# Privacy preserving IOT communication protocol

**Dr.M.Ramasubramanian[1], K.KrishnaSree[2], M.Rohitha[3], S.Malini[4]**

Professor[1],[2,3,4]Undergraduates
Department of Computer Science and Engineering,
Sridevi Womens Engineering College,
Hyderabad,Telangana.

**ABSTRACT: Recently Internet-of-Things has created a lots of changes in the real world.As IOT makes easy work but there is a lack of security practice raises the risk of privacy-sensitive user data leakage.Securing data transmission among IoT devices is used in Intelligent Connected Vehicles, Smart Home, Intelligent City.In order to secure the data we use cryptographic communication scheme in this device.Cryptographic communication is challenged by the limited resource of low-cost IoT devices, even negligible extra CPU usage of battery-powered sensors would result in dramatical decrease of the battery life. In this paper, to minimize the resource consumption, we propose a communication protocol involving only the symmetric key-based scheme, which provides ultra-lightweight yet effective encryptions to protect the data transmissions. Chaotic system model is used, i.e., Logistic Map, to resist against the key reset and device capture attacks. We semantically model such protocol and analyze the security properties.**

## 1.INTRODUCTION

IOT devices used in smart homes, smart city, Intelligent Connected Vehicles (ICVs) and so forth have become a fundamental part of our modern life. It is estimated that there will be 25 billion ‘‘connected’’ IoT devices by 2020, and the global economy will be impacted by the IoT sector’s expansion by more than $6 trillion by 2025. Such devices facilitate the automation, adaptability, efficiency, and convenience of our living space. In most cases, devices or sensors in IoT environment are connected using wireless channels

This means our protocol is resistant to device capture attack. In summary, the contributions of our research are as following.

1. We present a secure communication protocol based solely on symmetric cryptography scheme. Since it works independent on asymmetric cryptography, the resource cost is extremely low. Moreover, it is a general solution for secure end-to-end data exchange among devices in heterogeneous IoT environment.
2. We design an effective key delegation mechanism based on a chaotic system, i.e., Logistic Map. This mechanism helps to resist the device capture attack by randomselecting the parameters and initial values. Besides, we implements a synchronous rekey scheme to prevent key reset attack.
3. We comprehensively evaluate the security properties and resource cost of our protocol. The result illustrates that the safety and efficacy. Moreover, in the comparison analysis, our protocol outperforms existing chaotic system-based approach for smart home systems.

**SCOPE:**

In our work, the symmetric keys are managed in a synchronous mode based on chaotic system which can guarantee the confusion and diffusion of our cryptosystem.

## 2.Related Study

**A privacy preserving communication protocol for IoT applications in smart homes**

The development of the Internet of Things has made extraordinary progress in recent years in both academic and industrial fields. There are quite a few smart home systems (SHSs) that have been developed by major companies to achieve home automation. However, the nature of smart homes inevitably raises security and privacy concerns. In this paper, we propose an improved energy-efficient, secure, and privacy-preserving communication protocol for the SHSs. In our proposed scheme, data transmissions within the SHS are secured by a symmetric encryption scheme with secret keys being generated by chaotic systems. Meanwhile, we incorporate message authentication codes to our scheme to guarantee data integrity and authenticity. We also provide detailed security analysis and performance evaluation in comparison with our previous work in terms of computational complexity, memory cost, and communication overhead.

**A method for obtaining digital signatures and public-key cryptosystems**

An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the intented recipient. Only he can decipher the message, since only he knows the corresponding decryption key.A message can be “signed” using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in “electronic mail” and “electronic funds transfer” systems. A message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret primer numbers p and q. Decryption is similar; only a different, secret, power d is used, where $e * d \equiv 1 (\mathrm{mod}\ (p - 1) * (q - 1))$. The security of the system rests in part on the difficulty of factoring the published divisor, n.

