A Heuristic Approach for Securing Data of IoT Devices using MAC Address of the Devices and 3-DES Method

[1]Rashmi R Sonth, [2]Pranamya Y R, [3]Dr Deepak G, [4]Harish Kumar N
[1]Student, [2]Student, [3]Assistant Professor, [4]Asssistant Professor
[1]Computer science and Engineering,
[1]Dayananda sagar college of engineering, Bengaluru, India

Abstract : In this 21st century IoT is one of the exploding technologies in the consumer and business environments. As more and more devices are getting connected to the network, the urge of device authentication is growing high due to the requirement of secure communication with each other as well as the backend infrastructure. For its value to be realized any IoT device should first respect the confidentiality between the users. In this paper, we have proposed a authentication approach that works in two levels to provide a high level of security and surety for the data transmitted. We have presented asymmetric encryption for the data using public and private keys. Further, the unique MAC addresses of connected IoT devices has been exploited and encrypted using Triple DES method which acts as a second layer lock to increase the confidentiality of data.

IndexTerms **- Internet of Things, Authentication, Triple DES, Asymmetric encryption.**

I. INTRODUCTION

The Internet of Things (IoT) is a large network of computing devices that are embodied with unique id's (UIDs) and have the capacity to transmit and receive data in the network without any outside consent. An IoT ecosystem comprises of smart devices which are capable of receiving, sending and acting on the received data from environments using the embedded processors, sensors and communication hardware. IoT sensors share the sensed data through an IoT gateway or other devices by either analyzing it locally or sending it to cloud. The impact of IoT on user's lives is rapidly increasing as the cost of instrumenting physical devices with sensors and connecting them to other devices continues to drop.

Device authentication is a process of uniquely identifying the device based on an unique device ID. There are various methods used for authentication – Email authentication, password authentication, social network authentication, biometrics, two factor authentications, and many more. Picking the right authentication method is crucial for the job of security. Encryption is one of the methods that we have used for authentication. Encryption is a process of encoding any personal and private data or information so that only authorized users can access the data. There are two methods for encryption and a various algorithms are used during encryption. In Symmetric encryption, the same key is used for encryption as well as decryption whereas in case of Asymmetric encryption, a public and a private key pair is used each at sender's site and receiver's site. A number of algorithms like RSA, AES, DES, Blowfish, Twofish, etc. Are used for the process of encryption – decryption. In this paper, we have used a two factor authentication to provide a high amount of security. Two factor authentications sometimes called two-step verification or dual factor authentication is a way of providing two layer protection using two different authentication techniques for the sake of providing better level of safety. As the first authentication technique, we use an asymmetric algorithm to encrypt the data using receiver's public key. This encrypted data is recovered only by an authorized receiver who uses his private key for decryption. To provide device authentication, further, the encrypted data is further passed through Triple DES algorithm at sender's site and decrypted using the same algorithm at the receiver's site. As the MAC address is unique for an IoT device, we use the MAC address as the unique key for encryption and decryption process. The communicating devices need to exchange their MAC addresses beforehand by a private channel using which three keys – K1, K2, K3 are generated that encrypt – decrypt the data.

Literature survey is carried in Section 2. A brief description about the proposed architecture is elaborated in Section 3. Section 4 deliberates about the results obtained using the proposed approach. Conclusion is discussed in the last section.

II. LITERATURE SURVEY

Win, Yoshihisa et.al[1] presented a paper on Multi-receiver Encryption using Lightweight cryptographic system via Mutual Authentication. In order to avoid the revelation of his/her own data directly to the third party which is trusted, the proposed approach adopts public keys generated by device. To perform mutual authentication, external proxy is allowed to generate identity-based keys which are partial private to users. Proxy runs an algorithm which generates parameters with its secret master keys. To avoid escrow problem on key, this system allows the users run above algorithm to produce private key and public key.
Daddala , Wang, H and Javaid[2] developed an architecture on customized encryption algorithm to provide secure communication and authentication between devices. A customized encryption algorithm and a scheme to authenticate safely and

transfer information have been proposed. The algorithm provides slightly manipulated version of **Advanced Encryption Standard (AES)** and hence a new protocol is used for developing a key. The devices which communicate must own public keys of the associated devices they want to communicate with. The difficult feature of the algorithm is to ensure safe communication of data as attackers will not be able to decrypt the text in spite of having keys to access.

