International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 3060-3067

Study on Lightweight Cryptographic Algorithms for IoT

[1]Archana S Nadhan, [2]Dr I Jeena Jacob, [3]Dr Brahmananda S H
[1]Research Scholar & Assistant professor, Dept of CSE, GITAM (Deemed to be University), Bengaluru Campus, Karnataka, India.

[2] Associate Professor, Dept of CSE, GITAM (Deemed to be University), Bengaluru Campus, Karnataka, India.

[3]Professor, Dept of CSE, GITAM (Deemed to be University), Bengaluru Campus, Karnataka, India.

Abstract

With the arrival of Internet of things, most of the current world applications are adopting IoT concepts as it makes them modular, efficient and fast. However, IoT devices are interconnected and persist across wider geographical locations; hence it coexists and leads to a greater security risk. As a result of this, it is at most important to analyse the existing cryptographic ciphers on such devices and decide if they are feasible in terms of execution time, memory consumption and efficiency. The crucial elements which need to be addressed in IoT are Security and Privacy. In the layered architecture, the available solutions for security are still vulnerable to attacks. Therefore, in order to strengthen the security, lightweight cryptographic algorithms are used. In this paper a comparative analysis is provided on existing lightweight cryptographic algorithms which are used for providing security in IoT.

Keywords**:** *Internet of Things, lightweight cryptography, Information security, throughput, efficiency.*

1. Introduction

Today's world depends on the information presented on internet, in the form of captured images or text. Here human being is involved for compilation of the information. But the main disadvantage with the human participation is that, less accuracy and time constrained, which might lead to inconsistent and incorrect data. Hence, a system without any human to machine inter communications needed, which can automatically capture the data and transfer it to internet.[1]

The term "Internet of Things" (IoT) was coined in the year 1999, by a British technology pioneer named Kevin Ashton. He describes a system in which physical world objects are connected to the Internet and are enabled to sense and communicate. Ashton used the term to emphasize the power of connecting internet to Radio-Frequency Identification (RFID) tags within corporate supply chains in order to track and count goods without human involvement.

Internet of Things (IoT) has become quite a prominent term today. Generally, IoT is used to for specify scenarios which uses computing capability and Internet connectivity to a collection of connected everyday objects enabled with sensing and actuation [2].

Currently the impact of internet in science, humanity, business, education, government, and communication is huge and notable. Internet is found to be the most influential and mighty creations in human history. Now, with the idea of the internet of things being widely used, internet has become more favorable and desired to have a smart life in every aspect.

1.1 IoT Security Goals:

Confidentiality: It is a process by which only authorized users are allowed access to the data.
Integrity: It is a process in which data completeness and accuracy is preserved

ISSN: 2005-4238 IJAST

Non-repudiation: The process by which the communicating devices cannot deny its involvement in the occurrence or non-occurrence of an event that occurred in the IoT system during the communication.
Availability: It is the capability of an IoT system is to ensure the availability of its services and making it easily accessible when and where required by the user.
Privacy: The process which follows a set of rules and policies to allow the users to have control over their sensitive data.
Audibility: It is a process which ensures the IoT system to do a complete monitoring and keep account of its actions
Accountability: The process which makes sure that the user is responsible for his actions.
Trustworthiness: Identifying its own identity with the communicating party by appropriate measures and ensure trust in third party authentication. [7]

1.2 Security Attacks:

The security solutions existing in IoT systems are vulnerable to certain types of attacks as follows:
Man-in-Middle: In this an attacker will gain access to one of the communicating parties key and communicate with the other party, pretending to be the valid user who is supposed to do the communication.
Denial of Service (DoS): It is an attack method in which the network services will be completely stopped for the authorized user and the access is provided to the unauthorized user.
Masquerading: An attacker intruder pretends to be the authorized user by possessing the identity of a valid user.
Eavesdropping: Intruder can pay attention to the communication that happens between the sender and the receiver without the knowledge of the communicating parties. Hence this is an attack on confidentiality.
Differential: A small change in input behavior will create huge change in the output. The intruder can find the key from network transformations that occurred during communications.
Saturation: The physical and mental capabilities of the authorized party is used by the intruder who wants to again access.[8]

2. IoT Security Architecture

The functioning of IOT in real time is possible through the unification of various technologies. General architecture of trusted security system based on IOT is described [3]. Security system which includes a trusted network module trusted trusted terminal module and perception module. The IoT architecture is split into three layers: Perception layer, Network layer, and Application layer [4].

