Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

TRUST MANAGEMENT OF COMMUNICATION ARCHITECTURES OF INTERNET OF THINGS

Dr. Wang Haoxiang,
Director and lead executive faculty member,
GoPerception Laboratory, NY, USA
Email id: hw496@goperception.com.

Abstract: The Internet of things is the basic paradigm with the cluster of techniques that ensure innovations in the service rendered in various applications. It aims to develop a seamless connection between the tangible objects around and the information network in turn to provide a well-structured servicing to its users. Though the IOT service seems to be promising, the risks still prevail in the form of privacy and the security in user acceptance in utilizing the internet of things services, and its application. This makes the trust management very important for the internet of things. So the paper puts forth the distributed block chain involved trust system to manage the conveyance infrastructures of the internet of things paradigm. The evaluation of the proposed model evinces the enhanced security provided for the nodes of the IOT as well as its information exchange.

Keywords: Internet of Things, Block Chain, Light Weight Cryptography, Security and Privacy.

1. INTRODUCTION

The Internet of things has enabled a seamless communication between the tangible things that lie all around in the surrounding environment allowing them to act and react automatically without any human intervention. The limit less advantages of the internet of things has made it quiet prominent among most of the applications as the IOT ensures better money as well as time management. It is expected that the popularity of the internet of things would increase more and more in the forthcoming years in turn increasing the number of devices connected to it [1]. The increase in the size of the network eventually results with higher ventures of privacy, security and trust threats.

As the internet remains as the soul and heart of the internet of things, the security threats prevailing in the internet are more likely to attack the IOT paradigm also [2]. So it becomes necessary to protect the infrastructure and the information transfer in the internet of things by deploying a security measures to protect the devices of the internet of things as well as the information transfer in it from attacks [3].

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

The attacker usually identifies the vulnerable nodes to launch the security threat to the devices. This makes the trust management essential between the communication infrastructures of the internet of things. The figure.1 below shows the frame work of the trust management [4].

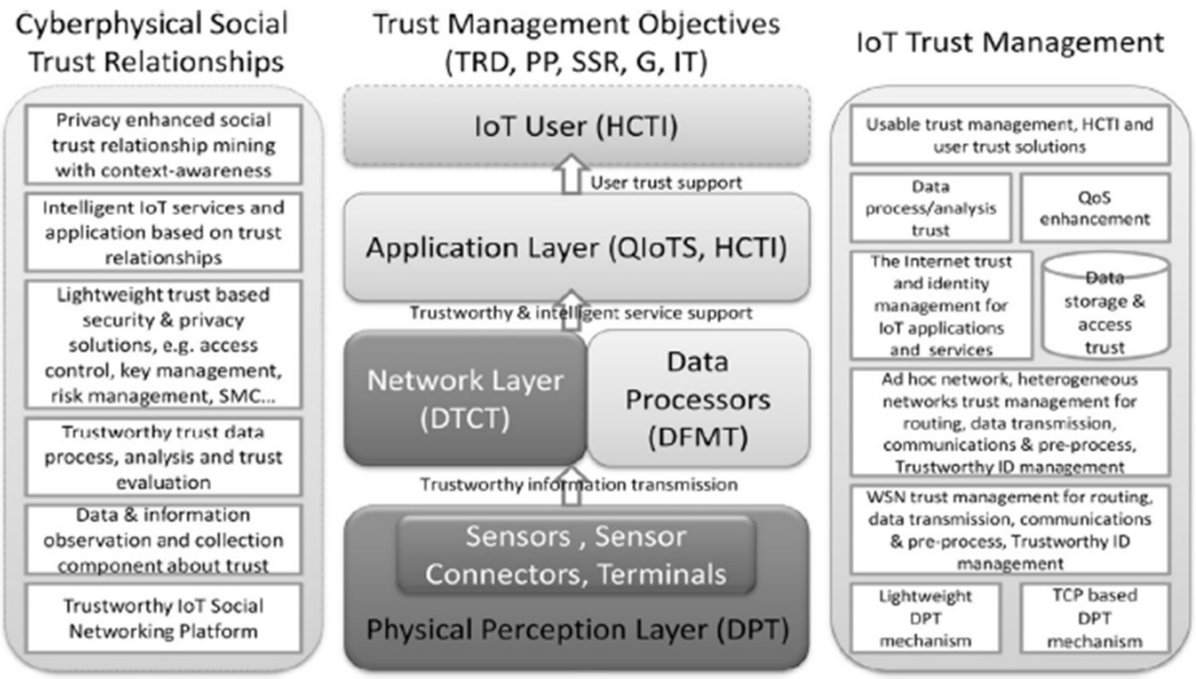

Fig.1 Trust Management Infrastructure [4]

The major problem in the internet of things paradigm is its inefficiency in the management of the node identity, due to the heterogeneous connection properties such as the life span of the connection, service demands and the degrees of the trust [5-10].