Guntuku and Pasupuleti S. K[3] proposed an authentication technique for IoT devices. Here, for security and integrity a special type of cryptography and chaotic maps for authentication is employed. This system first guarantees the authentication among tag, scanner device and cloud. Then security and Integrity of information is achieved during the communication through encryption based on elliptic curve and hashing system correspondingly.

Shaila Sharmeen , Shamsul Huda et.al[4] proposed a paper that analyzes the malware threats which are aimed on the devices and are used in industrial mobile-IoT networks. The designed new system is evaluated on dynamic ,static and hybrid analysis on data set which is fundamental in nature and selecting features , and extraction techniques and the accuracy obtained by the above methods are compared.

Sravani Challa, Ashok Kumar Das et.al[5] has introduced a system which is verified for security using **Burrows-abadi-Needham logic**. A safe and secure signature-based authentication is projected here. The proposed system comprises of BAN logic and informal analysis which proves the scheme is protected. Hence the author concludes his scheme is one of efficient in terms of both computation costs and communication.

Abdulaziz Aldaejand et.al[6] focused on the concept of improving cyber security against DDoS attacks for IOT devices and its networks. The proposed approach is based on above problems that drop the network performance. DDoS comprises of group attacker nodes and targets the object to prevent permissible users from accessing the resources of a system. IP systems actively guard and prevent the intrusions detected by IDS (Intrusion detection system) technique. The IDS reports are the source of the proposed system.

Trusit shah and venkatesan[7] proposed a solution to overwhelm the vulnerabilities confronted by the single password-based authentication method. They have proposed a multi-key based mutual authentication, where a secret key is exchanged between the IOT device and server and it is termed as a protected vault, which is a collection of equal sized keys. After every successful communication session, secure vault shares the content between IoT server and device.

Qian xu, Pinyi ren et.al[8] proposed a solution to overcome the eaves dropping with unknown number and locations for relay communications in IOT devices. Randomize-and-forward relay technique is applied for securing multi-hop communications**.** The solution is found mainly by first considering a single-antenna situation where all strategies are equipped with a solo antenna. All the above analyses are generalized to a multiple antennas.

III. PROPOSED ARCHITECTURE

The proposed architecture is as shown in fig 1. Asymmetric algorithm and Triple DES form the two phases. The prerequisite of this method is the sender and the receiver should exchange their MAC address by sending dummy packets through the 'arp –a' (address resolution protocol) command while they are connected to a common VPN or internet connection. First phase encryption is performed by a hybrid key formed from a 42 bit MAC address and file size converted in binary format. The second phase encryption is done using several keys formed using MAC address of both sender and receiver that they have previously exchanged. The following is the procedure of the proposed system:

3.1Algorithm for sender side

Asymmetric encryption:

Step 1: Build a hybrid key by XORing MAC address of sender and size of input file in binary format.

Step 2: Encrypt the file using the hybrid key obtained from Step 1.

Triple DES:

Step 3: Encrypt the encrypted data using the MAC address of sender that acts as key K1.

Step 4: Compute K2 by performing XOR on binary formats of MAC address of sender and MAC address of receiver.

Step 5: Decrypt the encrypted data using the key K2 obtained from Step 4.

Step 6: Encrypt the decrypted data using the MAC address of receiver that acts as key K3.

Step 7: Send this encrypted data to receiver.

3.2 Algorithm for receiver end

Triple DES:

Step 1: Decrypt the obtained data using the MAC address of receiver that acts as key K3.

Step 2: Compute K2 by performing XOR on binary formats of MAC address of sender and MAC address of receiver.

Step 3: Encrypt the decrypted data using the key K2 obtained from Step 2.

Step 4: Decrypt the encrypted data using the MAC address of sender that acts as key K2.

Asymmetric decryption:

Step 5: Build a hybrid key by XOR ing MAC ID of sender and size of file in bi nary format.

Step 6: Decrypt the data using the hybrid key obtained from Step 5.

