DEVELOPING LIGHTWEIGHT CRYPTOGRAPHIC SOLUTIONS FOR A TARGETED OPTIMIZATION OF INTERNET OF THINGS

Hardik Chaudhary

ABSTRACT

IoT empowers physical things to convey, figure and make choices dependent on any system action. This requires a safe answer for correspondence among heterogeneous gadgets. With the improvement in Information and Communication Technology (ICT), an interesting effect of keen things is seen in our regular day to day existence. IoT can consider clients that associate in heterogeneous conditions. In heterogeneous condition thought process of every client in IoT can be distinctive in type of correspondence and calculation and is hard to be judged. A malevolent client can decimate the security and protection of the system. This examination gives a nitty-gritty investigation of existing security answers for IoT. Right off the bat, a correlation of lightweight cryptography calculations is made on the premise of square size, key size, number of rounds, and plausible assaults. Afterward, the different security issues in IoT are talked about alongside conceivable arrangement. Security arrangements in IoT will improve the trust over IoT. A safe arrangement that will require less computational power and is less defenceless against existing assaults is wanted.

1. INTRODUCTION

IoT is a developing innovation in this growing time of shrewd things1. Shrewd things can be any physical items like telephone, workstation, cooler, AC, charger, and some more. IoT can be characterized as a system of particularly recognizable, available, and reasonable brilliant things that are fit for correspondence, calculation, and extreme basic leadership. It is referenced that things in IoT can be associated by utilizing remote associations like RFID, Bluetooth, ZigBee, WSN, WLAN, WMAN or Wi-Fi2. The number of things or users connected to IoT is growing exponentially and around 2020 the number of connections may reach 50 billion. Hence, the bandwidth requirement of IoT will also increase exponentially. Licensed and unlicensed bands are available for communication. Licensed bands are paid and are used in applications like 2G, 3G and many more. Unlicensed frequency bands are reserved for industrial, scientific and medical applications also known as ISM bands. The existing ISM bands are 433 MHz, 915 MHz and 2.4 GHz. The ISM band used in IoT is 2.4 GHz for Wi-Fi enabled communication. For the complete deployment of IoT different enabling technologies like RFID or sensors are required. As mentioned, RFID in IoT can be used to identify the things and track the current status of things in real time like its location3. RFID can be used in application like retail management, transport systems, security or inventory management. RFID use radio waves to identify the things uniquely through electronic barcodes. As described in4, RFID is built on three components- RFID tag/transponder, RFID antennas and RFID reader which maintain the data on the microchip. According to5, the two major components of RFID are RFID reader and

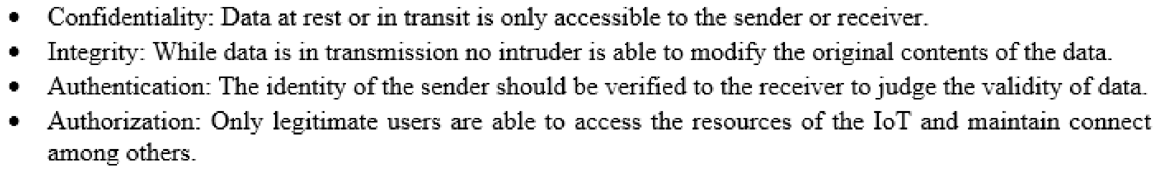
RFID tag. RFID tag is attached to each and every thing which is active in the network. It comprises of a microchip that is punched with unique identity of a particular thing. RFID reader is used to access the information from the tag and pass on this information to the application system6. Another technology that can be used in IoT is sensors. Sensors can be used to connect the information environment to the physical environment in IoT. Wireless Sensor Network (WSN) is used to sense and collect information related to an activity in real environment7 and that information is passed to the network for generating responses. The application areas of WSN are temperature control, humidity control, remote sensing, military any disaster management7. But WSN works only for collecting the data and is not able to process the data for final decision making. So, IoT took this advantage of WSN for collecting the data, and further apply processing on this data to take fruitful decisions7. IoT acts as an extension to WSN in aforementioned application areas and broaden them in more functional way8. The main objective of this research paper is to give an ideal view of challenges and security solutions for IoT. The paper is organized as follows: In Section 2, motivation to carry out this research work is mentioned. In Section 3, the related work on current lightweight algorithms in IoT for security is done. In Section 4, all the issues related to IoT are presented. Later, the review narrow downs to the most prominent issue in IoT, and its recommended solution.

