International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure and Lightweight Device Recognition Techniques for Constrained Application Protocol : A Survey

Prof. Subhashini R[1], Dr D G Jyothi[2],

[1]*Assistant Professor, Dept. of CSE, Cambridge Institute of Technology, Bangalore-560036*
[2]*Professor and Head, Department of AI & ML Bangalore Institute of Technology Bangalore*

Abstract - Internet of Things is one among the fastest growing technologies which introduced the concept of connecting surrounding things over internet and perform analysis over the data collected and sometimes even store the data for later use, or for historical analysis. There are plenty of things around which can be connected to IoT, some of which might be malicious and its very necessary to identify such devices before they infect the entire system. This paper proposes a survey on the lightweight authentication techniques to identify the devices of IoT for Constrained application protocol.

Key Words: Internet of Things(IoT), Authentication, Digital Signature, Constrained Application Protocol(CoAP).

1.INTRODUCTION

We utilise smart homes, smart automobiles, smart watches, and other smart devices on a regular basis in the new smart world. We can use technologies similar to those we envisage in our dreams, where everything is sentient and connected.

The IoT is an technology used to interconnect gadgets, for example, sensors, which can produce, impart and impart information to each other. In such a gigantic organization of interconnected smart objects, the identification of a specific object represents a principal task that impacts any remaining elements of the framework, for example, its administration, security highlights, access control, generally design, and so forth

IoT is comprised of nodes that are connected to one other for the purpose of monitoring, detecting, and gathering data from their surroundings and sending it among nodes or to a data collection centre. These nodes are typically limited in memory, have poor battery power, and have limited computational capabilities. Furthermore, these devices are commonly used in situations with a low bit error rate and a lossy communication channel. Because of the limitations of these devices and communication links, IoT require a more lightweight and dependable application protocol with an efficient congestion control mechanism.

The devices in IoT are interconnected to each other for the purpose monitoring,detecting and gathering data from environments and communicating it among different nodes also propagating it to a collection point. These devices are featured with constrained memory,less battery power, and constrained processing capabilities. Moreover, these devices are typically employed in low bit error rate environments with lossy communication link. The shortcomes of these deices and links requires a lightweight and reliable application protocol in IoT.because sometimes IoT devices might be sometimes using protocols which are obsolete which may tend to discovery of backdoors, allowing the gadget to be readily attacked.

Introduction to CoAP

Constrained Application Protocol (CoAP) is a particular application layer protocol for use with obliged hubs and compelled networks in the Internet of Things. CoAP is intended to empower straightforward, compelled gadgets to join IoT even through obliged networks with low data transmission and low accessibility and to provide a common web interface. It is by and large utilized for machine-to-machine (M2M) applications like shrewd energy and building computerization.

Few of the highlights of CoAP are

1. It resides over UDP transport Layer Protocol
2. Incorporation of IPv6 with 6LoWPAN
3. Supports unicast and multicating
4. Follows Request/Response behaviour
5. Low overhead than other protocols
6. Capability to act as Proxy and Cache.
7. For security makes use of DTLS protocol
8. Use of Uniform Resource Indicator (URI) Methods and
9. Behaves like HTTP

Security in CoAP

Some of the attacks occurring in CoAP protocol are
• Parsing attacks, in which a far off hub could be crashed by executing an inconsistent code on the hub

• Storing attacks, wherein an intermediary being able to store can acquire control. This might fill in as a danger for clients who are trading information with the intermediary, unconscious a potential gatecrasher in the organization

• The enhancement attacks, in which an assailant can utilize the end gadgets to change over a little parcel into a bigger bundle. A CoAP Server can truth be told diminish the intensification assaults by utilizing Blocking/Slicing modes.

• Satirizing attacks

• Cross-Protocol attacks, where the interpretation from TCP to

UDP is obligated to assaults.]

Vulnerability issues in CoAP

- DoS assaults are estimated as a necessary security issue. These assaults can be introduced with standard orders from distant areas, blended in with cutting edge instruments.
- Man In The Middle: MitM happens when an assailant catches bundles or correspondences between two tasks to one or the other cover or shift traffic between them. Aggressors could utilize MitM assaults to sharpshooter login certifications, spy on a casualty, harm or degenerate data.
- Sniffing: is a checking and catch technique for all information bundles that pass through guaranteed network. Assailants use sniffers to hold onto parcels of information that contain delicate data like passwords, account data, and so on.
- Application Layer: Constrained application convention is being normalized as the application convention for 6LoWPAN. Since still numerous protections, concern ought to emerge in future. A few weaknesses are crossprotocol assault, Threat of intensification, Proxying and storing, SYN flood, IP address satirizing

.