**Random key predistribution schemes for sensor networks**

Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. We present three

new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key predistribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, we present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

## III SYSTEM ANALYSIS

**EXISTING SYSTEM:**

This IoT are using in almost all fields like monitoring industrial machines, military area, agriculture fields and many more. This IoT communications can be hacked and controlled by attackers to send corrupted data and to avoid this problem we need to secure communication data by using encryption and decryption techniques but this technique require heavy computation and sharing of public and private keys. IoT are small devices which runs on battery power so cannot perform heavy computation and if they share keys then this keys can also be hacked.Existing system uses Asymmentric encryption which requires heavy computation.

**DISADVANTAGES OF EXISTING SYSTEM:**

- The main challenge of implementing a symmetric keybased protocol is designing a robust key delegation mechanism.
- The keys can't be distributed through public networks and require effective renewing and revocation strategies to maintain freshness

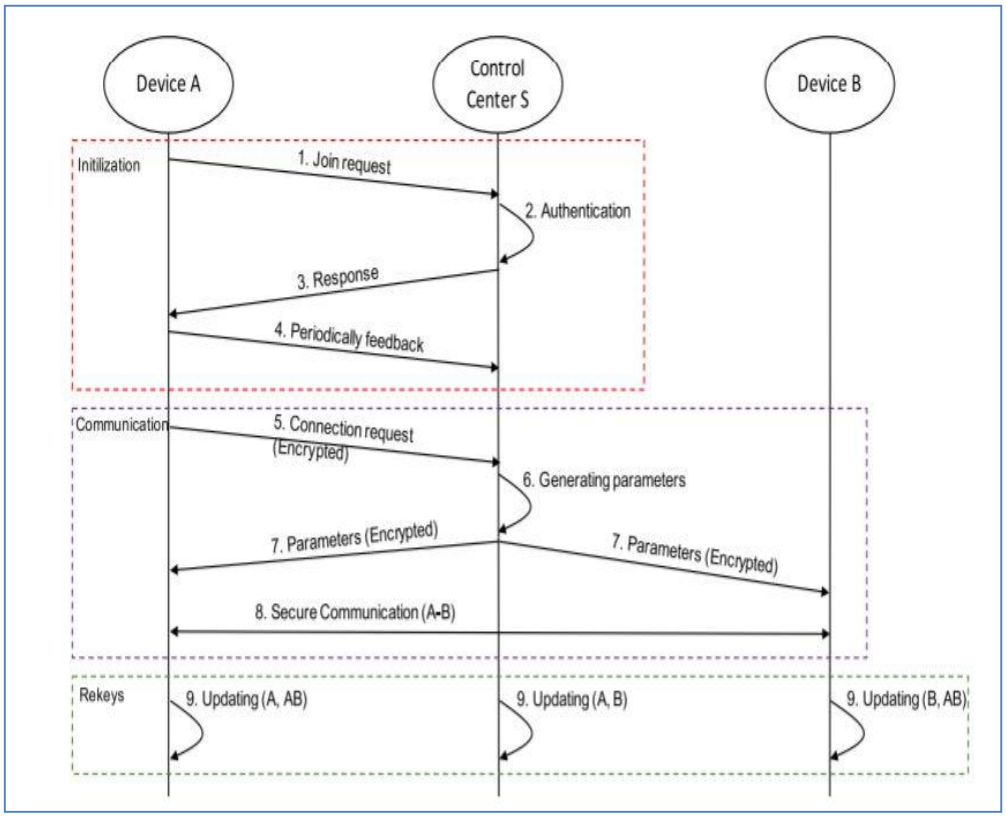
**PROPOSED SYSTEM:**

In this paper introducing light weight communication technique in heterogeneous (different) IoT environment to preserve data security and privacy. In propose paper no need to share any keys or perform asymmetric heavy encryption or decryption. In propose paper author using Control Center which distribute identities/keys to different IoT devices and in future if any IoT sending data then IoT will send his encrypted identity and MAC (message Authentication Code) to Control Center and Control Center will lookup IoT identity in database and verify MAC code and if both verification successful then authentication will be consider as valid and this process is called as INITIALIZATION.

**ADVANTAGES OF PROPOSED SYSTEM:**

In our work, the symmetric keys are managed in a synchronous mode based on chaotic system which can guarantee the confusion and diffusion of our cryptosystem.