3.3 Abstract visual of proposed architecture:

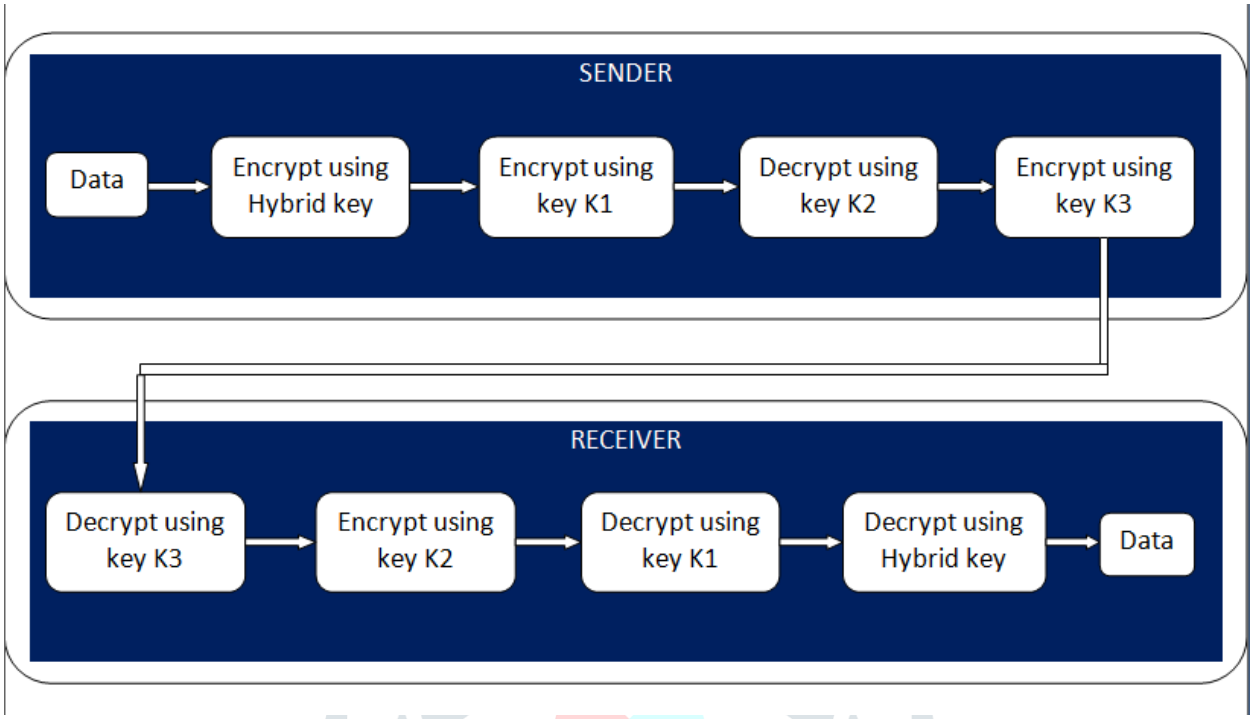

Fig 1:Proposed architecture

IV. RESULTS AND DISCUSSION

The proposed approach is implemented using python programming and is tested with sample input data taken from various files of different sizes. The proposed approach is compared with some regular approaches like DES, and RSA algorithms. Table 1 and 2 shows the comparative study with existing methods.

Table 1. Time taken for encryption on different file sizes

	Time to Encrypt Message			
Input File Size	1 kb	500 kb	1Mb	1Gb
RSA	2.19	6.65	9.89	48
DES	1.18	3.30	5.6	45
Proposed algorithm	6.66	7.83	8.22	70

Table 2. Time taken for decryption on different file sizes

	Time to Decrypt Message			
Input File Size	1 kb	500 kb	1Mb	1Gb
RSA	2.68	3.48	3.77	42.5
DES	1.0	1.50	3.50	25
Proposed algorithm	8.33	13.7	18.48	95