2. RESEARCH MOTIVATION

IoT helps in making associations between disparate things present in the heterogeneous condition. This sort of receptiveness and exceptionally less human intercession can make IoT presented to a number of assaults like the man in a centre assault, Denial of Service (DoS) assault. Also, any gadget can get to the system that prompts unapproved get to. These assaults can harm gadget physically and arrange associations as well. This will at last bargain the security and protection of IoT. As, IoT is asset obliged with less power, transmission capacity, less stockpiling, so a productive security arrangement is necessitated that won't eat through the assets of IoT.

3. CURRENT SECURITY SOLUTIONS IN IOT: RELATED WORK

IoT can use internet only for connecting and establishing communication between things in the network. There is much more to further work upon in IoT like making decisions after communicating and that too in real time. So, architecture of internet cannot be directly employed for IoT.



- Confidentiality: Data at rest or in transit is only accessible to the sender or receiver.
- Integrity: While data is in transmission no intruder is able to modify the original contents of the data.
- Authentication: The identity of the sender should be verified to the receiver to judge the validity of data.
- Authorization: Only legitimate users are able to access the resources of the IoT and maintain connect among others.

In literature number of architectures was proposed for IoT. Authors in9 mentioned that IoT have a three layered architecture. The three layers of IoT are perception layer, network layer and application layer from bottom to top. A 5 layered architecture was proposed in10 composed of perception, transport, processing, application, and business layer. With the increase in application requirements of the user a vast amount of data is shared among themselves. So, security and privacy of IoT is intricate than other networks as personal data of user is communicated like location, time, information. The security services required to be maintained in IoT so as to enhance the trust of users are Security architecture was proposed that will secure the data exchanged between business partners and assures above mentioned services11. A security and quality assuring architecture was also proposed in12 but it still has a challenge to manage the open related data in IoT. As IoT comprise of heterogeneous connected things, a standard architecture is imposed on all the things with 4 layers. Each layer will provide an inbuilt security protocol that will help to achieve security services before transmitting data from one layer to other.

4. SECURITY ARCHITECTURE OF IOT

• Physical/Perception Layer: It is the bottom layer of IoT that is combination of physical and MAC layer in internet architecture. It is used to collect the information using RFID, sensors, or GPRS. IEEE 802.15.4 is used as a standard specification at this layer for IoT. IEEE 802.15.4 works for low cost, battery operated things13. IEEE 802.15.4 security solution is available at this layer which is still vulnerable to attacks.

• Network Layer: The physical layer transmits gathered data to the network layer. The system layer is utilized to isolate the message to parcels and to course the bundles from source to the goal by utilizing the IPv6 tending to the instrument. As the number of associated things in IoT is growing so IPv4 address space is supplanted by IPv6 having more address space. Inbuilt cryptography conventions like AES, DES can be executed by utilizing IPSec at the system layer.

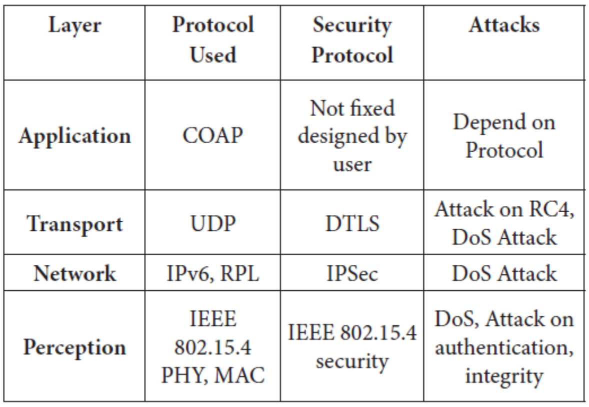
• Transport Layer: IoT uses User Datagram Protocol (UDP) for end to end communication. As UDP is an unreliable protocol so a security mechanism using DTLS is incorporated at this layer.

