ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Review on Internet of Things Attacks and Their Countermeasure using Lightweight Cipher Algorithms

Anandika sharma
Department of computer science
Punjabi university
Patiala, India

Dr.Amardeep singh
Department of computer science
Punjabi university
Patiala, India

Abstract- Due to the increasing demand of interconnected devices has led to the world "internet of things" which transform the real world into the virtual objects. After 1991 there is a great change in human life, industry and organization due to the development of interconnected devices which leads to speed up processes, reduce errors, and prevent theft to make automation in all areas. IoT covers wide range of applications like smart transport, smart health, smart city, smart farming and many more due to the increasing components in the IoT some components are unattended so it is easy to attack them. The combination of network, things and services IoT needs to be secured and privacy issues are the main concern. In this paper, a survey on evolution of IoT network, their attacks, and on the basis of application survey is done. From the survey, found that cryptographic techniques have been applied to secure the data on IoT. The IoT devices are resource constraint devices so conventional algorithms performance not efficient so lightweight algorithms required. Also, in this paper comparative analysis is done on lightweight algorithms.

Keywords- Internet of Things, Lightweight Cryptography, IoT Attacks.

I. INTRODUCTION

The definition of internet of things is still debate but it is network of devices, connected devices, smart devices and items embedded with sensors, actuators ,radio frequency identification(RFID) tags in which these devices can exchange and collect data from other devices. IoT term was first used by Kevin Ashton in presentation in 1998[1]. The term "internet of things "has arrived more than 12 years ago but come into existence when international telecommunication union (ITU) published the first report in 2005 [2]. Today internet of things has changed the life of people in a smarter way. IoT has connected million of devices through internet which given the future of computing and automation. So, increasing era of internet has been made to trust on internet and the smart devices. The increasing rate of IoT devices change the world into cyber world which brings the dependency on electronic system , sharing data, communication which leads to the new meaning of business, education, sociality for our society. In 2008 IoT is reported by US national intelligence council as one of the six emerging technologies which has a great impact on the US interest towards 2025[3]. IOT can develop at fast rate in this era in 1999: a big year for IoT, Kevin Ashton the executive director of Auto-ID centre lab coined the term internet of things, in 2000: LG introduce his first internet refrigerator plan, in 2003-2004:the term starts mentioned in publications like THE GUARDIAN,BOSTON GLOBE and the term can first appear as the title of the book, in 2011:CISCO, ERICCSON,IBM produce a large educational market on this topic. China continues to fund and support research in the field of internet of things at institutions like shanghai institute and the Chinese academy of science and finally news, videos ,presentation, events and IoT news added daily on the topic [4].

IoT is based on interfacing the digital objects and physical world via internet. The phase of network increases day by day. Later there is a phase of host to host network, mobile network, internet of people which connects people with social media, communicate via emails, playing video games and now the phase of IoT which connect devices with internet as well as with each other. With the combination of internet, RFID and sensor networks leads to the new version of technology that is machine to machine communication which is known as 'internet of things' the main goal of internet of things is to make world better for humans where the devices around us understand the situation and perform the action without any restriction.

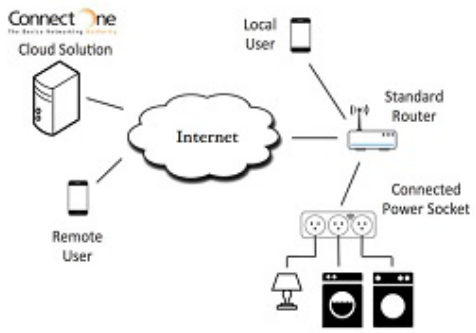

Fig. 1 Block Diagram of IoT

The block diagram for the internet of things given below which contains the devices, internet, cloud server, router and the user shown in fig 1.

Cloud solutions: It contains the whole data that can be processed, it behave as the data storage unit.

Internet: it is a network which provides variety of information and communication facilities.

