www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-7, Issue-3, Jun 2019
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Security in Internet of Things (IoT) Hashing Cryptographic Functions

Himanshu Kumar Shukla[1*], Satyam Dubey[2]

[1,2] Department of Computer Science & Engineering, BNCET, Lucknow (UP), India

[*]*Corresponding Author: himanshu0590@gmail.com, Tel.: +91-9415039360*

Received: 23/May/2019, Accepted: 18/Jun/2019, Published: 30/Jun/2019

***Abstract*—** Internet of Things (IoT) begins new era of wireless interconnected devices, where every device have connectivity among each other. As looking towards today IP-Based communication structure all protocols plays a vital role in providing ubiquitous connectivity in all existing devices. All these devices are connected to each other in IoT and perform communication by using IP-based protocol. Throughout this communicating structure devices under network connection can be protected but for IoT connecting every device with Internet may take network under unsecure zone. These small issues created big problem to challenge security measures existing these days in IoT. To resolve these type of problems of security we analysed existing algorithms and hash cryptographic function and presented a modified Algorithms to do same operation but in less time as well as in less memory space. We also discussed present research for IoT's security requirement and with also about future research path for IoT security and privacy.

***Keywords*—**Internet of Things (IoT); Wireless Sensor Networks (WSNs); Quality of Services(QoS); RC-5; Skipjack; AES; Low Power Wireless Personal Local Area Network (LoWPAN); Radio Frequency Identification (RFID).

I. INTRODUCTION

Because all impressive advantages of Networks of wireless sensors (WSNs) it has been main point of attraction for researchers during these past years. The very need of specific network for future generation throttles more work for new things which can be update in it. It contains many sensors that are wireless and which are combined to each other in a network and fetch particular amount or needed information. After this acquired information then go for its operation and transmission of processed information, otherwise directly send to the different sensors to do trend analysis and surveying the data. Those devises which are associated with IoT are visional that they are very small and cheap, an microprocessor, an battery, transceiver of less power consumption and an sensor. Four fundamental challenges occurred in IoT are follows:-

- Power Management
- Functioning of IPv6
- Security
- Standardization

In today era use of IoT is being using everywhere like Water supply, Electricity in major cities and also holds sensitive data like hospitals, banks, economics status, personal information.Hence a system need to be provided to secure these sensitive data from unauthorized access or hackers. IoT contain some phenomena like Low Power Wireless Personal Local Area Network (LoWPAN), Wireless Sensor Network (WSN), Machine-2-Machine Communication (M2M), Radio Frequency Identification (RFID). In recent days due to rapid increase in IoT technology implementation several security and privacy related issues have been observed. Due to connectivity everywhere all devices connected and communicate, this issues is mostly pronounced in these years. Constant increasing use of IoT always leaves major flaws in security and privacy. Hash cryptographic functions always been used as most secure method in security. Hashing includes secure transmission of data from source node to end node. Scalability and limited capabilities of devices also mean that old methods of cryptography are insufficient. The fundamental baseline of security must be robust and also be dynamic so that it can be updated and can be implemented with limited resources in future days too(>20years). Dealing with large population of devices it is understandable that some devices may get compromised. Therefore, implemented system must be meeting all requirements of IoT in terms of Security, privacy and reliability. As now internet communication evolved into IoT which composes of sensing devices, an appropriate secure communication method is required. In past recent years contribution of research shifted towards developing Low-Power device and implements them into network of internet. Many big research organizations like Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF) has already proposed methods in which stack of protocol has been implemented to perform end to end communication among all small devices, sensors, cameras etc. Here in this paper we focus on implementing standardized and secure communication protocol for IoT. Throughout paper we point security communication for IoT, various technologies used

for communication in IoT. We will also discuss various challenges arises and their possible solution techniques (Through hashing) as well as future strategies to solve further more issues that may can arise in future.

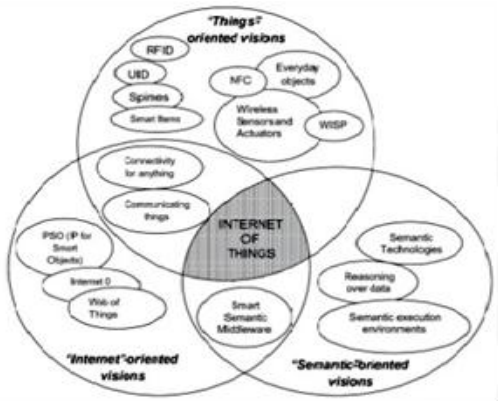

Fig.1. Internet of Things- a symbiotic representation between "Internet"-oriented visions, "Semantic"-oriented and "Things"-oriented visions.

