DOI 10.29042/2019-4758-4762

Helix Vol. 9 (1): 4758- 4762

A Hybrid Approach for Enhancing Security in IOT using RSA Algorithm

[1]M Krishna Sai, [2]N. Sivaramakrishna, [3]P V N S Ravi Teja, [4]Kolla Bhanu Prakash
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram,
Email: ksai444444@gmail.com, nelakuditisivaram@gmail.com, pvnsraviteja1120@gmail.com, drkbp@kluniversity.in

Received: 15th October 2018, Accepted: 29th January 2019, Published: 28th February 2019

Abstract
The internet of things is a system that related between digital machine, computer devices, mechanical machines objects and people and they are provided with unique identifiers and they are capable of transferring data from one network to other network with out human interaction. The internet of things is applied for many purposes in day to day life in medical and health care, transportation, building and home automation and the industrial applications such as manufacturing, agriculture, infrastructure application, metropolitan scale deployments, energy management, environmental monitoring etc. As we can see that the communication between us in current generation is mainly involved in communication through a network. So, taking the privacy and security as a criteria we need to provide a secure algorithm to protect the communication over the internet from the cryptanalyst. One of security algorithm to encrypt the data is RSA algorithm. In this paper, an overview of the hybrid RSA algorithm is explained.

Keywords
Cryptography, RSA Algorithm, Encryption, Decryption, Security.

Introduction

The term cryptography means to provide a confidentiality to a message or data that is send over a network. Cryptography is derived from Greek which stands for secret writing. The main objective of the cryptography is to provide the confidentiality. . The two important words used in cryptography are encryption and decryption. Encryption means to encrypt a secret message using a key. Decryption means to decrypt the encrypted secret message to get the original message. There are two kinds of cryptographic measures to gain these objectives: Symmetric Cryptography and Asymmetric Cryptography. There are many algorithms to provide the security like AES, DES, RSA, Railfence, DSA, Elgamal. AES, DES, Railfence comes under symmetric cryptography and RSA, DSA, Elgamal comes under Asymmetric cryptography. The main objective of these algorithms is to provide a secure way of communication over a network. For an asymmetric cryptography there is a key distribution happens between the users on the both ends. Key distribution means the transfer of keys between the end users.

Different Approaches of Cryptography:

Asymmetric Cryptography:

Asymmetric algorithms basically deal with two keys. One is the public key and the other is the private key. In these asymmetric algorithms the message will be encrypted through the public key, which is only known to the user, and the encrypted message will be sent to the receiver. The receiver will decrypt the encrypted message with the sender's private key. Public key will be announced publicly to every user. So, here the security is mainly involved to the private key. Here the encryption will be done using the sender's public key and the decryption will be done by the private key.

Symmetric Cryptography:

Symmetric algorithm deals with only one shared key. The Shared key will be used both for encryption and the decryption. The sender encrypts the message with the shared key and sends the encrypted message to the receiver. The receiver decrypts the message with the shared key to decrypt the message. Here if the key is compromised then the attack will be easy. So, here the security is mainly involved with the confidentiality with the shared key. It is a two way algorithm as it deals with only one key that is shared between the sender and the receiver. It is otherwise called as secure-key algorithm. The only advantage is the encryption of the data will be stronger.

Materials and Methods

Overview of RSA Algorithm:

RSA is an asymmetric cryptographic algorithm used by the computer devices for the encryption and decryption of the message for the secure transfer and it is one of the initial systems. The most important properties of public

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

key encryption scheme are: Public and private keys are used for encryption and decryption hence this is a property that is applicable for this algorithm than the symmetric encryption algorithm. The receiver will needs a unique key for the decryption and that key is referred as a private key and the receiver needs a unique key for encryption and that key is referred as a public key. This algorithm is complex by the attackers to identify the plain text from the cipher text and the public key. Even though this public key and private key are generated mathematically it is not such a easy to identify the private key from the public key.

The security of RSA relies upon the qualities of two separate capacities. The RSA cryptosystem is most famous open key cryptosystem quality of which depends on the reasonable trouble of calculating the simple huge numbers.

– Encryption Function

– Key Generation

If both of these two capacities are demonstrated non one-way, at that point RSA will be broken. Actually, on the off chance that a strategy for calculating productively is created, RSA will never again be sheltered. The quality of RSA encryption radically goes down against assaults if the number p and q are not substantial primes or potentially picked open key e is a modest number.

