Implementing Security Framework for Cloud based IOT Network

Radhika Rani Chintala, Haritha Kallepalli and Jahnavi Kotapati

May 19, 2021

Implementing Security Framework for Cloud based IOT Network

Radhika Rani Chintala, Kallepalli Haritha, Kotapati Jahnavi

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

***Abstract*— The Internet of Things (IOT) is a rapidly growing technology. Due to its networked nature and rapid implementation in various fields, "SECURITY" is taken into account a primary challenge. As there are many security vulnerabilities in the existing IOT framework there is a possibility of many security threats. This paper talks about the security loop holes in IOT devices and proposes a security framework technique which is based on Public Key Infrastructure certification mechanism. This framework represents how to authenticate both the IOT device and therefore the user through a cloud system using digital certificates.**

Keywords—IoT Security, Framework Layers, Security Issues ,Public Key Infrastructure, RSA Algorithm, Issue Of digital certificate, Implementation.

I.INTRODUCTION

In an organization, there can be any IoT device which is interlinked with sensors and this IoT device can have the ability to send and receive the information over the entire organization without any manual interaction happening in between. Due to this IoT technology the devices are able to have an intermediate connection to share the data among themselves in a particular secured network. IoT is an idea that interfaces all the gadgets to the web and let them speak with one another over the web. IoT is a very large organization of associated gadgets – all of which assemble and share information about how they are utilized and the conditions in which they are worked. IoT is attempting to extend the communication in human-i.e associate, contribute and team up to things. There are some real time examples where the concept of Internet Of Things is being used. For example there are connected cars in which IoT helps the car organizations to handle charging, parking, protection, and other requirements of the organizations naturally. IoT is also used in building Smart cities and smart homes. Smart city ensure the solution for all the problems which includes the solution for managing the traffic and the solution for to eradicate the problem of water distribution, and also provides a solution for unused materials management, and many. The Smart home technology ensures that there is a connectivity between required devices inside our houses. These include smoke detectors, house hold appliances, electrical devices, windows, locking system for doors and many more.

There are many advantages of using Internet Of Things which includes reduction of the development cost, and increase of efficiency and productivity in the business domain, the easy accessibility to the customers , and mobility. Using IoT any communication in the organization can be held very smooth which increases the productivity in the offices, small scale and large scale industries.

In this paper we are going to discuss about the existing framework layer of IoT technology and the importance of public key cryptography and digital certificate to prevail security and we are going to propose a modified RSA algorithm and a three way secured framework for IoT devices through which the security issues will be reduced.

II.BACKGROUND STUDY

Public Key Infrastructure

Public Key Infrastructure (PKI) is an innovation for the authentication of the clients and their required gadgets in this computerized world. The essential thought is to have at least one or more trusted parties to carefully sign the records ensuring that a specific cryptographic key is allocated to any specific client or their gadget. This key would then be able to be utilized as an identity for the client in advanced organizations.

The clients and their gadgets that have been assigned with certain keys are called as an "entity" in IoT. All in all, anything can be related with a key that it can use as the "identity" of that specific device. Other than a client or gadget, this key may be assigned to anything which includes a program or any component. The reason for a PKI is to safely connect a key with the respective device.

The client or the user should sign and validate the document and this document also consists of the key that is required to be assigned to the device. This is known as the "Certificate Authority (CA)". The "certificate authority" likewise has a cryptographic key that it utilizes for signing the required records. These documents which are having the sign of the client or user as well as the cryptographic key are called as the "certificates" which are required for the authentication purposes. In reality, the usage of these certificate authorities is very high and every PC and other devices undergo hundreds of certificates by default.

A public key framework depends on "digital signature" innovation, which utilizes public key cryptography. The fundamental thought is that the mystery key of every device is just known by that entity and is utilized for signing. This key is known as the private key. There is another key which has been obtained from it, called the public key, which is utilized for confirming the signatures yet can't be utilized to sign. This public key is made accessible to anybody, and this public key is also used and included in the certificate document.