Router: it is a network that connects the users or the objects with the internet for the communication.

Through router, the user and connected devices can interconnect with each other for the communication. So, the IOT is simply a interconnection of devices or the interconnection of user and the devices .radio frequency identification(RFID), sensors, actuators, WIFI, blue-tooth are the technologies that can be used for the transmission of data.

These devices are wirelessly connected with each other so there is a great need of security to preserve the data from unauthorized user. To preserve the privacy and security of data cryptography methods can be used to encrypt/decrypt the data.
The future will transform the real world into IoT with intelligent virtual objects. After 1991 there is a great change in human life ,industries and organizations due to the development of IoT. IoT is developed to speed up the processes, reduce errors and make the world flexible with the objects, which make the future of computing and communication. Now the main objective of users in IoT is to give the detailed view to the readers that what has been done and what still has to be done in this area where the security and privacy issues are the main concern of each user.
In 1982 and a group of computer science graduate students at Carnegie Mellon University in Pittsburgh [5] Pennsylvania, was thirsty some wanted a Coca Cola and some wanted water. But the Coke machine was on the third floor of the university and students feel frustrated when they found it empty. So the scientists connected the machine to the university's computer network. By checking online the researchers found the bottles was on the stock or empty. This turned out to be more efficient way so it's thought to be one of the first non computer objects to go online . some more examples like homeowner adjust the thermostat by using mobile app, air conditioner can be adjusted automatically ,garage shutter can be operated with smart phone apps and many more.
In 2010 GOOGLE introduces the new concept of self driving car project that was a major milestone in the development of internet of things.
In 2011, nest labs introduces the smoke detectors and self learning programs.
In 2013 GOOGLE introduces the eye ware glasses which operate on voice recognition . and at last but not the least in 2014 apple introduces the health kit and home kit for home and health automation system.
Here with the scenario, that the number of devices continues to rise so there is a need of security and privacy for the objects to interconnect with each other or with the network. Devices that are continuously connected with the internet need to be secure where poorly design IoT devices can expose or leak the private or confidential data into wrong hands. So according to survey many new nodes being added to the network or the internet that provide malicious actors with attack vectors and possibilities to carry out the security holes. Another concern along security is the privacy. When IoT devices are constantly tracking our action there is a great need of privacy of data. Ahmed Banafa an IoT expert explain the strategies will need to be developed to respect individual privacy concern across a broad spectrum while still forecasting a new technologies and services. Some of the attacks that are still; exist in the IoT technology can be discussed in section2.

II. SECURITY THREATS ON INTERNET OF THINGS

Due to the increasing technology of internet of things leads to some security threats. Each year brings the new technology for people to ease their lives but unfortunately these advances leads to the cyber security threats and large number of attacks on the surface . The IEEE survey [6] info graphic explains, chief information officer and chief technology officer say that in 2017 there is a biggest challenge is online security threats. There are some issues that we face today are compromised credentials, cross-site scripting (XSS), data breach, distributed denial of service attack, drones, malicious insiders, malware, ransom-ware, spear phishing .

- *Compromised credential*: sometimes hackers can find a list of user credentials for the main goal or sometimes its just a part of larger data haul. Then these credentials can be used for malicious of users for business purpose. In basic attackers simply guess the user password or tool to run thousand of options.
- *Cross-site scripting (XSS*): it is type of injection attack put on websites that accepts input but they don't separate the data and executable code until the input is delivered back to the user's browser, attacker can inject malicious code into the user system or extract the user's data.
- *Data breach:* attacker can target the data stored on servers. The sensitivity of the data explains how data can be potentially damaging to an organization structure, names, credit card numbers health information trade secrets .
- *Distributed denial of service:* attackers can mobilizing thousands of unique IP addresses as zombie agents and disrupt the function. Traditionally attacker can infect the computer with controlling malware while new versions include unsecured IoT devices and cloud services.
- *Drones:* these are very much developing technology but they also present a number of security risks in which some of the instances of them can be hacked even form long distances. The hacker can disrupt the corporate communication via unsecured WI-FI and Bluetooth signals.
- *Malicious insiders:* the organization , employees, formers or business partners can compromise with the system for revenge or personal gain. It is easy to misinterpret the attempt to perform job routine as "malicious " activity but actually one third are actually devious.
- *Malware*: it refers to the malicious users who can damage computer system and network .it represent in a number of ways and sometimes malware can be used to erase all the data on any system that run it.
- *Ransom ware:* it is a type of malware that locks or damage the a user's device then demand a payment to decrypt it. Lack of security in the IoT " jackware" may be the next frontier of ransom, and some of the IoT devices can be locked up for ransom.
- *Spear phishing:* it is a time tested form of attack in which the bogus emails that look authentic can be sent to the user to steals the confidential information like username and password to access finances.