The three layers have different features with different enabling technologies and large scale of information.
Perception layer is accountable for the data collection which is the main working of the IoT. Various devices like sensors, RFID tag, smart card and read erased used for gathering the data from the end devices. Perception layer has an extensive feature of comprehensive sensing. It uses the RFID system or the sensors to get end device's information anytime and anywhere. Every RFID electronic tag generally has a unique ID refereed as EPC (Electronic Product Code).The only reachable ID allocated for each physical target is the EPC. The other additional information like manufacturing date, expiry date related to the product is provided by a string inflicted on it [5].

ISSN: 2005-4238 IJAST

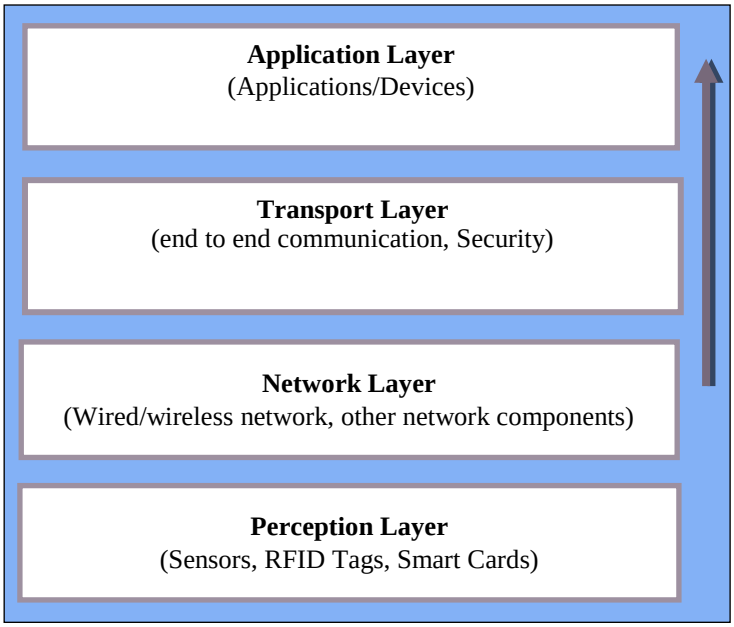

Fig 1: Architecture of IOT

The data gathered by the sensors in the network layer is sent to the internet. The data is transferred with the help of end devices, wireless/ wired network and other components to the network layer. Thus, the transmission of collected data is the main responsibility of network layer. And, this layer has an extra feature of reliable information delivery, thus the network layer also acts like the transport layer[21-22].

Transport layer is responsible for device to device communication. The User Datagram Protocol (UDP), which is an unreliable protocol, is utilized by the IoT. This layer has a Security mechanism built into it using DTLS.

The received information is analysed by the application layer and makes the control decisions. And application layer has the feature of identification and control between objects, devices and intelligent processing by connection. The application layer uses the intelligent computing technology such as cloud computing, Artificial Intelligence, Big data for Intelligent processing. It processes the information for intelligent control. Based on this the intelligent control decides like what things to do and when to do. Since the application layer is also called as process layer. [6]

Table 1. Protocols in IoT

Layer	Protocol	Security Protocol	Attacks
Perception	IEEE 802.15.4 MAC	IEEE 802.15.4 Security	Authentication, Integrity, DoS Attack
Network	IPv6, RPL	IPsec	DoS Attack
Transport	UDP	DTLS	Attack on RC4, DoS Attack
Application	COAP	Designed by user	Depends on protocol used

ISSN: 2005-4238 IJAST

Identifying its own identity with the communicating party by appropriate measures and ensure trust in third party authentication [7]. The physical and mental capabilities of the authorized party is used by the intruder who wants to again access.[8]

3. Lightweight Cryptographic Algorithms

Lightweight Cryptography [9] plans to answer the rapidly developing IoT applications that widely use extensive restrained limited power devices. As guaranteed by NIST, Lightweight cryptography is a subclass of conventional cryptography. Devices such as RFID, WSN and embedded frameworks are less reliable. Improving the designs for better security, improved execution speed and better resource requirements for typical resource limited environments are the goals to be achieved [10]. Distinguished association of hardware and software implementation is difficult. The correlation results in measurement of executing platform and measures of sufficiency [11].