PKI functions on asymmetric key methodology: a primary key and a public key. The private key can only be accessed by the owner of a digital certificate, and the client can share their public key to authorised users. A certificate is actually used to share this public key information to the respective users required. Private and public PKI keys must work together. A file that's encrypted by the private key can only be decrypted by the general public key, and the other way around . If the general public key can only decrypt the file that has been encrypted by the private key, having the ability to decrypt that file assures that the intended receiver and sender took part within the informational transaction.

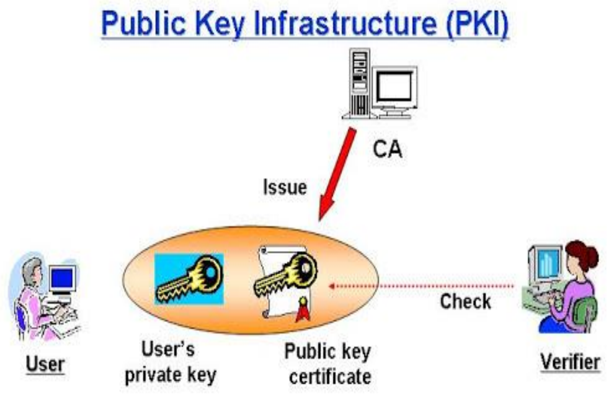


Figure 1.0: Public Key Infrastructure Working

III. LITERATURE SURVEY

In terms of security, authentication of IoT devices is a vital step in key validation and key sharing, otherwise systems are hospitable attacks like a man-in-the-middle. samples of protocols which will help with key sharing is that the Diffie-Hellman key generation protocol proposed by Whitefield Diffie and Martin Hellman. it's one among the components which permit secure communication for a good range of protocols like , SSH, OpenPGP, HTTPS. These protocols are utilized in browsers, mobile and desktop applications and enabled secure connection on Internet.

Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh in the paper [1], have highlighted this issue in their proposed study. They have focussed more on the security breaches in the existing technologies and they focussed more on explaining the different malware attacks that are possible in IoT devices including the android. They have also discussed the challenges which includes vulnerability problems and that are being faced in the present technology.

Various authorization and authentication issues are discussed . The authors provide different light weight cryptographic studies and the backdoor analysis in IoT devices.

Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, in the paper [2] which is a survey based study, authors have discussed several issues of the securities and vulnerabilities that exist during a layered architecture of an IoT infrastructure. They have explained the entire three layered architecture of IoT and have focussed on the vulnerabilities that are possible in each and every layer. They have also explained the security principles that are to be applied based on confidentiality, integrity , heterogeneity etc.. They have also discussed about the implementation of IoT in the future emerging 5G protocol.

Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, in paper [3], the authors have analysed various layered architectures of an IoT layered framework. They highlighted security vulnerabilities within three primary IoT layers: Perception, Transportation, and Application. Authors highlighted several threats on these layers, such as, Physical Attacks, Impersonation Attacks, DoS Attacks, Data Leakage, Malicious Code Injections etc. They also highlighted several security measures that are to be taken in each layer to avoid these security issues which includes RFID security measures , IPSec security channel, physical security scheme etc.

Whitmore, A.; Agarwal, A.; Da Xu, L in paper [16] highlighted several security challenges in various IoT networks including: Architecture Dependencies, Big Data, Robustness, and Privacy. The authors also highlighted the various applications of IOT in real time and the future scope or implementations in the technology

Sowmya, K. V., & Sastry, J. K. R in paper [22] have highlighted the basic issues that have an impact on the performance of IoT systems and enhancing the performance.

IV.RESEARCH GAP

As quoted in the literature survey there are many studies that address the security and privacy issues in the different layers of IOT implementation but due to the lack of more emphasis on a structured and robust security architecture, there are many security and privacy issues to be addressed. According to the understanding , there are many authentication and intrusion issues that can be faced in IOT implementation.

V. PROBLEM STATEMENT

As there are many security issues that can be faced when implementing IOT systems we have proposed a framework which can eliminate the security issues. In this framework when a new user or any new IOT device wants to exchange data they are first registered in the cloud services through digital certificates and then only legit and verified devices or users are allowed furtherly.