Also, some of the network security attacks can also be possible such as denial of service, man in middle attack, spoofing, eavesdropping and so on. Some of the attacks are*:*

- Modification attack: In this attack an intruder alters packet header address to direct a message to some different destination or some modify the data content to be send.
- Timing attack: This attack is a side channel attack in cryptography in which the attacker compromised with the cryptosystem by analyzing the time taken to execute the cryptographic algorithm

- Dropping attacks: This type of attack is a type of denial of service attack in which a router supposed to relay packet instead of discard the packet.
- Fabrication attack: In this type of attack a fake message is inserted into the network by an unauthorized person which results in loss of confidentiality, authentication, and integrity of message.

III. LITERATURE SURVEY

In this section, survey on IoT networks, applications and their attacks have been done.

Jozef Glovaa, Tomáš Sabola, Viliam Vajdaa[7],in this paper explains the smart devices that come in existence also leads to the fast environment. with the increasing devices the business opportunities also increases which leads to the automation, production of devices maintenance and so on environment converges to the smart environment that makes energy ,transport, health intelligent this new invention change the business in the way of marketing and distributed products. this paper also show the importance and usefulness by applying value-based functions to new business model based on internet of things and how this sustainable business can be developed for an IoT platform.

Grant Ho, *et al*. [8], in this paper author explains the smart locks that replaces the traditional locks, these locks can be operated through mobile phones. But the security of these locks are the main challenge for the users. Here author explains some attacks on smart locks and analyze the five commercial locks with respect to these attacks. in this author explains the security analysis and the four threats like physical attacker, revoke attacker and replay attacker who attacks the smart locks. security goals can be explained and prevent the unauthorized user to unlock the door. author proposed two approaches to defend the attacks and provide better security for the internet of things.

Rolf H. Weber [9], n this the author describe the security and privacy challenges as authentication, access control, client privacy is the major concern , international challenges established the task on research of the legal aspects of the internet of things. Privacy enhancing technologies can be discussed such as virtual private network(VPN), transport layer security(TLS),DNS security extension and private information retrieval. the european commission provides the legal aspects to the radio frequency identification in 2009 but there are still remain some milestones . four challenges can be establishes are verticality, global , ubiquity and technicality ,these are the requirements for establishing legal framework for IoT environment .the author explain the legal aspects to know more about the privacy of IoT and encounter that the effective regulations can be established before the proper IoT take place in the scenario.

GAN Gang, *et al.* [10], IOT and give some solutions to overcome these risks .there is a difference between internet and internet of things where IoT can depend on some aspects like real time, safe and reliable and resource assurance .here author discuss the two big problems that is IPV4 address and the network itself security are the two bottlenecks. sensor network should have the ability to fight against DOS attacks. Encryption mechanism can be used to hide the data during transmission. hop by hop encryption is not suitable as it cannot hide the text message on transmission where end to end encryption is also not suitable due to the destination address can be revealed to the public where the authorized user can attack the system. the author conclude that the network security is the main concern where a single mistake can hack the whole network.