The paper proposes the distributed block chain deployment (DBC) in the internet of things to manage the trust of its communication infrastructure [11-13]. The paper further involves the light weight cryptography (LWC) to secure the information transfer in the internet of things.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

The paper proceeds the block chain deployment and the light weight cryptography to manage the trust of the nodes and the information transfer respectively in the IOT in section 2. The details of the end results acquired are provided in the section 3 and the section 4 holds the concluding part that presents the summarization of the work done in the paper.

2. PROPOSED DESIGN

The internet of things is usually comprised of multitudes of electronic devices that are heterogeneous and aided with varying hardware setups to establish connection among the other tangible commodities. Due to the heterogeneity and the changing communication set up of the IOT, the Internet of things[14] become vulnerable to the hackers for example the devices used in the internet of things could be any portable device (smart phones or tablets or laptops etc.) that holds a different configurations for the hardware used in it this makes them heterogeneous and more over all the devices do not have constant connection to the network , some extend a constant connection , some extend a periodic connections that can be disabled or enabled whenever needed and some always remains offline. This makes the hacker to introduce the fake nodes into the IOT paradigm and manipulate the nodes in the communication environment. So the authentication becomes essential for the devices involved in the IOT network before a communication has to be extended. The fig.2 shown below provides the vulnerabilities found in the IOT due to the connection changes that exists for different type's devices.

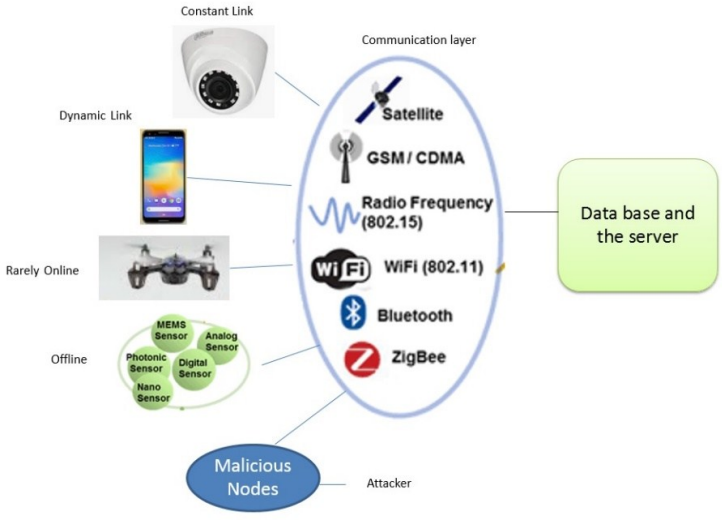

Fig.2 IOT Device Heterogeneity and Dynamic Links

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

2.1. DBC FOR MANAGING THE TRUST IN THE NODES

The proposed design utilizes the multi-tier block chain (M-BC) involved node identity administration (NIA) to handle the dynamic internet of things environment. The steps below in table.1 details the procedure of the M-BC involved NIA for the managing the trust in the communication architectures of the IOT.

Step 1	**Add all the IOT devices as entities to the block chain**
Step 2	**Assign unique identities to the devices (nodes)**
Step 3	**Categorize the devices based on the configuration (to avoid the heavy storage and computation)**
Step 4	**Define tags for the devices in the IOT as less mass devices , complete devices and supervision devices.**
Step 5	**Assign tags to the devices based on the life span of the connection and the hard ware configurations**