Proposed Model

As we know that the RSA algorithm is mainly involved with private key. So, we are going to provide the security for the private key. Our model is that we are going to provide a password that combines two parts. One part will be directly known with the sender and the other part will be generated by the algorithm. This means user will generate half password and the remaining half will be generated by the algorithm. This password will be send to the user before encrypting the message and only if that validates the user can proceed further otherwise the user can't proceed. So by this model we can increase the security of the Private key. So, even if the private key is known to the hacker he needs another step to dug in. This slightly improves the complexity but it will rather increase the security in other hand. This algorithm has 3 modules

1.Password Generation

2.Validation

3.RSA Algorithm.

Password Generation:

Here the algorithm generated password will be created. The password will be generated randomly by importing the module called random. The password will be generated by using all the ASCII characters , including everything, so that it will not be easy to crack. The algorithm generated password along with the user password will be added and it will be stored safely into a file.

Validation:

Here the file in which the password is stored will be sent to the user by using an file sharing protocol and then the user takes that password and he will try to authenticate with that credentials if the password is correct it will be validated and can send the message or data. If the credentials don't match the validation doesn't takes place. If the validation is successful the algorithm will write the certain command into another file.

RSA Algorithm:

Here before the use of the RSA algorithm the file that is created in the validation module will be read by the algorithm if the command matches with required one then the user can be able to use the RSA algorithm and can encrypt the data and can establish a connection and sends that encrypted data to the receiver. The receiver will decrypt the data using the private key.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

By following these modules the user can send the message securely to the receiver. There will be another security layer on the message that we are encrypting so it will be really difficult for someone to see the message other than the sender.

Overview of New Model:

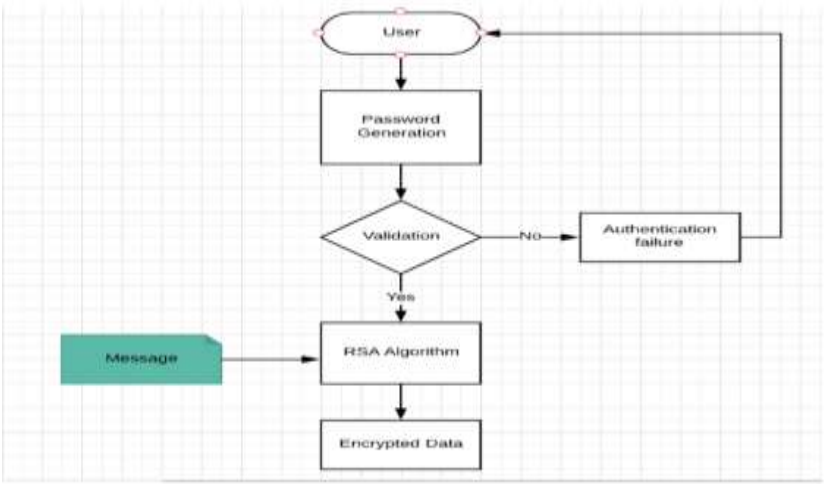
As we know that the RSA algorithm deals with two keys. If the private key is compromised then there is no matter of encryption and decryption. So, this proposed model, in password generation module, the length of the password generated is of variable length. That means the password that is generated will be of some finite length but the length of the password is not known even to the user. So, even for the hacker to attack with a brute force attack it takes a lot of time. Because the brute force attack is mainly about finding different patterns which will be easy only if the length is known. So the hacker cannot hack this. And the other thing is the remaining part of the password will be generated by the user. Hacker needs to know the password generated by modified algorithm, user input password and the part how these passwords are integrated.

In the integration of the password there are three cases:

1. In the beginning :
   Here the algorithm generated password will be in the front followed by the user input password. For example, if the algorithm generated password is xdf54# and the user input password is 234gd then the total password after integrating in the beginning is xdf54#234gd.
2. In the end :
   Here the user input password will be in the front followed by the algorithm generated password. For example, if the algorithm generated password is xdf54# and the user input password is 234gd then the total password after integrating in the beginning is 234gdxdf54#.
3. In the middle :
   Here one password lies within the other password. The user input password will be placed in the middle of the algorithm generated password. For example, if the algorithm generated password is xdf54# and the user input password is 234gd then the total password after integrating in the beginning is xdf234gd54#.

So, we can observe that the security of the modified RSA algorithm is better than the RSA algorithm.

Flow Graph



First the user will go for the generation of the password. In this the generation of password the user will manually enter the password he wants to keep. The algorithm will automatically generate the other half part with some variable length. This will be recorded somewhere in a file and that file will be accesses only to the preferred user.

The user will check for that one time password that is in the file and the user will validate the password.

In the validation part the user will go to that validation module and there the user will type the password. If that password matches with the password that is present in the database then the program will send one command to another file that is present somewhere on the database.