• Application Layer: The actual deployment of intelligence of IoT is understood at this layer. It can be used in number of applications like retail, social activity, health, or for personal use. Constrained Application Protocol (CoAP) is used on this layer for the constrained IoT devices. The existing protocol at each layer, along with security protocol and attacks at each layer is summarized shown in Table 1.

CoAP was earlier using the security of IPSec and DTLS. The predefined security mechanisms are vulnerable to aforementioned attacks. So, cryptography algorithms can be incorporated in them. Cryptography algorithms can be symmetric and asymmetric. Symmetric algorithm uses a single private key for communication. Sender and receiver share same key for communication. Symmetric key assures confidentiality and integrity of data, but do not guarantee authentication. Advantage of symmetric is less number of keys required with less key size. Disadvantage is secure key distribution among both the parties, and it does not authenticate the sender.

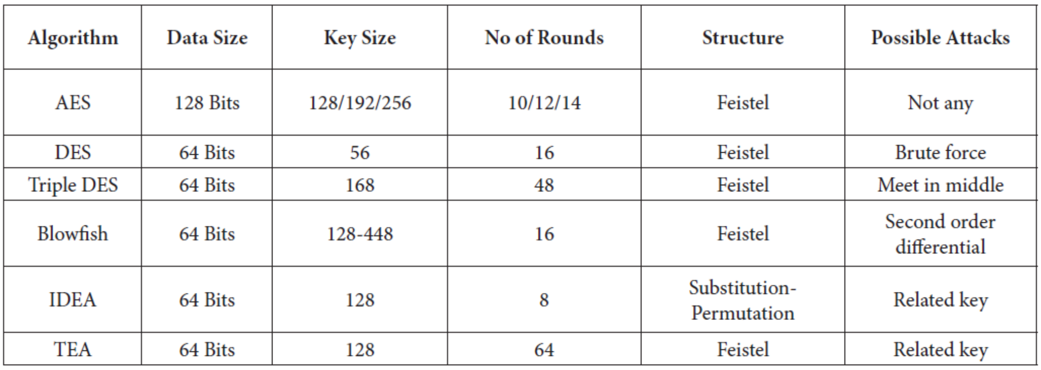
Traditional Symmetric algorithms AES, DES, Triple DES, Blowfish, IDEA are compared on the basis of their properties like data size, key size, number of rounds, structure and existing attacks shown in Table 2. Asymmetric uses pair of public and private key for communication. Asymmetric assures confidentiality, integrity, and authentication. For confidentiality and integrity sender encrypts the data using public key of receiver that can be only decrypted by private key of receiver. To assure authentication, data is encrypted by private key of sender and receiver confirms it by decrypting it with public key of sender. Advantage of Asymmetric cryptography is it supports all security services, but disadvantage is the large size of key which will increase the complexity of algorithm. The most common algorithms used are RSA by Rivest, Shamir and Adleman, Deffie Helmen key exchange (DH), Elliptic Curve Cryptography (ECC), and Hash functions. Traditional Symmetric and Asymmetric algorithms are not apt for IoT environment due to the limited power devices, low computational resources, and less memory capacity of IoT.