Somayya Madakam, *et al*. [11], in this paper authorities the overview of internet of things, their architecture, the new technologies, their daily usage and the how the things can incorporate the new world .due to the development of IT technology there is a great change in the life of people where IoT can track and has ability to code objects which help the companies to develop their business in fast rate. the author explain the time series, requirement, aliases and many more which helps the user to start with the IoT. the recent technologies that take place are RFID, some protocols, electronic product code, barcode, wifi, bluetooth, zigbee, near field communication, actuators. So, the IoT can make the future automotive. There are still some standardization by the government and the some privacy and security issues are the future recommendations.

Shubham Bhatia, *et al*. [12], this paper explain the concept of IoT their technology like RFID tags which used radio waves to identify the item , sensor that collect the data from environment and send it to other devices. They explain the trends that devices can interact and take decision independently and the architecture by ITU having five layers sensing ,accessing ,networking ,service and interface layer.

Rolf H. Weber, Evelyne Studer [13], in this paper they explain the cybercrimes security, that firstly they explain the issues of security like integrity, confidentiality, authenticity. Due to mass scale development of IoT devices can increase the threat of attacks publically or privately .there is no definition of cybercrime as ITU international telecommunication union explain the cybercrime as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets ".they explain the cyber landscape by threat agents, threat tools and threat types. further they explain the IoT technologies as RFID tags, sensors and acutators which are responsible for the transfer of data from one place to another through network . the vunerability of attack like lack of transport of encryption data, insufficient authorization and authentication, insecure web surface ,insecure software and firmware. sol some of the legal frameworks can be made like budapest convention and so on some legal frameworks or government policies.

From the survey, observed that the internet of things technology is so vast that the number of connected devices can be increasing day by day which in turns the organization are concerned with the degree of reliability of these devices. Radio frequency identification (RFID) and sensors are the technologies that are responsible for the transmission and the communication of data from one place to another. The numbers of components of the internet of things are increasing which leads most of the components unattended, so, the authorized user can easily hack the system. So, there is a need to secure the IoT system with good infrastructure. The biggest challenge of IoT is the security. A poorly design IoT device can leak or expose the original data or important information in authorized person. IoT brings more benefits for the people but it also raise a number of problem concerning security and

privacy which is the main barrier to adopt IoT system. So it is important to build the confidence among users to adopt the IoT culture with confidentiality, integrity and authority of data. So to preserve the integrity and authentication of data the cryptographic algorithms can be used to secure the data in the IoT environment but the conventional cryptographic algorithms are not supported the IoT constrained devices due to their high complexity and the large block size. The security, performance and the resource requirement of conventional cryptography algorithms are optimize for the desktop environment so it is difficult to implement in resource constrained devices of IoT. To overcome from conventional algorithms we use the term lightweight cryptography, the term was invented by NIST in 1999[14].

IoT has many applications in the area of smart cities, where the urbanization can be done with the sensors, automation can be done so that the response of each activity can be observed. Green IoT can be made by the integration of social network with IoT[15]. Another area of application can be observed in the health care centre where the private data can be transfer safely one mistake can result in the loss of life, so different methods can be applied for the integrity of data in health care centre[16]The cancer informatics of cancer centre announced the collaboration of big data methodologies in the cancer care. Most of the patients spend their life outside the clinic so IoT introduce PGHD unparalleled program in which the cancer patient can be under smart home environment so that their each move can measure their heart rate, weight, blood pressure ,galvanic skin response, hydration and so on[17].IoT can help in the transportation system for tracking by using RFID tags, tags can be inserted in the cars or the transportation system to track the location of origin and destination, thus the IoT can help in the logistics industry to improve the quality of products [18]. T implement these application in future, the IOT environment would be secure enough. So the lightweight algorithms can be introduce for the constrained devices of IoT to overcome the problem of security and privacy.