II. Related Work

Internet Engineering Task Force (IETF) has taken great efforts to standardize security measures with IoT. Application layer protocol has been adopted specially constraints to an IoT application. Constrained Application Protocol (CoAP) is top example of secure protocol. CoAP operates basically on Datagram Transport Layer Protocol (DTLP). Hence it is necessary to implement enhance form of DTLP for IoT ecosystem. It basically requires three things extended record layer for communication (multicast), raw public key and profiling of DTLS in context to compromise size implementing on embedded devices. If a wireless sensor is attached to IoT many challenges will arises like establishing secure data transmission between sensor and Internet Host and setup a secure channel for communication. A Sign Cryptography has been implementing between sensor and Internet host communication which can work in heterogeneous environment like online and offline mode to secure communication. This scheme secures communication from adaptive chipper text attack. It has several advantages first as confiditinatily, non-reputation, integrity and authentication in a one integrated step. Second step it performs cryptography in which sensor sends an encrypted request which only be open by public key infrastructure situated at Internet Host. In last step it performs signcryption into two step offline mode and online mode. In, online mode lightly information about message small computation is done. In, offline mode in absence of any information about message heavy computation needs to be done. This technique provides solution for basic problem integrating wireless sensor network in IoT. This mechanism only works when a node in Identity Based Cryptography (IBC) sends message to a node in public key infrastructure. It does not support reverse process hence provides security from outside attackers. The idea of applying IoT with smart homes we discussed earlier. An integrated system must discuss with its full brief introduction. This system has major status of scalability. With higher scalability this structure can be integrated with other technique but with same interface. Many factors also been introduced in communication to work with RFID tags. It also discusses that why currently present encryption algorithms like RC-5, RC-4, Skipjack are not applicable for secure encryption. Wireless sensor network contains many constraints like power consumption, speed. The security measures getting to be implemented must also take these constraints into consideration in which energy is a most important key factor. This energy consumption factors also increases life of system. The proposed encryption algorithm must contain some basic operations like shifting and Exclusive-OR so that system will be less dependent to hardware. By reducing hardware involvement much amount of energy can be saved in wireless sensor network. Since many challenges arising these days in IoT regarding security which are as follows:-

- Data protection and User privacy
- Identification and Authentication management
- Policies integration and Trust management
- Control access and Authorization
- End to End Communication security
- Attack dodging security system

We applied same fundamental used in conventional method of encryption in RC-4 but resolved issues of concatenation which are further discussed below. The small skipping of operation not only save memory in sensors but also saves energy throughout system. Which also makes system reliable and maintains integrity for future purpose? Due to less dependency on hardware system provides more scalability which further could be used for updating. Hence, Cryptography is been used for many past years in every field of security because output produces from hashing can't be obtained back even after reversing process also. Since hashing cryptographic technique is software oriented technique.

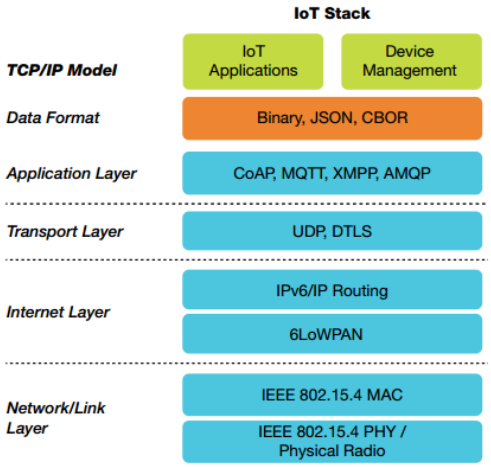

Fig. 2. Internet of Things "IoT" Stack Protocol Structue.

III. PROPOSED ALGORITHM

Major Concern that arises in communication of IoT based sensor network that security can be provided among sensors communication ,but when it comes to sensor and an Internet Host (IH) this situation takes security to new level where old conventional methods of cryptography is not well applicable. Therefore, instead of communicating each device to Internet we replace this structure from common access point where each device communicates to internet from this point. A cryptographic hash function ensures security with in wireless sensor network (Inside network). This algorithm is designed in keeping certain points regarding sensor nodes that they have less memory, less energy and less computation power. Hence, proposed algorithm is discovered in under less software support measures so it can be easily implemented on sensor nodes. Now According to above analysis we can divide main problem into two sub-problems:-

- Security Inside network among sensor nodes.
- Security when WSN is connected to internet.