FRAMEWORK LAYERS IN IOT DEVICES

There are three different important layers in the IoT technology:

1) Perception Layer
2) Transportation Layer
3) Application Layer

Perception layer:

The perception layer is that the physical layer, which has sensors which are used to sense the information and gather them for various purposes. It senses some physical parameters or identifies other smart objects within the environment. This layer features are utilized for communicating and processing of sensor information.

Transportation layer:

Transport Layer provides transparent transfer of knowledge between end users, This layer provides the transfer of the data services to all the above layers.

Application layer:

The critical goal of Internet of things (IoT) is to make sure effective communication between objects the appliance layer is liable for providing services and determines a group of protocols for message passing at the application level.

DIGITAL CERTIFICATES

Digital certificates are the digital documents that contain the identity of the clients or users along with their cryptographic keys, (one public and one private), which will be wanted to encrypt and sign information digitally. the most purpose of the digital certificate is to make sure that the general public key contained within the certificate belongs to the entity to which the certificate was issued, in other words, to verify that an individual sending a message is who he or she claims to be, and to then provide the message receiver with the means to encode a reply back to the sender.

Encryption techniques using public and private keys require a public-key infrastructure (PKI) to support the distribution and identification of public keys. Messages are often encrypted with either the general public or the private key then decrypted with the opposite key. Without certificates, one could send data encrypted with the private key and therefore the public key would be wont to decrypt the info , but there would be no assurance that the information was originated by anybody . All the receiver would know is that a legitimate key pair was used. In essence, a Certificate Authority or CA then may be a commonly trusted third party that's relied upon to verify the matching of public keys to identity, e-mail name, or other such information.

The Certificate Authority (CA)provide us the information in just one certificate which includes the public keys of the respective user and the encryption algorithms that are used to encrypt the data, the user or clients information , the digital certificate of the Certificate Authority which is already verified and validated , and the validity time period of that certificate. These "Digital Certificates" are required for the digital transactions which includes e-mail, electronic funds transfers and many more.

UNDERSTANDING RSA ALGORITHM

The RSA algorithm is that the basis of a cryptosystem -- a set of cryptographic algorithms that are utilized for security administrations or purposes - which empowers public key encryption and is widely wont to secure sensitive data, particularly when it's being sent over an insecure network like the web .RSA was first designed in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman.

Public key cryptography uses two different but interlinked keys –in which one is . the general public key are often shared with everyone, whereas the private key must be kept secret.

In RSA cryptography, both the general public and therefore the private keys can encrypt a message; the other key from the one wont to encrypt a message is employed to decrypt it. This feature is the main cause why RSA has become the foremost widely used asymmetric algorithm: It avails a way to assure the confidentiality, integrity, authenticity, and data storage.

Many protocols which include secure shell, OpenPGP, S/MIME, and SSL/TLS believe RSA for encrypting and digital signature functions. it's also utilized in software programs -- browsers are a clear example, as they have to determine a secure connection over an insecure network, just like the internet, or verifying a digital signature. RSA signature verification is one among the foremost commonly performed operations in network-connected systems.

A. Existing Algorithm:

1)Select p, q any two prime nos. $p \neq q$

2)Calculate n = p x q

3)Calculate Ø(n) = (p−1) x (q−1)

4)Select integer e such GCD

GCD(Ø (n),e) =1 ; 1< e< Ø(n)

5)Calculate d such d ≡ e−1(mod Ø (n))

6)Public key PU = [e, n]

7)Private key PR = [d, n]

8)Consider plain text M , M < n

9)Find cipher of plain text by

C = M^e mod n

10)Transmit the coded message to receiver by sender

11)Find plain text from cipher by receiver using

M = C^d mod n

LIMITATIONS FOR EXISTING RSA ALGORITHM

1) As is transmitted ‘n’ in public key its factor can be discovered by hit and trail, because of which e and d can discovered effectively and security remainder of RSA calculation get decreased.

2) The programmers or intruders can encrypt plain content utilizing public key and get original confidential secret message.

To avoid the security issues in the existing RSA Algorithm we have provided a modified algorithm to enhance the security of RSA Algorithm

MODIFIED RSA ALGORITHM

1) We use three random prime numbers rather than two prime random number for calculating ‘n’.

