Abstract—Internet of Things is the Connections of embedded technologies that contained physical objects and is used to communicate and intellect or interact with the inner states or the external surroundings. Rather than people-people communication, IoT emphasis on machine-machine communication. This paper familiarizes the status of IoT growth. The IoT embeds some intelligence in Internet connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. This paper addresses the existing development trends, the generic architecture of IoT, its distinguishing features and possible future applications. This paper also forecast the key challenges associated with the development of IoT. It emphasizes the use of lightweight algorithms to increase the security of content with less iteration.

Keywords—Internet of Things, ubiquitous computing, Lightweight Algorithm, IoT architecture, IoT applications, IoT security.

I. INTRODUCTION

Internet of Things (IoT) is a network of connected devices with unique identifiers in the form of an IP address which have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment in which they reside and/or themselves [1]. IoT provides better chances of making world a greater level of accessibility, availability, scalability, confidentiality, and interoperability [3].  But, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. [2], IoT is widely applied to social life applications such as smart grid. IoT is considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning [4].

The IoT links real life and physical activities with the virtual world, the numbers of Internet connected devices are increasing at the rapid rate. These devices include personal computers, laptops, tablets, smart phones, PDAs and other handheld embedded devices. Mobile computing devices use different sensors and input mechanisms that can sense, do compute, decides on the actions to be done and transmit processed decisions & data over the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected. [5]. IoT devices are increasing in many folds day by day, in mean time power requirement and processing capacity of device is being considered as a key factor while designing IoT devices.

Due to size constraint and power utilization data security becomes vulnerable while computing using small or low-powered IoT devices. Low-energy technologies in the Internet of Things (IoT) era are still unable to provide the reliability needed by the industrial world, particularly in terms of the wireless operation that pervasive deployments demand. Most of the industrial wireless performance has achieved good results, but it is difficult task to achieve energy-requirement of an application [6]. Enabling low-powered IoT devices with efficient algorithms to handle Data Security, Integrity and Availability is need of the hour. In this paper we bring out current algorithms used in IoT devices and its performance with respect to low-powered devices and also propose research guidelines on how it can be improved.

II. IOT ARCHITECTURE

IoT devices are commonly now available in following segments of daily use, Consumer Services, Smart house; Smart meters in energy division, Smart mobiles, and Smart wearable devices on consumer computing devices, connected cars, Motors and manufacturing metrics, Physical objects[42] are the few areas where industry utilizes power of IoT.

<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocol Used</th>
<th>Security Protocol</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>CoAP</td>
<td>Not fixed designed</td>
<td>Depends on Protocol</td>
</tr>
<tr>
<td>Transport</td>
<td>UDP</td>
<td>DTLS</td>
<td>Attack on RC4, DoS Attack</td>
</tr>
<tr>
<td>Network</td>
<td>IPv6, RPL</td>
<td>IPSec</td>
<td>DoS Attack</td>
</tr>
<tr>
<td>Perception</td>
<td>IEEE 802.15.4</td>
<td>IEEE 802.15.4</td>
<td>DoS, Attack on authentication, integrity</td>
</tr>
</tbody>
</table>

Revised Version Manuscript Received on 22 February, 2019

D.M. Sheeba, Dept of Computer Science, New Prince Shri Bhavani Arts & Science College, Chennai, India. (e-mail: mesheeba.co.in)
R. Varalakshmi, Dept of Computer Applications, VISTAS, Chennai, India. (e-mail: rvara.scs@velsuniv.ac.in)
N. Anbumani, Networks & Cryptography, Selima Groups, Chennai, India. (e-mail: me@anbumani.co.in)
The physical objects are equipped with Radio-Frequency Identification (RFID) tags. The RFID adaptor can detect data from RFID tags, applying the RFID adaptor in IoT environment, it can interoperate data/events of other applications in IoT [41]. To secure the interoperability of data and physical objects several layers and protocols are defined to prevent attacks and vulnerabilities [45].

The common architecture of IoT devices / Computing devices through Internet has Application, Transport, Network, Physical Layers. Each layer is enabled with different kind of algorithm or security measure to handle data securely [44]. When we talk about power consumption at each layer, it depends on how frequently computing done on incoming data.

A. Physical Layer

Physical Layer is bottom layer of IoT responsible for sensing and providing required data for processing. On connectivity front, these are connected to Ethernet or Wi-Fi networks and secured by non-alterable physical Universally Unique identifiers (UUID) [7].

B. Network Layer

Network Layer is responsible for communicating with network management and communication channels through multiple protocols [8] as in Fig 2.

C. Data Processing Layer

Data Processing Layer is responsible for providing services based on available data from sensing devices stored in databases [9]-[10].

In above architecture, each layer carries the data till Application Layer to present it as a usable and meaningful data. In this stream of data flow Security, Integrity, Confidentiality is essential in order to maintain a reliable IoT network [11].

III. RECENT SECURITY THREATS & COUNTER MEASURES IN IOT DEVICES

An IoT system can be attacked physically, or attacked from within its network, or from applications on the system, and lastly from attacks on encryption schemes. IoT is implemented using various existing [47] network technologies (Wireless Sensor Networks, RFID, Internet, etc.). Thus, there is a need for a proper categorisation of the attacks such that it encapsulates all of the different types of threats, so that better counter measurements can be developed and implemented for securing it. However, it is worth mentioning that Environmental Attacks (Earthquakes etc.) are omitted from this paper as their scope is beyond our research that focuses on intentional attacks from an adversary.