To make it less software dependent we had made slight changes in existing algorithms in Input plain text block size and at place of public key we used one master key permutation for every round to produce cipher text of respective plain text. This change let limited 32 rounds of permutation for producing cipher text and this let less software computation as well as less memory consumption in sensor nodes as limited rounds leads to fixed storage of data during every permutation round.

IV. WORKING OF PROPOSED ALGORITHM

As we discussed above major problems arises when sensor nodes are connected to internet. Therefore, on the place of connecting every sensor node separately to internet, a common access point can be setup so that nodes can access internet from there. So that we can apply network security on a single access point which is easy to implement. This functioning makes it easier to stop unauthorized access from single access point which has been shown in fig. 3. This mechanism only work when sender is from Identity based cryptography and receivers from public key infrastructure. Therefore using other key and message sending reverse mechanism will also be applied. The main motive of developing this algorithm is just minimizing the computation process so that sensor nodes which usually used to have less specification can also secure.

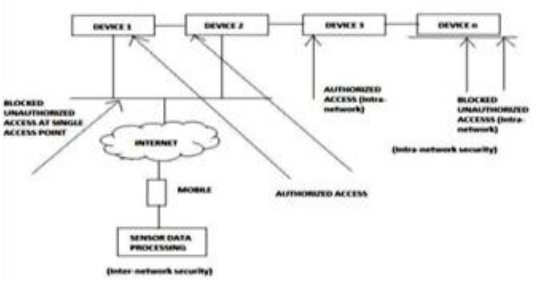

Fig. 3. Single Access Point Structure

The existing cryptographic algorithms on IoT to provide security measures are discussed below with their functioning and also functionality difference between existing algorithm and proposed algorithm.

RC-5

Under this algorithm plain text can be of size 32, 64 or 128 bits and size of the key is from 0 to 2048 bits. It can have multiple rounds from 0 to 255 but it usually takes block size of 128 bits which makes 12 rounds to complete form cipher text. Hence, then also RC-5 can be broken by differential attack due many number of rounds. More numbers of rounds are good for security but consume more CPU power

.

Skipjack

Plain text 64 bits and key size 80 bits. It is very unbalanced technique of 32 rounds. It is very unsafe for attack due to shorter size of key.

AES

Plain text 128 bits and key sizes can be 128, 192 or 256 bits. Also having 10, 12 and 14 rounds each. Adding round keys, shifting rows, adjusting columns etc. these are operation that takes place every round.

The proposed algorithm takes 64-bit as a plain text and uses a 128-bit master key as input. Which produces 64-bit of key (Cipher Text) as an output. Its complete rounds are 32 in count which consist some algorithmic functionality like initial processing, round function, sun-key division and final transformation. All other sub-keys are derived from master key. In each round we needed 4 keys which make 128 keys with 32 rounds. After each round changes have been done in plain text and which supported by modular division by 8 operations. To maintain integrity in RC-5 initial values are stored in S1V. Which takes space and makes algorithm more predictable and randomness cannot be achieved. Therefore, we removed this storage in our proposed algorithm to achieve randomness.

The initial permutation (S1V)

145,57,133,33,65,49,83,61,113,171,63,155,74,50,132,248,236,218,192, 217,23,79,36,72,53,210,38,59,54,208,185,12,233,189,159,169,240,156, 184,200,209,173,20,252,96,211,143,101,44,223,118,1,232,35,239,114, 114,109,161,183,88,66,219,78,157,174,187,193,199,99,52,120,89,166, 18,76,241,13,225,6,146,151,207,177,103,45,148,32,29,234,7,16,19,91, 108,186,116,62,203,158,180,149,67,105,247,3,128,215,121,127,179,9, 175,251,104,246,98,140,11,134,221,24,69,190,154,253,168,68,230,58, 153,188,224,100,129,124,162,15,117,231,150,237,64,22,152,165,235

Fig. 4. Initial Saved Value (S1V) in RC-5

Concatenation is also a complex operation requires more CPU cycles **S=Temp1.Temp2.Temp1** which is a cost effective function still this operation is removed from proposed algorithm.