2)Here we pass value of ‘x’ rather than ‘n’ publicly key and personal key.

3)This approach is safer than RSA algorithm because the public key and personal key exponent are often found only by knowing the three prime numbers p, q, and r and which may be known only through ‘n’, but ‘n’ isn't transmitted in any key .

Thus it's very difficult to understand e and d hence encrypted message cannot read easily.

2) Modified Algorithm:

1)Select p, q and r any three prime nos. $p \neq q \neq r$

2)Calculate n = p x q x r Its length is vital length which is typically expressed in bits.

3)Calculate Ø(n)= (p−1) x (q−1) x (r−1)

4)Calculate integer e which is predicated on

$$\sqrt{n} < e < Ø(n)$$

- GCD(Ø (n),e) =1 i.e. e and Ø(n) are co prime
- e is brief bit length and little hamming weight

5) Compute X (to replace n)

- If p>q then consider X such

$$n - p < X < n \text{ and } GCD(X , n) = 1$$

- If p<q then consider X such that

$$n - q < X < = n \text{ and } GCD(X , n) =1$$

6)Calculate d such that d ≡ e−1(mod Ø (n))

7)Now the Public key PU = [e, X]

8)Now the Private key PR = [d, X]

9)Consider plain text M, M < n

10)Find cipher of plain text by

$$C = M\text{^}e \bmod X$$

11)Transmit the coded message to receiver by sender

12)Find plain text from cipher by receiver

ADVANTAGES OF MODIFIED RSA ALGORITHM

1) It takes longer time to get keys in RSA algorithm than in Modified RSA algorithm. Therefore, in terms of the key generation speed, Modified RSA algorithm is best than RSA algorithm.

2) It gives more security in modified RSA algorithm than in RSA algorithm. Therefore, in terms of security level. Modified RSA algorithm is best than RSA algorithm.

3)It takes longer time to encrypt text in Modified RSA algorithm than in RSA algorithm. Therefore, in terms of message encryption speed, RSA algorithm is best than Modified RSA algorithm.

4)It takes longer time to decrypt text in Modified RSA algorithm than in RSA algorithm. Therefore, in terms of decryption speed, RSA algorithm is best than Modified RSA algorithm.

5)The total "execution time" of both algorithms takes near Modified RSA about same time and storage requirement for plain text and RSA cipher text under both the algorithm is additionally same

VII. PROPOSED WORK

There are various security issues that may cause the existing IoT framework vulnerable to threats . As there is no framework which is more structured and robust thre are still many privacy issues . In IoT infrastructure there is a maximum possibility of threats due to poor authentication , access control and some intrusion attacks. In our proposed framework, we've focused on these security issues and proposed a secure framework which may provide a facility to register an IoT device using Digital Certificate also as user to the cloud server. After completing registration process, only a real , registered user can only have access to use an IoT device available within the network.

As illustrated in Fig. 4.0, the proposed framework is at its preliminary stage. The framework is predicated on PKI system that manages certificates, systems and application to uniquely identify users, services and devices that are getting used during a network. An efficient PKI should be transparent and ready to achieve security principles, specially authentication and data integrity. This framework consists of IoT devices, users, cloud, certification authority and registration authority. Before communication with one another , users and IoT devices got to be registered to the cloud through their verified Digital Certificate.

These certificates are often obtained through the RA, or are often derived from trusted application certificates (that are anchored through an RA). Here we propose that the cloud application is authenticated through PKI, but that the cloud application then issues certificates for devices and users

Thus the cloud application further issues separate certificate for device and for users these certificates are represented as (D1, D2… Dn) and (Uc1, Uc2…Ucn) simultaneously. Third and most vital entity during this framework may be a centralized cloud, which stores and indexes all the certificates with their respective keys (Dc1, Dc2… Dcn) or (Uc1, Uc2… Ucn) in its centralized storage. A Registration authority provides the PKI anchor which is further anchored through a certificate issued by a CA.