NIST has started the project of lightweight cryptography in 1999 when the current NIST approved cryptography algorithms cannot fit into the resource constrained devices of IoT, where the plans for the standardization of these algorithms can be discussed [19]. In this report, the performance advantages over conventional algorithm like smaller block size that is 64bit rather than 128bit is used, smaller key size, simple rounds that is use 4-bit s-box rather than 8bit s-box in AES , simple key schedule, and minimal implementation. The lightweight primitives and the standards can be discussed with the NIST project[20] having some requirements like security strength, flexibility , cipher-text expansion and so on. The report can give the overall view of the lightweight cryptography with some future questions.

IV. LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS

So many lightweight cryptographic algorithms can be designed but we restrict our vision on recent algorithms that are recently used in IoT devices such as PRESENT, SIMON and SPECK AND PICO.

PRESENT: it is presented as a lightweight cryptography algorithm in ISO/IEC 29192-2:2012 [21], it resolve the differential attacks on 31 rounds. It is used as a ultra lightweight algorithm for the security. It work on substitution layer having 4bit input and s-box as output for hardware implementation. It has a key size of 80 or 128bits and block size of 64bits.

SIMON and SPECK: It is more flexible and secure algorithm which perform a variety of implementations on given platform. SIMON is developed for the optimization of hardware devices where as SPECK is used for software devices. They supports a variety of block sizes of 32,with key size of 64bit, 48bit block size with 72,96 bit key size, 64bit block size with 96,128 bit key size, 96 bit block size with 96, 144 bit key size and 128 bits block size with 128,192,256 bits key size[22]. They have better throughput than PRESENT algorithm.

PICO: it is substitution and permutation based network based on SPECK and SIMON. It consumes less flash memory than PRESENT and has a strong substitution layer. It operate on block size of 64bits and key size of 128 bits. It has a very compact structure and consumes less lower than PRESENT algorithm[23].

These are the some lightweight algorithms that used in some IoT devices or resource constrained devices. The comparative analysis of some lightweight algorithms can be discussed in table1.

Table 1: Comparative Analysis of Lightweight Algorithms

ALGORITHM	DATA SIZE	KEY SIZE	NO OF ROUNDS	STRUCTURE	POSSIBLE ATTACK
AES[24]	128	128/192/256	10/12/14	FIESTAL	NOT ANY
DES[25]	64	56	16	FIESTAL	BRUTE FORCE ATTACK
TRIPLE DES[26]	64	168	48	FIESTAL	MEET IN MIDDLE
PRESENT[22]	64	80/128	32	SUBSTITUTION	-
PICO[27]	64	128	31	SUBSTITUTION & PERMUTATION	-

V. CONCLUSION

In this review paper, we explain the concept of IoT, their origin, architecture and security concepts. Firstly the need of IoT is explained with the architecture and to resolve the security cryptography technology is used. The present attacks in IoT can be explained. From the literature survey the need of security is a major concern in IoT devices, so to resolve the attacks the term lightweight cryptography term can be used in which the block size is reduced for the constrained devices of

IoT. Some algorithms like PRESENT, PICO, SIMON AND SPECK can be explained with the dimensions of block size and key size which are used for the constrained devices with security.

VI. REFERENCES

[1] Research on the architecture of IoT in advanced computing theory and engineering. 2010.

[2] Jozef Glovaa,, Tomáš Sabola , Viliam Vajdaa, "Business Models for the Internet of Things Environment," Science Direct, 15 (2014) 1122 – 1129 .

[3] S.C.B. Intelligence, Disruptive civil technologies, in: Six Technologies with Potential Impacts on US Interests Out to 2025, 2008.

[4] https://www.postscapes.com/internet-of-things-history/

[5] Carnegie Mellon University – CMU SCS Coke Machine

[6] Transmitter.ieee.org

[7] Jozef Glovaa, Tomáš Sabola, Viliam Vajdaa," Business Models for the Internet of Things Environment," Elsevier science direct volume 15, 2014, Pages 1122-1129.