Table.1 Procedures of M-BC involved NIA

The tags assigned served as an authentication and enabled to confirm that no illegal access was taking place. The less mass devices were assigned to the devices with the very low computation capability and less lifetime, the devices that were always in connection with the IOT was tagged as the complete devices and the device with the very less computation capacity and increased life time was tagged as supervision nodes. The block chain is assigned particular to the complete devices and the less mass devices are allowed to take part in the DBC without overloading the complete devices. The DBC incorporated with the identity-verification makes possible the NIA by enhancing the level of trust in the devices and reducing the snooping of the attackers, as it would be very difficult and costly for the attackers to retain the link with the network and frequently fake the identities respectively

2.2. LWC TO PROTECT THE INFORMATION EXCHANGE IN IOT

The Distributed-BC deployment in the IOT allows a trust management among the nodes in the internet of things overcoming the difficulties in the NIA that prevails as the loop hole for the illegal access. Further the proposed

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

model also sets the cryptography into action in the application layer to secure the end to end data conveyance. The proposed model uses a light weight cryptography. The light weight cryptography unlike the conventional cryptography methods aims to minimize the size of the circuit, the ROM/RAM, the power used, the delay in transmission and enhance the throughput.

The light weight security incorporates a substantial security [15-17] level compared to the convention al cryptography methods. It reduces the difficulties in the implementation as it utilizes shorter length blocks or the secret key which is usually a 64- bit or 80 bit. The light weight cryptography methods are roughly classified in two types similar to the conventional cryptographies as symmetric and asymmetric based on the secret key generation. The proposed method utilizes a symmetric encryption-decryption method in the application layer of the IOT to secure its information transfer.

The blocks /stream ciphers are the core functions of the cryptography based on symmetric key. The core functions are applied to the data packets that are ready for transmission for the purpose of authentication. This process is known as the block cipher mode (BCM). The authentication of the complete information is known as the Cipher Block Chaining-Message Authentication Code (CBC- MSGAC). The efficiency in the functioning of the BCM needs to be improved to render a light weight cryptography. The fig.3 below shows the BCM operation mode

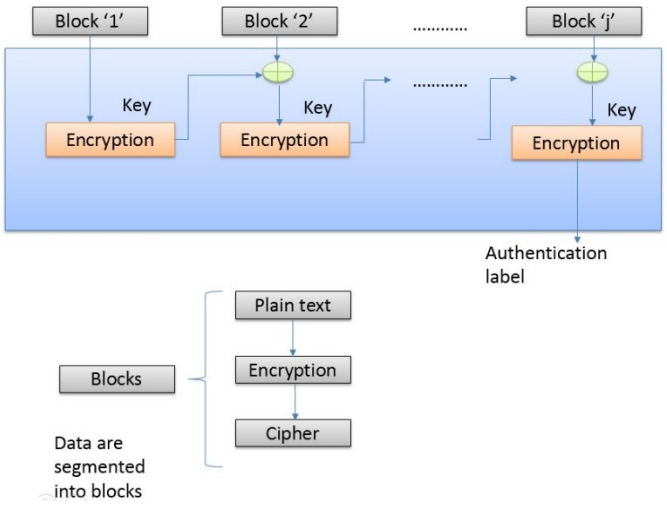

Fig.3 Schematic of BCM

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

The TWINE-1[17] a light weight block cipher is employed in the proposed method. The Description of the TWINE-1 block cipher is listed below in the table.2

TWINE-1	Advanced Encryption Standard
Has 2k gates	Has 14 k gates
Efficiency is higher	Efficiency is lower compared to the TWINE-1
Operates at twice the speed of AES	Operates a speed lower than TWINE-1
ROM size 512 bytes	ROM size 1K bytes

Table.2 TWINE and AES Description

The employment of the Light weight cryptography in the IOT information exchange enhances the efficiency in the end to end communication by activating an end to end security [18-20], ensures a lower power consumption and lower foot print of the cryptographic primitives compared to the conventional cryptography. The proposed method could be very effective in the industrial plants, health care and other applications where a protection for the personal information is necessitated.