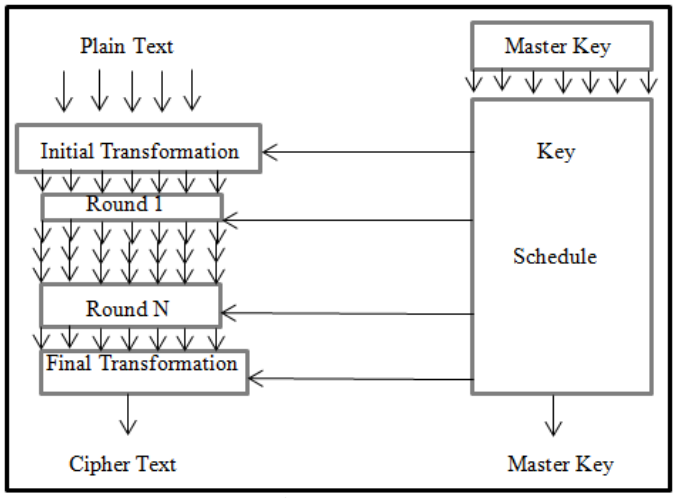

Fig. 4. Confidentiality architecture

Every hash algorithm has 3 fundamental steps i.e. Padding, Compression and truncation. Now describing functioning of proposed algorithm on basis of these fundamental steps.

PADDING RULE: - Under this rule message is divided in blocks of 512 bytes each and if last block doesn't add up to 512 then padding bits (followed by 0, 1) are added to make 512 bytes.

PADDING BITS+MESSAGE= 0mod512
Compression consist of three steps

- Key scheduling algorithm(KSA)
- Modified version of key scheduling algorithm(MKSA)
- Modified Random Generation Algorithm

Key Scheduling Algorithm (KSA): -
INPUT: - Message
OUTPUT: - State Array
Initialize state array 1-256
Apply A= (a+s[b] +C [Bmod64]) mod256 (it can be from 1-256)
Swap s[b] and s[a]

Modified Version Of Key Scheduling Algorithm:-
INPUT: - Message and State array
OUTPUT: - Update state array
Apply A= (a+ s[b] +C [Bmod64]) mod256 (it can be from 1-256)
Swap s[b] and s[a]

Modifies Random Generation Algorithm: -
INPUT: - State Array
OUTPUT: - Updated State Array
Do
b= (b+1) mod256
A= (a+ s[b]) 256
While (Message length)
Swap s[a], s[b]
KSA and MKSA are almost similar only changes occur in their input stream and initialization of state array is done in KSA.
TRUNCATION RULE: - One bit is taken from each 256 and added up with 16 bits of index which gives complete 272bits (34 bytes).
One bit change in plain text cause changes in cipher text hence diffusion is achieved.
Similarly One bit change in master key changes whole cipher text.
For example: -
PLAIN TEXT 0 1 2 3 4 5 6 7
MASTER KEY 0 1 2 3 4 5 6 70 1 2 3 4 5 128 1 25
CIPHER TEXT 1 40 1 2 6 6 0
If any attacker have cipher text which is 6 and having plain text alphabet T with it. Then also he cannot substitute value of 6 with H because every time change in plain text cause change in cipher text. Hence, algorithm produces different cipher keys for same plain text. Hence many operations are got removed in modified key scheduling algorithm since which put less computation in our existing algorithms. So main factor that works in our algorithm is plain text size of 64-bits and a common master key 128 bits which produces 64 bits size of cipher text as output hence less operation and small computation makes it works really fast. RC-4 itself works faster (3/47) times then MD4. Our proposed algorithm itself contains less operations then RC-4. As we can also see in increase in number of output bits as total sum of 272bits. It also significantly works on 8-bit processors as RC-4 do.