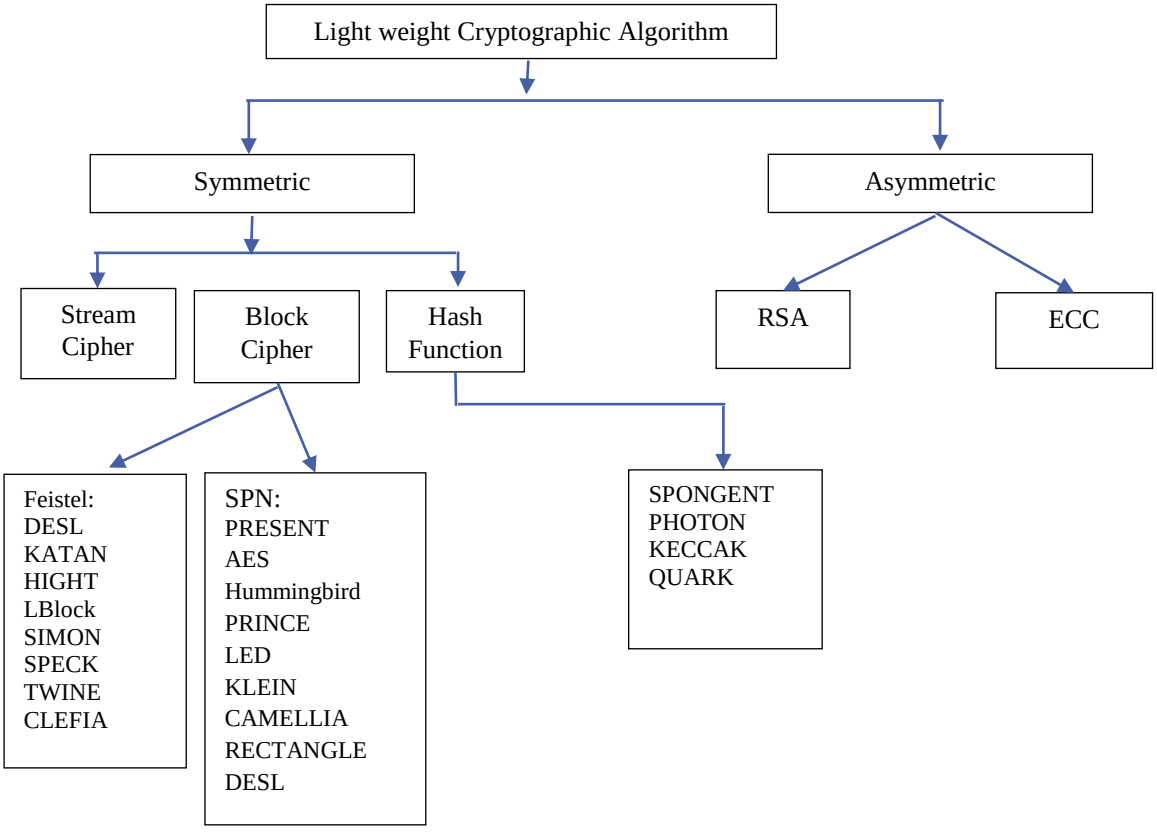

Fig.2 Classification of Lightweight Algorithm

4. Symmetric Key Cryptography

4.1.1 Block ciphers

Many other block ciphers with lightweight properties have been proposed since the introduction of Advanced Encryption Standard (AES) among those, PRESENT and CLEFIA [12] are studied in detail to learn about their implementation and security aspects. Both algorithms are under consideration for “Lightweight Cryptography”. These ciphers can be readily used in practical systems.

4.1.2 Stream ciphers

A portfolio of promising new stream ciphers is selected from ECRYPT II eSTREAM project [13]. The eSTREAM portfolio currently used contains total 7 algorithms. Trivium, Grain v1 and MICKEY v2 are the algorithms which has lightweight properties among these.

ISSN: 2005-4238 IJAST

4.1.3 Hash functions

NIST conducted the Cryptographic hash algorithm "SHA-3" competition which gained many people's attention. SHA-3 was supposed to be a general-purpose hash function by origin. But none of the algorithms chosen as finalists satisfied the lightweight properties. Extensive Research on various lightweight dedicated hash functions are carried out at various levels [14][16][17][18]. We can ensure more security by constructing lightweight hash functions which are based on lightweight block cipher.