3. RESULTS

The Distributed-Block chain for the administrating the Node identity is developed on the Ethereum platform that is capable of developing as well as evaluating the set up. The proposed architecture with the block chain in the NIA is evaluated to ensure its degree of management in presence and the absence of the compromised devices (CD). The fig.4 show the trust level for the IOT network in the absence of the malicious nodes, with and without the DBC involvement.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

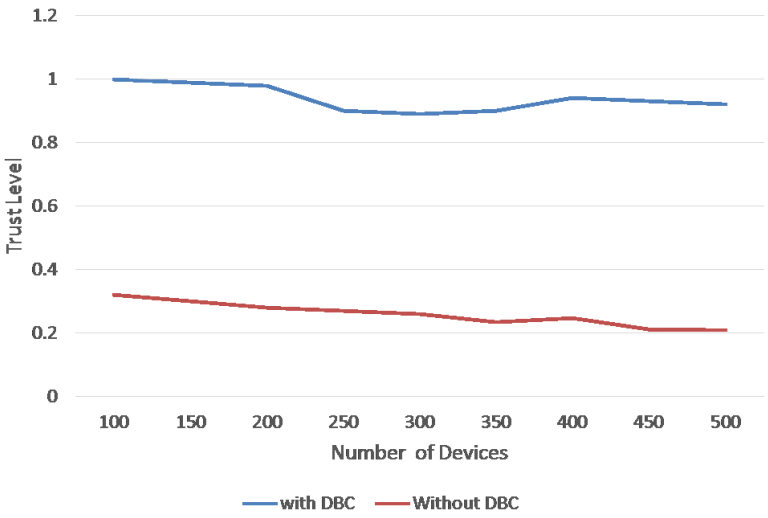

Fig. 4 Trust level of IOT in Absence of CD

The fig.5 shows the trust level of the IOT in the presence of the CD with and without the involvement of the block chain that is distributed.

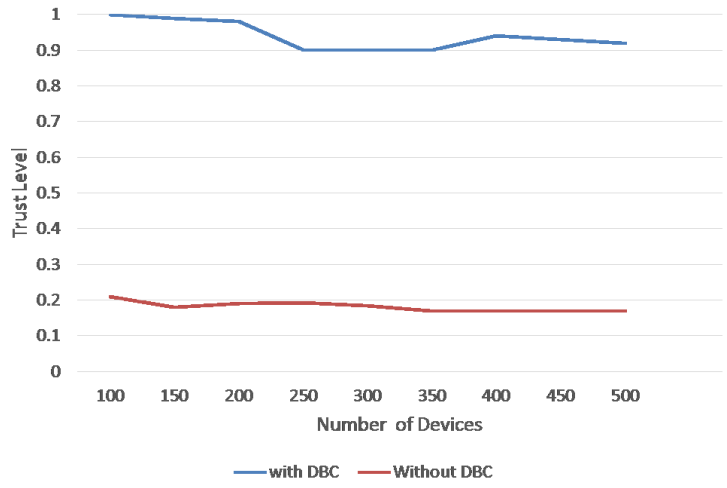

Fig. 5 Trust level of IOT in Presence of CD

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

The percentage of the security enhancement achieved by activating the end to end security through the light weight cryptography is evaluated with the network simulator-2 for varying number of interactions in the internet of things is presented below in the fig .6

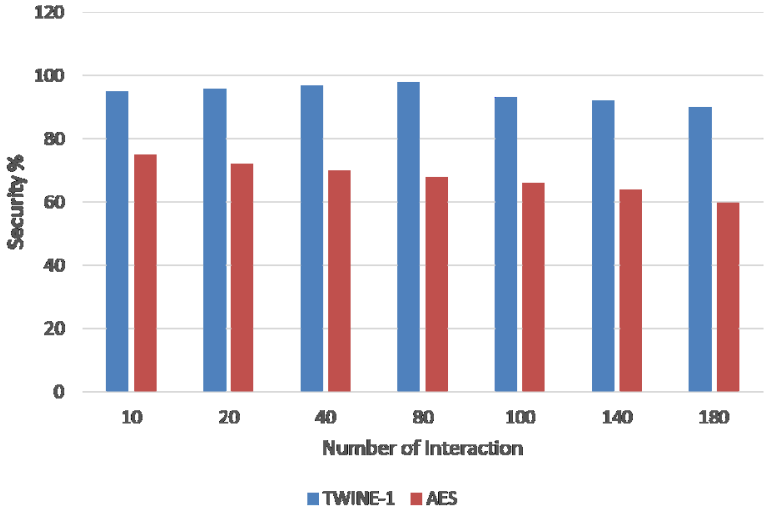

Fig.6 Security Percentage

4. CONCLUSION

The trust management that is very essential to avoid the security threats in the devices engaged in the internet of things is achieved in the paper by utilizing the multi-tier distributed block chain that provides a very efficient administration of the node identity eluding the snooping of the malicious nodes. Further to enhance the security level in the exchange of the information's the proposed method incorporates a LWC-TWINE that performs effectively in both hardware and software for activating the end to end security in the data conveyance. The evaluation of the proposed method shows the trust level and the security level gained by the multitier-DBC and the LWC-TWINE respectively. As a future scope the paper is to address the security breaches in the data collection layer by engaging the light weight cryptographic methods to it.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2019)
Vol.01/ No. 02 Pages: 121-130
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2019.2.005