[8] Grant Ho Derek Leung, Pratyush Mishra, Ashkan,Hosseini, Dawn Song, David Wagner," Smart Locks: Lessons for Securing commodity internet of things devices," ACM, '16 May 30-June 03, 2016.

[9] Rolf H. Weber," Internet of Things – New security and privacy challenges," ELSEVIER science direct.

[10] GAN Gang,LU Zeyong,JIANG Jun,"Internet of Things Security Analysis," IEEE 30 August 2011.

[11] Somayya Madakam, R. Ramaswamy, Siddharth Tripathi," Internet of Things (IoT): A Literature review," scientific research Vol.3 No.5, May 2015.

[12] Shubham Bhatia1, Abhishek Chauhan2, Vaibhav K. Nigam3, "The Internet of Things: A Survey on Technology and Trends" International Research Journal of Engineering and Technology," (IRJET).

[13] Rolf H. Weber, Evelyne Studer ," Cybersecurity in the Internet of Things: Legal aspects," ESLSEVIER 10.1016/j.clsr.2016.07.002.

[14] www.nist.gov

[15] Nilesh Mali1, Prof A. B. Kanwade,' "A Review on Smart City through Internet of Things (IOT),"Volume 2, Issue 6, June 2016

[16] K. Niranjana Devi, R. Muthuselvi," Secret Sharing of IoT Healthcare Data Using cryptographic algorithm," International Journal of Engineering Research Volume No.5 20 May 2016.

[17] Arlene E. Chung, MD, MHA, MMCi, Roxanne E. Jensen, PhD, and Ethan M. Basch, MD, MSc. "Leveraging Emerging Technologiesand the "Internet of Things" to Improve the Quality of Cancer Care," jop.ascopubs.org,Volume 12 / Issue 10 / October 2016.

[18] B. Karakostas, "A dns architecture for the internet of things: A case study in transport logistics," Procedia Computer Science, vol. 19, pp.594–601, 2013.

[19] NISTIR 8114 Report on Lightweight Cryptography Kerry A. McKay Larry Bassham Meltem SönmezTuran Nicky Mouha Computer Security Division Information technology laboratory, march 2017.

[20] International Standard ISO/IEC Information Technology - Security Techniques. Lightweight Cryptography. 2012.

[21] Bogdanov A, Knudsen L.R, Leander G, Paar C, Poschmann A, Robshaw MJ, Seurin Y, Vikkelsoe C. Present: "An Ultra-Lightweight Block Cipher. Berlin Heidelb,": Springer; 2007. p.0 450–66.

[22] Ray Beaulieu, Douglas Shors ,Jason Smith, Stefan Treatman-Clark ,Bryan Weeks, Louis Wingers,"THE SIMON AND SPECK FAMILIES OF LIGHTWEIGHT BLOCK CIPHERS," National Security Agency 9800 Savage Road, Fort Meade, MD 20755, USA, 19 June 2013.

[23] Gaurav Bansod , Narayan Pisharoty, and Abhijit Patil, " PICO : An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing," Defence Science Journal, Vol. 66, No. 3, May 2016, pp. 259-265.

[24] Shivlal Mewada, Pradeep Sharma, S. S. Gautam," Exploration of efficient symmetric AES algorithm,",IEEE, 19 September 2016, 10.1109/CDAN.2016.7570921

[25] C.P. Sotiriou, Y. Papaefstathiou." Design-space exploration of a cryptography algorithm," IEEE, 01 June 2004, 10.1109/ICECS.2003.1301922.

[26] Dudhatra Nilesh, Malti Nagle," The new cryptography algorithm with high throughput,t",IEEE, 16 October 2014, 10.1109/ICCCI.2014.6921739.

[27] Gaurav Bansod, Narayan Pisharoty, and Abhijit Patil," PICO : An Ultra Lightweight and Low Power Encryption Design for Ubiquitous Computing, " Defence Science Journal, Vol. 66, No. 3, May 2016,