International Journal of Modern Education and Computer Science, Vol.8, No.4, pp.33-45, 2016.

Authors' Profiles

MD Sajid Bin- Faisal has completed his Master of Science in Computer Network & Architecture and got his Bachelor of Science (BSc) in Computer Science & Engineering (CSE) at American International University-Bangladesh (AIUB) from the year 2017 to 2020. He has an enthusiasm over the research field of IoT, Network Security & Cryptography, Graph Theory, Algorithms & basic applications of Mathematics in modern world problems.

Dr. Dip Nandi is working as a Professor and Director for Faculty of Science & Technology (FST), at American International University- Bangladesh (AIUB). His research interest includes IOT, Data Mining, E-Learning etc.

Mashiour Rahman is working as an Associate Professor and Associate Dean of Faculty of Science and Technology in American International University- Bangladesh. His research interest includes Algorithms, Data structure, M-learning etc. He can be contacted at mashiour@aiub.edu.

How to cite this paper: Sajid Bin-Faisal, Dip Nandi, Mashiour Rahman, "Dual Layer Encryption for IoT based Vehicle Systems over 5G Communication", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.2, pp.17-30, 2022. DOI: 10.5815/ijitcs.2022.02.02