2. Literature Survey

Paper [1] proposed a wide ranging and lightweight security design to get the IoT all through the lifecycle of a gadget. The arrangement depends on the lightweight HIMMO conspire as the structure stone and shows how HIMMO isn't just productive asset wise, yet that it empowers progressed IoT conventions and organizations. HIMMO can be effectively incorporated in current conventions at the somewhat low expenses of symmetric cryptographic arrangements, includes that before were just possible with topsy-turvy cryptography.
HIMMO and PSK don't offer non-reudiation a gadget A can sign information with the key it uses to speak with gadget B, and guarantee that the information has been endorsed by B utilizing the last option's key for speaking with A.

Paper [2] portrays review on numerous strategies for distinguishing or perceiving things like Radio Frequency Identification (RFID), Barcode/2D code, IP address, Electronic Product Codes (EPC), and so on. Nonstop advancement in IOT space and the enormous number of articles associated with the Internet day to day require a better ID technique to adapt to the quick improvement in this field.

Lightweight IoT gadget recognition confirmation method is proposed. In any case, the DFI (critical/solid stream review)[3] improvement is used to productively eliminate stream related quantifiable parts considering completely assessments is plot used stream related quantifiable features to address the approach to acting of IoT devices and a divert remember decision procedure for light of NSGA-III to pick strong components.The proposed plan can achieve commensurate accuracy with significantly less vertical.

Its future work will focus in on cloud organizations. Directions to fuse the models, ensure the steadfastness of the section, and work on the presentation and security of the circled device ID structure will be the point of convergence of future work.

Paper [4] shows that there is a critical benefit to involving PCA PRINCIPAL COMPONENT ANALYSIS for both SVM and NN-based oddity identification. Doing so works on the exhibition and adequacy of malware recognition models, and diminishes how much information that should be put away on the gadget for on-gadget anomaly discovery, subsequently making it helpful for constrained IoT gadgets

Paper [5] presents three fundamental commitments. (I) It empowers secure correspondence in the IoT utilizing lightweight compacted at this point standard consistent IPsec, DTLS, and IEEE 802.15.4 connection layer security; and it examines the advantages and disadvantages of every one of these arrangements. The proposed security arrangements are executed and assessed in an IoT arrangement on genuine equipment. (ii) This proposal likewise presents the plan, execution, and assessment of an original IDS for the IoT. (iii) Last yet not least, it additionally gives instruments to safeguard information inside constrained nodes.

Work [6] intended to provide confidentiality, authentication and integrity of data on move between IoT end nodes and server systems. This paper proposes a lightweight mixture encryption framework involving ECDH key trade component for creating keys and laying out association, advanced signature for validation, from that point AES calculation for encryption and decoding of client information record. The proposed mix is alluded to as "three way gotten information encryption instrument" which decipher all the 3 assurance plans of validation, information security and confirmation with the attributes of lower estimation cost and quicker speed makes it strong for programmers to break the security framework, in this manner defensive information in transmission.

Its Future work focuses on to carry out this half and half methodology in IoT continuous application and really take a look at the strength of proposed mixture calculation.

The lightweight cryptography [7] is better than the ordinary cryptography. In equipment executions, chip size and energy utilization are less contrasted with the overall cryptography. In programming executions, the more modest code and RAM size are ideal for lightweight applications. The natives of the lightweight cryptography are encryption, hash capacities, and advanced signature. The sensor information is scrambled by utilizing hash capacities and advanced signature. In this venture, we are involving the above approaches breaking

down the security in IoT.This paper introduced an instrument to recognize the information which is gotten by the approved framework by utilizing the one of a kind ID of the gadget. The propose technique is to get the gadget information from the assaults like control of information and altering of information. The framework is catching the information from the IoT gadgets and afterward put away in a cloud asset for gadget has the restricted asset. The cloud information isn't completely secure even it is verify to conquer this issue mark and check plot is to get the information and approve the information is altered or changed