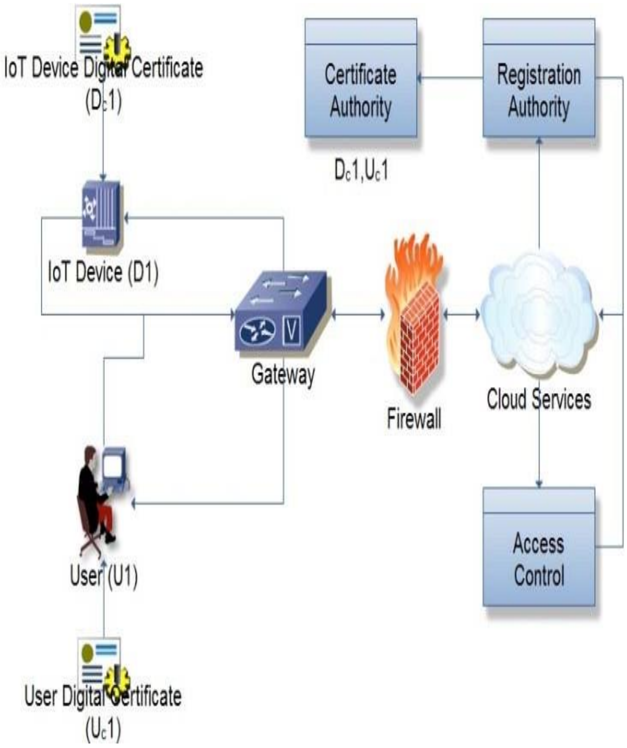


Figure. 4.0. Three-way Security Framework for Cloud based IoT Network

Abbreviations	Descriptions
CA	Certification Authority
RA	Registration Authority
D1	IoT Device 1
D2	IoT Device 2
Dc1	Digital Certificate of device 1
U1	User 1
Uc1	Digital Certificate of User 1
IoT	Internet of Things
PKI	Public Key Infrastructure

Table 1.0:Abbrevations used in Figure 3.0

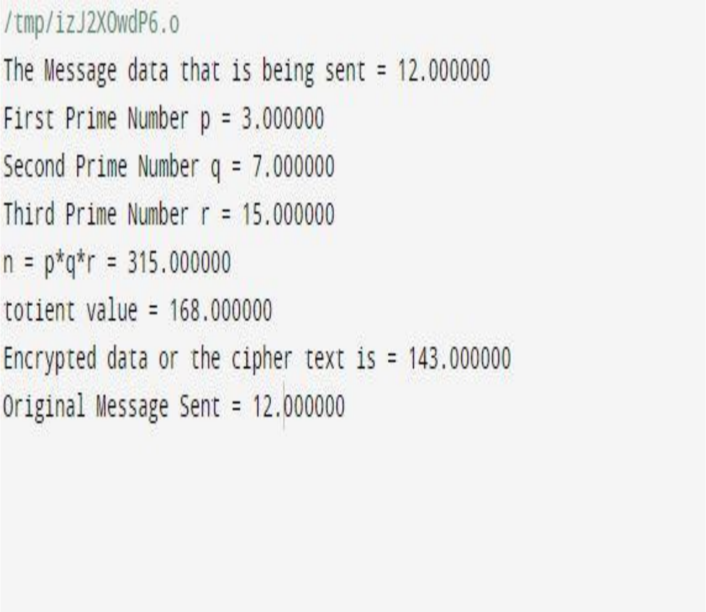
When a user registers, the cloud application verifies the user identity (e.g. by employing a second factor like SMS or email) before generating a certificate to store within the centralized cloud and issuing the certificate to the user’s end-application through a suitably protected TLS channel. Similarly, a tool features a unique certificate issued by the seller (here we assume the cloud and device vendor are the same). The device certificate and unique device identifier (included within the certificate) can then be installed before shipping. The cloud stores and indexes all certificates, devices and users.

When the user wishes to use the device, the cloud application verifies the user certificate from the cloud index and check the access control which is defined within the management system.