Table 1. Security protocols in IoT



Layer	Protocol Used	Security Protocol	Attacks
Application	COAP	Not fixed designed by user	Depend on Protocol
Transport	UDP	DTLS	Attack on RC4, DoS Attack
Network	IPv6, RPL	IPSec	DoS Attack
Perception	IEEE 802.15.4 PHY, MAC	IEEE 802.15.4 security	DoS, Attack on authentication, integrity

Table 2. Comparison of existing symmetric cryptographic algorithms



Algorithm	Data Size	Key Size	No of Rounds	Structure	Possible Attacks
AES	128 Bits	128/192/256	10/12/14	Feistel	Not any
DES	64 Bits	56	16	Feistel	Brute force
Triple DES	64 Bits	168	48	Feistel	Meet in middle
Blowfish	64 Bits	128-448	16	Feistel	Second order differential
IDEA	64 Bits	128	8	Substitution-Permutation	Related key
TEA	64 Bits	128	64	Feistel	Related key

So, lightweight security algorithms were proposed for IoT. Lightweight solutions are light in terms of their key size, memory requirements and execution time so that fewer resources will be utilized as compared to heavy weight solutions.

5. SYMMETRIC LIGHTWEIGHT

Algorithms FOR IoT

• Advanced Encryption Standard (AES): AES is used as an inbuilt solution in COAP at application layer. It is a symmetric block cipher standardized by NIST. It uses substitution permutation network and works on 4*4 matrix having block length of 128 bits. Every byte gets affected by subbytes, shiftrows, MixedColumns, AddRoundKey14. Key size than can be used is 128, 192, 256 bits. AES is still vulnerable to man-in-middle attack15.

• High security and lightweight (HIGHT): Hight uses very basic operations like addition mod 28 or XOR to work for Feistel network. It has a block size of 64 bits, work in 32 rounds on128 bit keys16. Its keys are generated while encryption and decryption phase. A parallel implementation of higth was proposed in17 that requires less power, mentioned in few lines of code, and improves speed for RFID systems. Higth is vulnerable to saturation attack.

• Tiny Encryption Algorithm (TEA): TEA is used for constrained environments like sensor networks or smart things. It is written in very few lines of code. It does not use a complex program but requires simple operations of XOR, adding and shifting. It uses a block size of 64 bits and 128 bit keys and does not make use of existing tables or any predefined computations18. Number of variants exists for TEA like extended TEA19, Block TEA and so on. These extensions try to resolve the problems in original TEA like equivalent keys. But still due to its simple operations TEA and its variant are susceptible to number of attacks.

• PRESENT: It is based on SPN and is used as ultra-lightweight algorithm for security. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. It has key size of 80 or 128 bits and operates on 64-bit blocks20. PRESENT has been presented as a lightweight cryptography solution in ISO/IEC 29192-2:2012 “Lightweight Cryptography”21. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds22.

• RC5: It was first coined by Rivest for rotations that are data independent23. It posses Feistel structure and can work well as lightweight algorithm as it is used in wireless sensor scenarios. RC5 is considered as w/r/b, where w refers to word size, r stands for number of working rounds, and b will tell about the number of bytes in encryption key. RC5 generally works on 32 bit size but its variants can be 16, 32, 64. It can work for 0, 1, .., 255 rounds using 0,1,..255 key bytes. Standard key size is 16 byte on 20 rounds of operation. RC5 is vulnerable to differential attack24.

• Based on literature review conducted, comparison of all aforementioned symmetric lightweight algorithms is made on the basis of code length, structure, number of rounds, key size, block size and attacks shown in Table 6. Asymmetric Lightweight Algorithms for IoT

• RSA: It was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. RSA works on generating public and private key pair by selecting two large prime numbers25. Find their modulus and choosing at random their encryption key and thus calculating the decryption key. Public key is published openly whereas private key is made secure26. A more secure RSA encryption is proposed in27 that is used to encrypt and decrypt files for maintaining privacy of

user.

• Elliptic Curve Cryptography (ECC): It requires less key size as compared to RSA. Hence it has fast processing and less storage requirements. It was invented by28. It s built on algebraic system where it takes two points on elliptic curve. Discrete logarithm problem is used to generate key that is used to compute key. In29 a secure hardware implementation on ECC is proposed for small areas that will lead to faster computations in real time. ECC is optimized for 6LoWPAN nodes by working on its complex multiplication operation. Rather than using microprocessors operation for multiplication, bit shifting is used in30 to optimize the use for low power devices.