4.1.4 Asymmetric Key Cryptography

The requirement for public key primitives is much larger than that of symmetric key primitives, since the lightweight public key primitives are used for key management protocols in IoT networks. There are no such primitives which are promising that will be meeting all the security requirements and all lightweight properties when compared to the typical conventional algorithms such as RSA and ECC at this point of time. Although some asymmetric key primitives like ECC can be constructed with comparatively smaller footprint, we cannot assure that they can have a reasonable execution time [15].

5. Results on Comparison

5.1 Memory Requirement:

PRINCE and SPONGENT are found to be the best in terms of space requirement while comparing with the other lightweight algorithms. CAMELIA is found to be extremely expensive when compared to PRESENT.

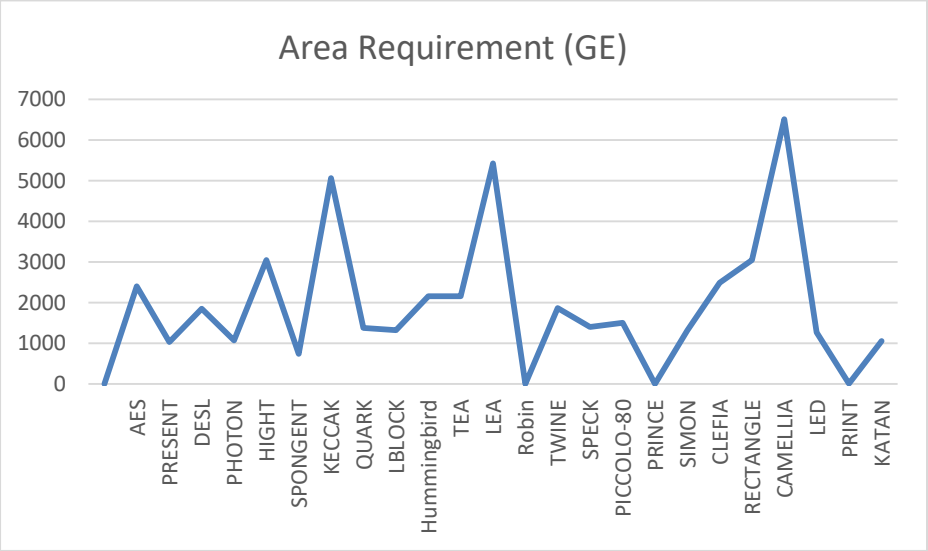

Fig.3 Comparing the Lightweight Algorithms

5.2 Energy Consumption:

On analyzing the above algorithms, it is found that Piccolo and TWINE is efficient in terms of power consumption. Whereas PRINT is costly in terms of power Consumption.