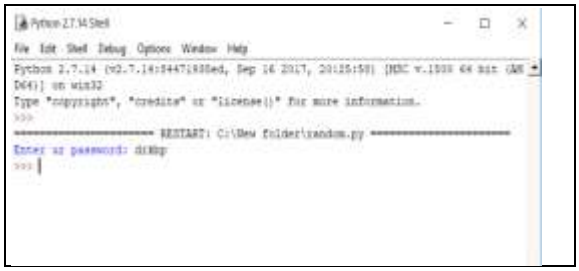
In the RSA module first thing it will do is the checking part. It checks if the user is the one who has right to send the message to the receiver. It checks basing on the command that is generated by the validation module.

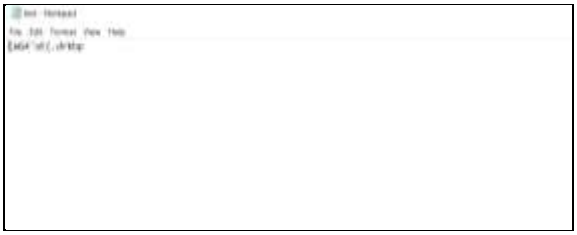
If the validation is “TRUE” then the user can type the message he wants to send and can encrypt the data and can send it to the receiver.

If the validation is “FALSE “then the user cannot access. So, the user will get the authentication failure message.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Results and Discussion
For Testcase 1:





  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Discussion about the Test case:

For Testcase:

In the first figure the algorithm asks the user to manually add the password the user wants to append. Here the user can select the characters from 0-9,a-z,A-Z,special characters. In the same module the algorithm will automatically add some characters to the user added password from some variable length.

In the second figure, the algorithm will automatically sends the password, both algorithm generated and user generated to a file. Only the authenticated user can see this and can know the password. This password changes every time.

In the third figure, the validation of the password takes place the password that is there in the file, which is known only to the user will authenticate it and then it will sends some commands if the validation is successful or the validation is not successful.

In the fourth figure, the commands will be sending to a text file. True, this is the command that will write in the file if the user is the right person to validate. False, this is the command that will write in the file if the user is not the right authenticator.

In the Last segment, Here the algorithm will take the input from the file which contains the commands and it will take the input from it. If the command is True only then the RSA algorithm happens. Here as you can see the message is taken from the user as an input that means he is the valid user. So, then it will authenticate the message and it will encrypt with the public key of the receiver and sends the encrypted text to the receiver.

In the Last segment, Here the algorithm will take the input from the file which contains the commands and it will take the input from it. Here we can clearly see that the as he/she is not the right person to authenticate so it says sorry message and the process stops. The process stops because of the failure case as it saves a lot of time.

Conclusion

In this Paper, We proposed a hybrid encryption approach by integrating our own module to the defined RSA algorithm. This will improve the security of the in various real time applications like Bank accounts, Social media, Secure texting In an android mobiles etc.,. Not only will these it enhance the security of any application that works with the sharing of a key. We have taken two factor authentications into our criteria to improve the security of the RSA algorithm. I can say that it improves security but, if we need security it takes some time to process. So, we can surely say that we improved the security of the RSA algorithm. Comparing with the normal RSA algorithm this hybrid algorithm will enhance more security. It takes bit time more than the normal RSA algorithm because we have added two modules to it to increase the security. So, by integrating this approach to the RSA algorithm the security, confidentiality is improved.

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory, Nov. 1976,22: 644-654.

[2] AtulKahate, “Cryptography and Network Security”, ISBN-10:007-0648239, Tata McGraw-Hill Publishing Company Limited, India, Second Edition, pages 38-62,152165,205-240.

[3] R. Rivest,A. Shamir, L. Adleman, "A Method for Obtaining Digital for Signatures and Public-Key Cryptosystems", Communications of the ACM, vol. 21 (2), pp. 120-126, 1978.

[4] William Stallings, “Cryptography and Network Security”, ISBN 817758011-6, Pearson Education, Third Edition, pages 42-62,121144,253-297.

[5] Sattar J Aboud, “An Efficient Method for Attack RSA Scheme”, 978- 14244-44571/09/$25.00 IEEE, 2009.

[6] Kolla Bhanu Prakash, Dorai Rangaswamy M.A. (2016), “ContentExtraction of Biological Datasets Using Soft Computing Techniques”, Journal of Medical Imaging and Health Informatics, American Scientific Publishers, Vol. 6, 932- 936.

[7] Prakash, K.B., Dorai Rangaswamy, M.A., Ananthan, T.V., Rajavarman, V.N. "Information extraction in unstructured multilingual web documents", 2015, Indian Journal of Science and Technology, 8(16),54252.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495