6. ATTACKS ON EXISTING ALGORITHMS

Existing security solutions in IoT are still vulnerable to following attacks:

• Denial of Service (DoS): It will halt the services of network for the authorized users due to access of network connection requests from unauthorized users.

• Man-in-Middle: In this an intermediary user is able to get the key of one of the sides and will start communication as if it is the valid party.

• Eavesdropping: Intruder is able to listen the communication between sender and receiver. So this is attack on confidentiality.

• Masquerading: An intruder possess the identity of any other authorized user. So it can tear down the resources of IoT.

• Saturation: In this intruder will try to use the physical and mental ability of authorized party by its immense use.

• Differential: Change in input behavior will affect the output. So this attack is able to find the key from network transformations.

7. RESEARCH CHALLENGES IN IOT

This study reveals number of challenges allied to IoT.

• Lack of human intervention may lead to physical as well as logical attacks.

So challenges can be things related or network related. Challenges concerning things are power limitation, heterogeneous platforms, and security and privacy. Network related issues are scalability, bandwidth issues, and security and privacy.

8. RESEARCH PROBLEM

Now-a-days IoT is admitting in homes, work places, social places or in business firms that will open doors for security and privacy challenges. So, security and privacy issues are becoming major reasons of concern in operation of IoT. The amount of loss that can occur is prominent to imagine if any attack is injected in IoT. Various attacks on IoT exist like eavesdropping, spoofing, Denial of Service (DoS), replay attacks, false signals injection. These attacks will tear down the security services of IoT like confidentiality, integrity, and authentication; moreover, it will impact the privacy of users. IoT provides inbuilt primitive security solutions at each layer, which are still vulnerable to attacks. Traditional cryptography and authentication schemes do not fit well in IoT scenario due to its constrained resources like power, real time execution. So, lightweight cryptography solutions tend to work well in IoT. Number of lightweight Symmetric and Asymmetric cryptography algorithms exists in literature like AES, HIGHT, RC5, PRESENT, RSA, ECC and many more. These existing solutions do not guarantee an optimum level of security in real time communication due to more execution time, code length, and memory requirements. Execution time includes time for key management and distribution, encryption and decryption that decides the effectiveness of the protocol. Asymmetric algorithms are slow due to their large key size, whereas symmetric algorithms can provide only confidentiality and integrity but no authentication leading to attack on availability. This can affect real time information collecting and processing and will fritter away the resources of IoT. This calls for a secure algorithm for IoT that will guarantee services like confidentially, integrity and authentication in optimal time.

9. PROPOSED IDEA

On the basis of literature survey carried out many researchers have proposed lightweight symmetric and asymmetric security algorithms for IoT. Symmetric algorithms provide confidentiality, integrity, have small key size, and are less complex but they do not offer authenticity and distribution of keys in them is a challenging task. On the other hand, asymmetric algorithms provide confidentiality, integrity, and authenticity, but their key size is too large which make them more complex and not apt for constrained IoT scenario. So, there is a need of secure algorithm that will map best features of lightweight symmetric and asymmetric algorithms in such a way that it will take less execution time with optimum energy requirements and will assure all security services like confidentiality, integrity and authenticity.

10. CONCLUSION

IoT faces a number of difficulties like power, data transfer capacity, versatility, heterogeneity, security, and protection. Security and protection is the most basic test to unravel to keep up the trust of clients in IoT. Pre-characterized security arrangements at each layer are as yet defenceless to assaults. So cryptography calculations can be utilized to guarantee security. Be that as it may, customary overwhelming weight calculations are not adept for IoT because of their compelled condition. Consequently, interchange lightweight cryptography arrangements symmetric just as awry can be utilized.