Public key certificates require the subsequent services: a repository for certificates; creation and revocation of certificates; and, management of key histories. The management system contains: key backup/recovery; systems for non-repudiation of digital signatures; and, automatic updates of key pairs and certificates. These digital certificates include information like public key, name, and expiry date of the certificate. The Certification authority represents the foremost critical part in PKI because it acts as a source of trust and supply services to assure a private level of authenticity to the entities when exchanging information.

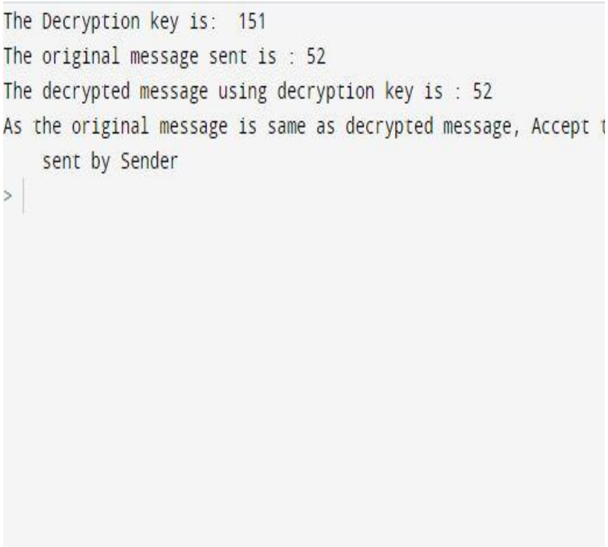
The proposed security framework is predicted to be robust and highly secure because it has covered the first gap that exist on the appliance layer of an IoT infrastructure.

VIII. RESULTS



```
/tmp/izJ2XOwdP6.o
The Message data that is being sent = 12.000000
First Prime Number p = 3.000000
Second Prime Number q = 7.000000
Third Prime Number r = 15.000000
n = p*q*r = 315.000000
totient value = 168.000000
Encrypted data or the cipher text is = 143.000000
Original Message Sent = 12.000000
```

Figure 3.0: Implementation Results For Modified RSA Algorithm



```
The Decryption key is:  151
The original message sent is : 52
The decrypted message using decryption key is : 52
As the original message is same as decrypted message, Accept t
    sent by Sender
>
```

Figure 4.0: Implementation Results for Modified RSA Issue and Verification of Digital Signature

IX.ANALYSIS GRAPH

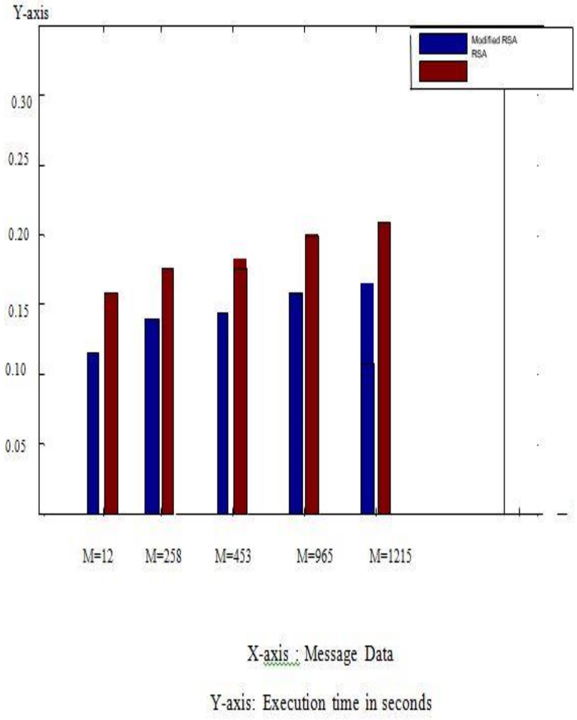


Figure 5.0: Total execution time comparison between RSA and Modified RSA

Message Data	***Modified RSA execution time***	***RSA execution time***
M=12	*0.103*	*0.152*
M=258	*0.146*	*0.177*
M=453	*0.148*	*0.181*
M=965	*0.175*	*0.209*
M=1215	*0.183*	*0.216*

Table 2.0 : Message Data and Total execution time comparison between RSA and Modified RSA

X. FUTURE SCOPE

The proposed structure is the primary stage of development. In the upcoming studies there can be a possibility to analyse the authentication protocols that can be used in the proposed framework and can implement this structure in real time scenario with the required analysis and results.