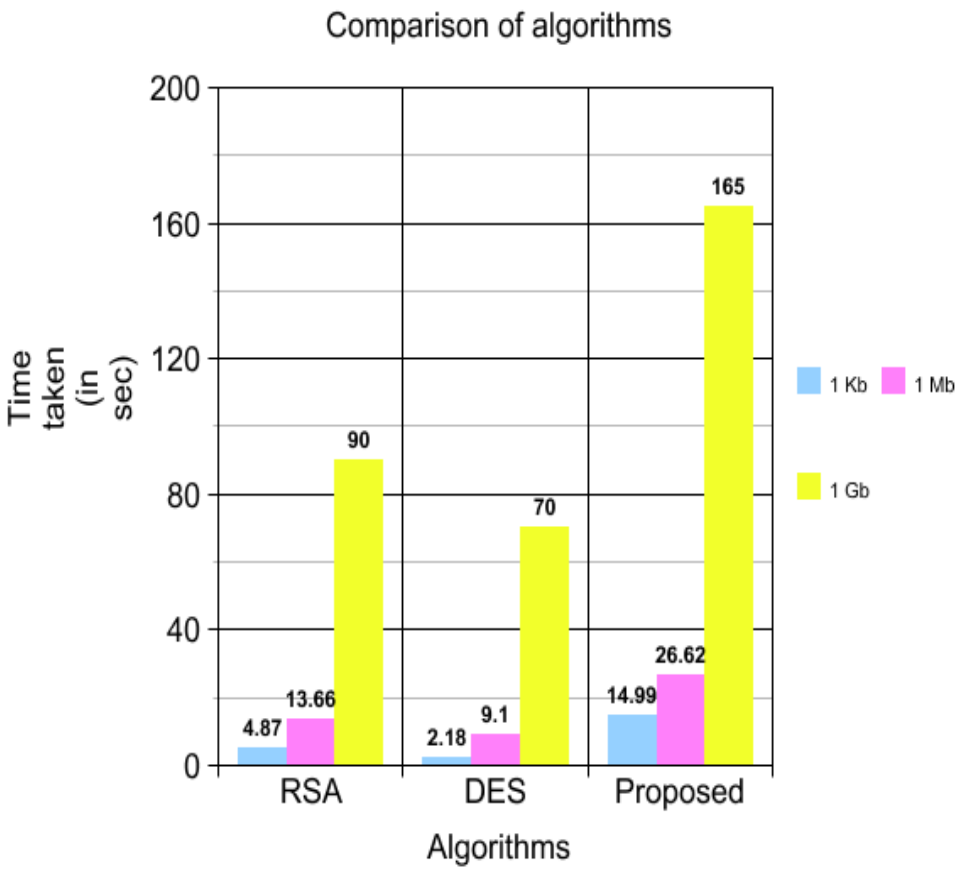

Fig 2:Comparison of algorithm

V. Conclusion

A two-layered authentication approach for IOT objects has been discussed in the paper. This approach uses the mechanism of asymmetric encryption and Triple DES concept to provide a higher level of security for the devices. Further enhancements can be done by developing another phase of authentication.

VI . References

[1] Daddala, B., Wang, H., and Javaid, A. Y. (2017). Design and implementation of a customized encryption algorithm for authentication and secure communication between devices. 2017 IEEE National Aerospace and Electronics Conference (NAECON). doi:10.1109/naecon.2017.8268781

[2] Win, E. K., Yoshihisa, T., Ishi, Y., Kawakami, T., Teranishi, Y., & Shimojo, S. (2017). A Lightweight Multi- receiver Encryption Scheme with Mutual Authentication. 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC).

[3] Guntuku, C., & Pasupuleti, S. K. (2018). Secure Authentication Scheme for internet of Things in Cloud. 2018 3rd International Conference On internet of Things: Smart Innovation and Usages (IoT-SIU)

[4] Sharmeen, S., Huda, S., Abawajy, J. H., Ismail, W. N., & Hassan, M. M. (2018). Malware Threats and Detection for Industrial Mobile-IoT Networks. IEEE Access, 6, 15941–15957.

[5] Challa, S., Wazid, M., Das, A. K., Kumar, N., Goutham Reddy, A., Yoon, E.-J., & Yoo, K.-Y. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. IEEE Access, 5, 3028–3043.

[6] Xu, Q., Ren, P., Song, H., & Du, Q. (2016). Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations. IEEE Access, 4, 2840–2853.

[7] Shah, T., & Venkatesan, S. (2018). Authentication of IoT Device and IoT Server Using Secure Vaults. 2018 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).

[8] https://www.python.org/

[9] https://www.tutorialspoint.com/

[10] https://www.geeksforgeeks.org/