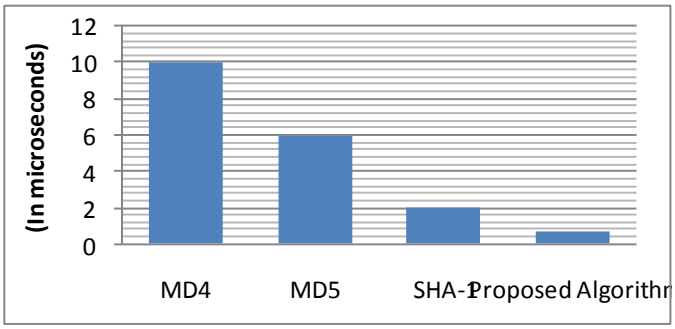

Fig. 5. Relative Compare of Authentication Algorithms

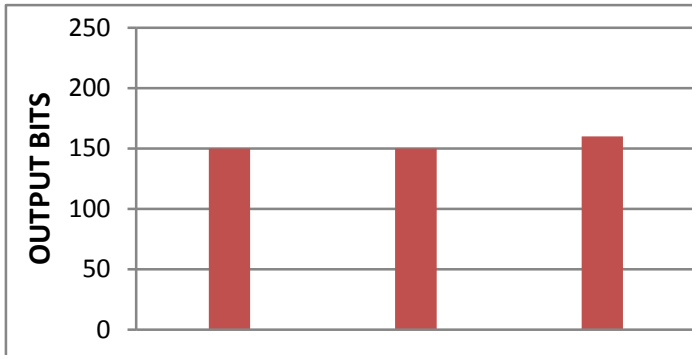

Fig. 6. Comparison on basis

IV. CONCLUSION

After calculating and collecting all the results in every possible situation that proposed algorithm is less software dependent which makes it reliable for sensor nodes. It is difficult to break security measures of proposed algorithm by brute force. Main fundamental quality of cryptographic function confusion and diffusion can achieved. Single change in plain text causes change in master key as well as in cipher text too. It is highly secure, efficient and fast ($3/50^{th}$ of time) when compared to existing algorithm.

REFERENCES

[1] Alberto M.C Souza and Jose R.A. Amazonas, 'A Novel Smart Home Application Using an Internet of ThingsMiddleware',European Conference on Smart Objects, Systems and Technologies, pp. 1-7, June 2013.

[2] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi, 'Internet of Things for Smart Cities', IEEE Internet of Things Journal, Vol. 1 No.1, pp. 22-32, February 2014.

[3] Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman,'Wireless Sensor Networks and the Internet of Things:Do We Need a Complete Integration?', SecloT Japan, November 2010.

[4] Chang, K. C. Gupta and M. Nandi, "RC4-Hash: A New Hash Function Based on RC4", Proc. INDOCRYPT, LNCS 4329, pp. 80-94, Springer, 2006.

[5] Fagen Li and Pang Xiong , 'Practical Secure Communication forIntegrating Wireless Sensor Networks Into the Internet of Things'

[6] Kelly, S.D.T., Suryadevara, N.K., Mukhopadhyay, S.C.,'Towards the implementation of loT for Environmental Condition Monitoring in Homes', Vol.I 3 No. 10, pp. 3846-3853, August 2013.

[7] M.Tharani, M.Senthilkumar , 'Integrating Wireless Sensor Networks into Internet Of Things For Security' IJIRCCE VoI.2 No.1, March 2014.

[8] Ming Wang, Guiquing Zhang, Jianbin Zhang, Chengdong Li, 'An loT-based Appliance Control System for Smart Homes' ICICIP , pp. 744-747, 2013.

[9] Dr. Pritam Gajkumar Shah, Javeria Ambareen, 'A Survey of Security Challenges in Internet of Things (loT) Integration with WSW, AUSJOURNAL,2014.

[10] Pormante, L. Rinaldi, C. Santic, M.Tennina, S., 'Performance analysis of a lightweight RSSI-based localization algorithm for Wireless Sensor Networks', ISSCS , pp. 1-4, June 2013.

[11] Sang-Eon Lee, Sang-Ho Shin, Geum-Dal Park and Kee-Young Yoo, 'Wireless Sensor Network Protocols for Secure and Energy- Efficient Data Transmission' Proceedings of the CISIM'08 on Computer Information Systems and Industrial Management Applications, pp. 157-162, June 2008.

[12] Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig,'Securing the Internet of Things A Standardization Perspective', IEEE INTERNET OF THINGS JOURNAL, Vol. I, No. 3, pp. 265-275, June 2014.

[13] Wade Trappe, Lawrence C. Washington, 'Introduction to Cryptography with Coding Theory.

[14] Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, Dong Hoon Lee, 'Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks' International conference on Information assurance and security, pp. 73-76., 2008.

[15] Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, 'Smart community An Internet of Things Application', IEEE Communications magazine, Vol. 49 No.ll, pp. 68-75, November 2011.

Author Profile:

Mr. Himanshu Kumar Shukla have completed B.Tech Information Technology in year 2012 and M.Tech in Computer science & Engineering in year 2015 form Shri Ramswaroop memorial University Lucknow. He is currently working as Assistant professor at AKTU, Lucknow, India. His area of Research is Cryptography Security System with IOT, trying to get more and more achievements in this field. He has 4 years of teaching experience and 2 years of Research Experience.

Mr. Satyam Dubey have completed B.Tech Computer science & Engineering in year 2014 and M.tech in Computer science & Engineering in year 2018 form Amity University Noida India. He is currently working as Assistant professor at AKTU, Lucknow, India. His area of Research is Cryptography Security System with IOT, trying to get more and more achievements in this field. He has 1 year of teaching experience, 2 years of Research Experience, and 1 year Industrial field Experience.