A summary of the classification [12]-[14] of the attacks is shown in Table I below.

An IoT system consists of three different layers each with vulnerabilities and security attacks. To address these attacks and to successfully protect the IoT system, this section presents a multi-layered security approach that should be structured to give an optimal layered protection at each layer in an IoT system [15]-[23] as shown on the next page in Table II.

### Table I

<table>
<thead>
<tr>
<th>Physical Attacks</th>
<th>Network Attacks</th>
<th>Software Attacks</th>
<th>Encryption Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Tampering</td>
<td>Traffic Analysis</td>
<td>Virus and Worms</td>
<td>Side Channel Attacks</td>
</tr>
<tr>
<td>RF Interference</td>
<td>RFID Spoofing</td>
<td>Spyware and Adware</td>
<td>Man In The Middle Attack</td>
</tr>
<tr>
<td>Node Jamming</td>
<td>RFID Cloning</td>
<td>Trojan Horse</td>
<td>Cryptanalysis Attacks: a) Cipher Text Only Attack b) Known Plaintext Attack c) Chosen Plaintext or Cipher Text Attack</td>
</tr>
<tr>
<td>Malicious Node Injection</td>
<td>RFID unauthorised Access</td>
<td>Malicious scripts</td>
<td></td>
</tr>
<tr>
<td>Physical Damage</td>
<td>Sinkhole Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Man In the Middle Attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sleep Deprivation Attack</td>
<td>Denial of Service</td>
<td>Denial of Service</td>
<td></td>
</tr>
<tr>
<td>Malicious Code Injection on the Node</td>
<td>Routing Information Attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybil Attack</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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, Diffie-Hellman 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. 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.

IV. 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 4x4 matrix having block length of 128 bits. Every byte gets affected by subbytes, shiftrows, MixedColumns, AddRoundKey[24]. Key size than can be used is 128, 192, 256 bits. AES is still vulnerable to man-in-middle attack[25].

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 keys[26]. Its keys are generated while encryption and decryption phase. A parallel implementation of highth was proposed in[27] that requires less power, mentioned in few lines of code, and improves speed for RFID systems. Hight 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 computations[28]. Number of variants exists for TEA like extended TEA[29], 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 blocks[30]. PRESENT has been presented as a lightweight cryptography solution in ISO/IEC 29192-2:2012 “Lightweight Cryptography”[31]. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds[32].

RC5: It was first coined by Rivest for rotations that are data independent[33]. 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 attack [34].

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 1.

<table>
<thead>
<tr>
<th>Symmetric Algorithm</th>
<th>Code length</th>
<th>Structure</th>
<th>No. of rounds</th>
<th>Key Size</th>
<th>Block Size</th>
<th>Possible Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>260</td>
<td>SPN</td>
<td>10</td>
<td>12</td>
<td>8</td>
<td>128</td>
</tr>
<tr>
<td>HIGHT</td>
<td>567</td>
<td>GFS</td>
<td>32</td>
<td>12</td>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>TEA</td>
<td>114</td>
<td>Feistel</td>
<td>32</td>
<td>12</td>
<td>8</td>
<td>64</td>
</tr>
<tr>
<td>PRESENT</td>
<td>936</td>
<td>SPN</td>
<td>32</td>
<td>80</td>
<td>64</td>
<td>80</td>
</tr>
<tr>
<td>RC5</td>
<td>Not fixed</td>
<td>ARX</td>
<td>20</td>
<td>16</td>
<td>32</td>
<td>128</td>
</tr>
</tbody>
</table>

V. SYMMETRIC 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 numbers[35]. 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 secure[36]. A more secure RSA encryption is proposed in[37] 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 by[38]. It is 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. In[39] 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 in[40-45] to optimize the use for low power devices. Differential: Change in input behavior will affect the output. So this attack is able to find the key from network transformations.

VI. 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.

VII. 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. IoT uses wireless communication that is vulnerable to number of attacks like eavesdropping, man-in-the-middle, Denial of Service (DoS) and many more. Any device can connect to the network so that may cause unauthorized access to the network. IoT devices are resource constrained in terms of power and bandwidth so exercising intricate security solutions can hinder the efficient working of devices. So challenges can be things related or network related. Challenges concerning things are power limitation, heterogeneous platforms, and security and privacy[55]. Network related issues are scalability, bandwidth issues, and security and privacy.

VIII. 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[51-54]. 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[46]. 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 confidentiality, integrity and authentication in optimal time.

IX. 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[50]. 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[56] 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.

X. CONCLUSION

IoT faces number of challenges like power, bandwidth, scalability, heterogeneity, security and privacy. Security and privacy is the most imperative challenge to solve to maintain the trust of users in IoT[49]. Pre defined security solutions at each layer are still susceptible to attacks. So cryptography algorithms can be used to assure security. But traditional heavy weight algorithms are not apt for IoT due to their constrained environment. Hence, alternate lightweight cryptography solutions symmetric as well as asymmetric can be used.

REFERENCES


49. Cooper, J.; James, A. Challenges for Database Management in the Internet of Things. IETE Tech. Rev. 2014, 26, 320–329. [CrossRef]