References

[1] Raj, Jennifer S., and Abul Basar. (2019). QOS OPTIMIZATION OF ENERGY EFFICIENT ROUTING IN IOT WIRELESS SENSOR NETWORKS. “Journal of ISMAC”, 1(01), 12-23..

[2] Saied, Yosra Ben, Alexis Olivereau, Djamal Zeghlache, and Maryline Laurent. "Trust management system design for the Internet of Things: A context-aware and multi-service approach." *Computers & Security* 39 (2013): 351-365.

[3] Karthiban, Karthiban, Mr K., and Jennifer S. Raj. (2019). BIG DATA ANALYTICS FOR DEVELOPING SECURE INTERNET OF EVERYTHING. "Journal of ISMAC." , 1(02), 129-136

[4] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." *Journal of network and computer applications* 42 (2014): 120-134.

[5] Mugunthan, S. R. "SECURITY AND PRIVACY PRESERVING OF SENSOR DATA LOCALIZATION BASED ON INTERNET OF THINGS." *Journal of ISMAC* 1, no. 02 (2019): 81-91.

[6] Andrea, Ioannis, Chrysostomos Chrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges." In *2015 IEEE Symposium on Computers and Communication (ISCC)*, pp. 180-187. IEEE, 2015.

[7] Valanarasu, Mr R. "SMART AND SECURE IOT AND AI INTEGRATİON FRAMEWORK FOR HOSPITAL ENVİRONMENT." *Journal of ISMAC* 1, no. 03 (2019): 172-179.

[8] Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems." *Computer Communications* 97 (2017): 1-14.

[9] Suma, V. "SECURITY AND PRIVACY MECHANISM USING BLOCKCHAIN." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 45-54.

[10] Bhalaji, N. "QOS AND DEFENSE ENHANCEMENT USING BLOCK CHAIN FOR FLY WIRELESS NETWORKS." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 1-13.

[11] Eder, Thomas, Daniel Nachtmann, and Daniel Schreckling. "Trust and Reputation in the Internet of Things." *Universität Passau, Tech. Rep.* (2013).

[12] Pandian, A. Pasumpon. "ENHANCED EDGE MODEL FOR BIG DATA IN THE INTERNET OF THINGS BASED APPLICATIONS." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 63-73.

[13] Liu, Yan, and Kun Wang. "Trust control in heterogeneous networks for Internet of Things." In *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 1, pp. V1-632. IEEE, 2010.

ISSN: 2582-4104

[14] Sathesh, A. "ENHANCED SOFT COMPUTING APPROACHES FOR INTRUSION DETECTION SCHEMES IN SOCIAL MEDIA NETWORKS." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 02 (2019): 69-79.

[15] Shakya, Subarna. "AN EFFICIENT SECURITY FRAMEWORK FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT." *Journal of Artificial Intelligence* 1, no. 01 (2019): 45-53.

[16] Sivaganesan, D. "BLOCK CHAIN ENABLED INTERNET OF THINGS." *Journal of Information Technology* 1, no. 01 (2019): 1-8.

[17] Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." *Sony Corporation* (2008): 7-10.

[18] Bashar, A. (2019). SECURE AND COST EFFICIENT IMPLEMENTATION OF THE MOBILE COMPUTING USING OFFLOADING TECHNIQUE. Journal of Information Technology, 1(01), 48-57.

[19] Kumar, R. Praveen, and S. Smys. "A novel report on architecture, protocols and applications in Internet of Things (IoT)." In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, pp. 1156-1161. IEEE, 2018.

[20] Jyothirmai, Pondi, Jennifer S. Raj, and S. Smys. "Secured self-organizing network architecture in wireless personal networks." *Wireless Personal Communications* 96, no. 4 (2017): 5603-5620.

ISSN: 2582-4104