ISSN: 2005-4238 IJAST

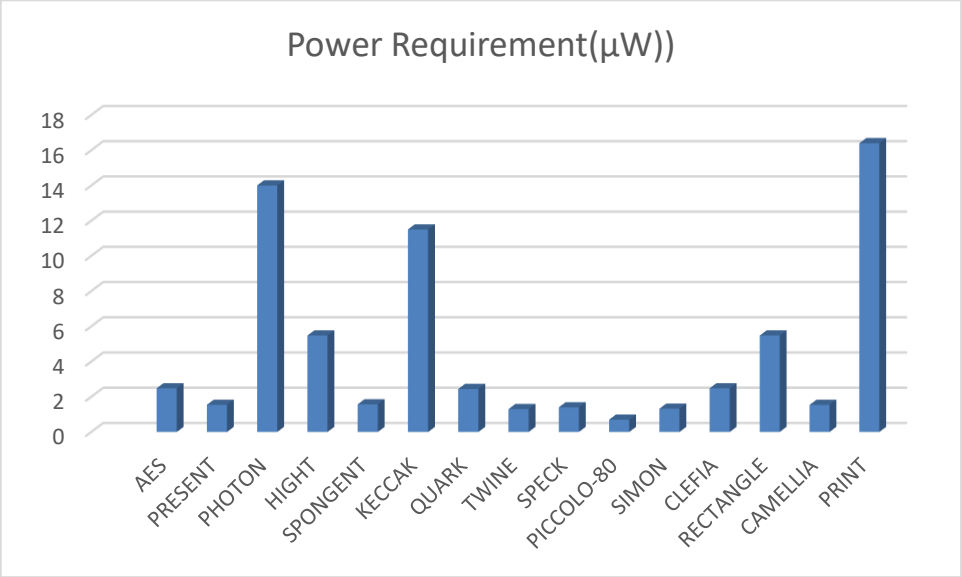

Fig.4 Power Consumption by the Lightweight Algorithms

5.3 Execution Speed:

RECTANGLE is found to be the faster in execution when compared to other listed algorithms and PHOTON, PICCOLO are relatively slower. From the comparison it is presumed that combining the hash algorithms with symmetric algorithms might be an effective way to achieve overall effectiveness.

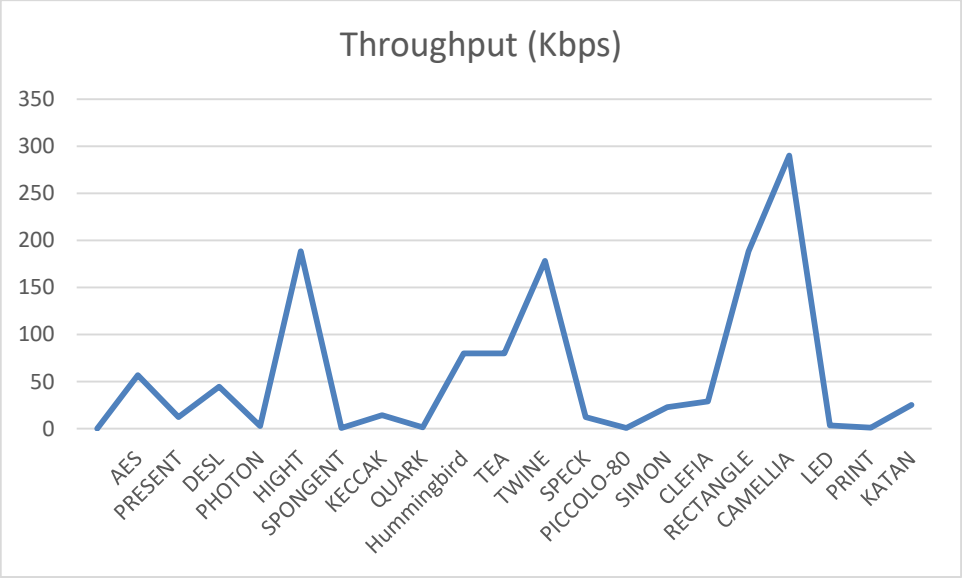

Fig.5 Performance of Hash Algorithms and Symmetric Algorithms

6. Conclusion

In this paper, a major set of lightweight block cipher algorithms are investigated and analysed in terms of the algorithm specifications and security aspects. Analysed different Symmetric cryptographic algorithms as well as Asymmetric cryptographic algorithms for IoT. As discussed previously, some of lightweight block cipher algorithms uses Feistel network while the others used the SPN, but each of these one has their own properties. Moreover, in researching and analyzing the different existing lightweight block cipher algorithms, it was found that the

ISSN: 2005-4238 IJAST

algorithm with many S-boxes ensures better security. Furthermore, with well-designed linear operations, higher security can be provided but the cost dependent on the design.

References

[1]. J. Borghoff, et al., "PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications," in Advances in Cryptology – ASIACRYPT,in Springer Berlin Heidelber , vol. 7658, pp. 208-225, July 2013.
[2]. Shibutani, et al., "Piccolo: An Ultra-Lightweight Blockcipher ",in International Association for Cryptologic Research, LNCS 6917, pp. 342–357, Dec 2012.
[3]. LeventErtaul, et al., "Performance Analysis of CLEFIA, PICCOLO, TWINE Lightweight Block Ciphers in IoT Environment", Int'l Conf. Security and Management, 2017
[4]. Xiong Li, et al., "Research on the Architecture of Trusted Security System Based on the Internet of Things" 2011 Fourth International Conference on Intelligent Computation Technology and Automation
[5]. Conner, Margery (May 27 2010). "Sensors empower the "Internet of Things" pp. 32–38. ISSN 0012-7515
[6]. Mayuri A. Bhabad, Sudhir T. Bagade "Internet of Things: Architecture, Security Issues and Countermeasures", International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015
[7]. Vinoth Kumar V, Karthikeyan T, Praveen Sundar P V, Magesh G, Balajee J.M. (2020). A Quantum Approach in LiFi Security using Quantum Key Distribution. International Journal of Advanced Science and Technology, 29(6s), 2345-2354.
[8]. Umamaheswaran, S., Lakshmanan, R., Vinothkumar, V. et al. New and robust composite micro structure descriptor (CMSD) for CBIR. International Journal of Speech Technology (2019), doi:10.1007/s10772-019-09663-0,
[9]. Maithili, K , Vinothkumar, V, Latha, P (2018). "Analyzing the security mechanisms to prevent unauthorized access in cloud and network security" Journal of Computational and Theoretical Nanoscience, Vol.15, pp.2059-2063.