XI. CONCLUSION

In this paper we have presented a security framework which is predicated on PKI infrastructure and implemented on IoT network. especially the work here concentrates on the three- way system authentication: device-to-cloud; user-to-cloud; and thus user-to-device.

The proposed Three-way IoT Authentication Framework is at its preliminary development stage. In our upcoming studies, we aim to present detailed investigations into the specified authentication phases and authentication protocols with sufficient results and outcomes to verify and validate out proposed work.

XII. REFERENCES

[1] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," *YOP : 2014 Publication : IEEE*

[2] Kai Zhao, Lina Ge, "A Survey on the Internet of Things Security" *YOP:2013 Publication IEEE*

[3] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan "Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures" *YOP : 2015 Publication : IEEE*

[4] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on „ n ‟ prime numbers," vol. 1, no. 2, pp. 63–66, 2013

[5] "A Critical Analysis on the Security Concerns of Internet of Things (loT)", *Perception*, vol. 111, 2015.

[6] T. ElGamal, ‘‘A public key cryptosystem and a signature scheme based on discrete logarithms,’’ IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[7] R. L. Rivest, A. Shamir, and L. Adleman, ‘‘A method for obtaining digital signatures and public-key cryptosystems,’’ Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978

[8] A. H. Al-Hamami and I. A. Aldariseh, "Enhanced method for RSA cryptosystem algorithm," Proc. - 2012 Int. Conf. Adv. Comput. Sci. Appl. Technol. ACSAT 2012, pp. 402–408, 2013.

[9] B. P. U. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on „ n ‟ prime numbers," vol. 1, no. 2, pp. 63–66, 2013

[10] A. K. Hussain, "A Modified RSA Algorithm for Security Enhancement and Redundant Messages Elimination Using K-Nearest Neighbor Algorithm," vol. 2, no. 1, pp. 159–163, 2015

[11] D. Jagadiswary and D. Saraswady, "Estimation of Modified RSA Cryptosystem with Hyper Image Encryption Algorithm," vol. 10, no. February, pp. 1–5, 2017

[12] S. Chokhani, W. Ford. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527[S], 1999-03.

[13] N. Priya and M. Kannan, "Comparative Study of RSA and Encryption," International Journal Of Engineering And Computer Science, vol. 6, no. 1, pp. 19867 - 19871, January 2017

[14] H. Chen, X. Shen, and Y. Lv, ‘‘A new digital signature algorithm’’ J. Softw., vol. 5, no. 3, pp. 320–327, Mar. 2010

[15] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things" in Future

Internet-FIS 2008 Lecture Notes in Computer Science Vol. 5468, 2009, pp 14-28.

[16] Whitmore, A.; Agarwal, A.; Da Xu, L. The Internet of Things—A survey of topics and trends. Inf. Syst. Front.2015,17, 261–274

[17Y., Dong, X., & Sun, W. Chang, "Influence of characteristics of the Internet of Things on consumer purchase intention," Social Behavior and Personality: an international journal, vol. 42, no. 2, pp. 321-330, 2014.

[18] The Public-Key Cryptography Standards ", RSA Data Security Inc., November 1993

[19] RSA Data Security, "Understanding PKI". 1999

[20] "The internet of things: A survey", *Computer Networks*, vol. 54, pp, 2010.

[21] Pavan Kumar, T., Hemanth Krishna, R., Sai krishna, M., & Meghana,J. (2018). Smart home system based on IoT. International Journal of Engineering and Technology(UAE), 7(2.8 Special Issue 8), 500-502.

[22] Sowmya, K. V., & Sastry, J. K. R. (2018). Performance evaluation of IOT systems - basic issues. International Journal of Engineering and Technology(UAE), 7(2), 131-137.

[23] Sri Lakshmi, K. M., Sairam, P., Yeswanth, V., & Akhila, A. (2018). IOT based monitoring of household electricity appliances. International Journal of Engineering and Technology(UAE), 7(2.32 Special Issue 32), 174-176.