**IV SYSTEM DESIGN**




So to avoid above mention problems we introduce a light weight communication technique in heterogeneous (different) IoT environment to preserve data security and privacy. In this no need to share any keys or perform asymmetric heavy encryption or decryption. Using Control Center which distribute identities/keys to different IoT devices and in future if any IoT sending data then IoT will send his encrypted identity and MAC (message Authentication Code) to Control Center and Control Center will lookup IoT identity in database and verify MAC code and if both verification successful then authentication will be consider as valid and this process is called as INITIALIZATION.

Establish SESSION Key: Once after successful initialization of DEVICE 'A' then session key will be establish and source IoT can use this session key to send and receive N number of messages. Device 'B' can also be authenticated with Control Center in similar

manner and session key will be established. Once after session key set then both device A and B can communication with each other.

Communication: Once after session set then device A can encrypt data using timestamp and symmetric encryption technique and then send to Control Center and then Control Center will authenticate both sender Device A and receiver Device B and once after authentication then Control Center send encrypted data to destination Device B which will receive and decrypt data.

So in this we haven't used any public or private key sharing or heavy AES computation and just by using simple MAC and symmetric encryption with Control Center, provided security to data and will be consider as light weight security.

To implement above technique we don't have any IoT device so we are implementing above concept using simulation to achieve data security. We use using CHAOTIC random number to generate identity for each IoT.

- **Generate the IOT link**
  Using this module we generate the IOT link.
- **Establish the session keys**
  Using this module we establish the session keys.
- **Establish the communication**
  Using this module we establish the communication between devices.

**Algorithm:**

**Advanced Encryption Standard**

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

## VI CONCLUSION

In this we present an ultra-lightweight device-to-device secure protocol solely based on the symmetric key-based scheme. Our protocol provides generic protection for heterogeneous IoT environment. In this protocol, the synchronous key delegation mechanism is designed using a chaotic system, i.e., Logistic Map, which ensures the unpredictable, unrepeatable and determinate properties of the symmetric keys. We comprehensively evaluate the security and efficacy of the proposed protocol, and examine the resistance against some harmful vulnerabilities. The result shows that our protocol outperforms the previous symmetric key-based work for smart home systems.

## FUTURE ENHANCEMENT:

Security is big challenge in internet of things scenario. For the prevention of threats in scenario of internet of things used various security models. The cryptography play an important role in security concern in internet of things. The cryptography provides public and private cryptography algorithms for the generation of key for the process of authentication and authorization. The security threats is big barrier of reachability of internet of things. Now need to provide better security protocol stack for the prevention of security and authentication of data.

## REFERENCES

1. T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, ''A privacy preserving communication protocol for IoT applications in smart homes,'' IEEE Internet Things J., vol. 4, no. 6, pp. 1844–1852, Dec. 2017, doi: 10.1109/JIOT.2017.2707489.
2. J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, ''Nei-TTE: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city,'' IEEE Trans Ind. Informat., vol. 16, no. 4, pp. 2659–2666, Apr. 2020.
3. Z. Tian, X. Gao, S. Su, and J. Qiu, ''Vcash: A novel reputation framework for identifying denial of traffic service in Internet of connected vehicles,'' IEEE Internet Things J., to be published.
4. Sumsung Smartthings Developers Documentation. [Online]. Available: https://smartthings.developer.samsung.com/blog/en-us/2019/ 01/17/Shape-the-Future-of-IoT-with-SmartThings
5. J. Van Bulck, J. T. Mühlberg, and F. Piessens, ''VulCAN: Efficient component authentication and software isolation for automotive control networks,'' in Proc. 33rd Annu. Comput. Secur. Appl. Conf. (ACSAC), Orlando, FL, USA, Dec. 2017, pp. 225–237, doi: 10.1145/3134600.3134623.
6. 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, doi: 10.1145/359340.359342.
7. W. Diffie and M. Hellman, ''New directions in cryptography,'' IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: 10.1109/TIT.1976.1055638.
8. C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, ''Elliptic curve lightweight cryptography: A survey,'' IEEE Access, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.