[10]. Ghafari, V.A et al.,.: "Fruit-v2: ultra-lightweight stream cipher with shorter internalstate". Int. Assoc. Cryptol. Res (IACR) (2016)
[11]. Praveen Sundar, P.V., Ranjith, D., Vinoth Kumar, V. et al. Low power area efficient adaptive FIR filter for hearing aids using distributed arithmetic architecture. Int J Speech Technol (2020). https://doi.org/10.1007/s10772-020-09686-y,

[12]. S. Velliangiri, P. Karthikeyan & V. Vinoth Kumar (2020) Detection of distributed denial of service attack in cloud computing using the optimization-based deep networks, Journal of Experimental & Theoretical Artificial Intelligence, DOI: 10.1080/0952813X.2020.1744196

[13]. K Ravindranath, et.al., "Security key provided for Group Data Sharing in Cloud Computing "in the International Journal of Advanced Sciences and Technology (IJAST), ISSN: 2005-4238, November-2019.
[14]. K Ravindranath, et.al., "An Advanced Secured Privacy Preserving Techniques for Cloud Using Numerical SQL Query's " in the International Journal of Advanced Sciences and Technology (IJAST), ISSN:2005-4238 , November-2019.
[15]. P S RajaKumar, et.al., "Optimized and Efficient Computation of Big Data in Heterogeneous Internet of Things " in the International Journal of Engineering and Advanced Technology (IJEAT), ISSN:2249:8958,Volume -9, Issue-1, PP:6005-6010, October-2019.

ISSN: 2005-4238 IJAST

[16]. M Arutselvan, et.al., "A Perspective of Probabilistic Misbehaviour Detection Scheme in Vehicular Ad-hoc Networks" in the International Journal of Innovative Technology and Exploring Engineering (IJITEE), SSN: 2278-3075, Volume - 8 Issue – 7,Page No:1098-1102, April 2019.

[17]. G Sreeram, et.al., "Improving Cloud Data Storage Performance Based on Calculating Score using Data Transfer Rate Between the Internetwork Drives" in the International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249 -8958, Volume-8 Issue-4,Page No: 1830-1835, April 2019.

[18]. L.Hemanth Reddy, et.al., "Deployment of a Secured Web Application using Cryptanalysis in Cloud Environment" in the International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249 -8958, Volume-8 Issue-4, Page No: 1841-1844, April 2019

[19]. K Sreenivasa Rao, et.al., "Detecting Fake Account On Social Media Using Machine Learning Algorithms" in the International journal of Control and Automation "2005-4297, Vol. 13, No. 1s, (2020), pp. 95-100, April 2020.

[20]. G.Sreeram, et.al., "Efficiency and Stationing in Edge Computing"in the International Journal of Advanced Sciences and Technology (IJAST), ISSN: 2005-4238, Vol.29, 9s, (2020) pp.112-119.

[21]. Karthikeyan, T., Sekaran, K., Ranjith, D., Vinoth kumar, V., Balajee, J.M. (2019) "Personalized Content Extraction and Text Classification Using Effective Web Scraping Techniques", International Journal of Web Portals (IJWP), 11(2), pp.41-52

[22]. Vinoth Kumar, V., Arvind, K.S., Umamaheswaran, S., Suganya, K.S (2019), "Hierarchal Trust Certificate Distribution using Distributed CA in MANET", International Journal of Innovative Technology and Exploring Engineering, 8(10), pp. 2521-2524

ISSN: 2005-4238 IJAST