A validation technique between CoAP server and CoAP client utilizing CoAP message payloadis presented in paper [8]. It evades the upward of executing extra convention to get the correspondence. It utilizes just two handshake messages to finish the common confirmation between gadgets. Absolute information bytes sent among client and server for verifying each other is around 300 bytes in particular. Absolute validation time incorporates one full circle time and handling time spent on both the compelled hubs. It aims to use AES symmetric key calculation for encoding and decoding information in CoAP client and CoAP server. It is a square code calculation with 128 pieces of consistent square size. It has key sizes of 256 pieces, 192 pieces and 128 pieces length. It is accepted that the 128 cycle key is adequate for encryption and unscrambling in obliged gadgets of IoT framework as they have low handling capacities. AES encryption with 192 piece key and 256 cycle key

In paper [9], four unique ways to deal with IoT gadget ID in view of the organization traffi is proposed. In the first place, a two-stage Random Forest classifier utilizing highlights separated from a 1 hour window of gathered trafficis used. Then, 2D Convolutional Neural Network on a flood of crude bundles is used. Afterward, Random Forest and Decision Tree classifiers on highlights separated from a 1 second window of organization traffic is made use. The paper shows that while the precision of these models is high when tried on the dataset from a similar period as the preparation dataset, the exactness corrupts over the long haul when assessed on dataset gathered outside of the preparation time frame.

A plan and execution of a lightweight bootstrapping administration for IoT networks that use one of the application conventions utilized in IoT: Constrained Application Protocol (CoAP)is presented[10]. Furthermore, to give adaptability, versatility, support for huge scope sending, responsibility and personality league, This plan utilizes advancements like the Extensible Authentication Protocol (EAP) and Authentication Authorization and Accounting (AAA).The paper named this assistance CoAP-EAP. Lightweight CoAP-Based Bootstrapping Service for the Internet of Things. In this sense, future work has been made arrangements for the utilization of other EAP strategies (e.g., EAP-AKA.

In paper [11] all functioning philosophy for hash developments alongside their positive and negative angles is described. Likewise, a fair examination of a few hash configuration has to be given for the effectiveness of its clients. The creators concentrated on four different hash developments, to be specific Blake, JH, Keccak, and SHA. In correlation with SHA-2, Blake's throughput proportion is about a large portion of that of the last option. In the fourth, Keccak utilized a wipe development that utilized a proper stage however which could without much of a stretch be acclimated to exchange conventional security strength for throughput, permitting it to create either an enormous or little hash yield. Its equipment execution is uncommonly productive, as well as its security edge. Keccak likewise have characterized altered tying modes that give valid encryption. Additionally, the throughput of Keccak is obviously superior to SHA-2.

The work [12] presents a particular lightweight matching convention for Internet of Things (IoT) empowered gadgets that is custom-made for the climate of savvy homes. The convention uses encryption methods to give verification, classification and protection. Convention presents two significant extraordinary elements of mark and trust. Mark is separated in view of different boundaries and is utilized for common verification. Trust is additionally fundamental to have secure correspondence between IoT gadgets and the passage. No correspondence happens assuming the degree of trust is underneath sure limit esteem. Another significant boundary for example area is utilized to ensure that the IoT gadgets are inside the limit of the savvy home and furthermore to separate among authentic and ill-conceived IoT gadgets. The proposed convention is investigated and evaluated against a few dangers and assaults that could be sent off on the IoT empowered gadgets and organizations. Security investigation and intricacy examination has likewise been played out that show that the proposed convention isn't just lightweight yet additionally gives an OK degree of safety, protection, classification, network survivability and versatility to different assaults

Fostering of a lightweight common verification convention [12] in view of an original public key encryption conspire for shrewd city applications. The proposed convention takes a harmony between the effectiveness and correspondence cost without forfeiting the security. On a similar security level, the convention execution is essentially better compared to existing RSA and ECC based conventions. The proposed convention is a n-pass lightweight common confirmation convention. The worth of n is connected with the ideal security level of the convention and the framework boundaries of the encryption conspire. Our lightweight shared confirmation convention applies the proposed encryption plot as a structure block.

The paper[14] presents a scientific categorization and a writing audit of validation in the IoT setting. The examination of an enormous range of validation conventions/plans prompts recognize various necessities and open issues that ought to be thought about by scientists and engineers while growing new confirmation plans for IoT organizations and applications. This paper presents a scientific categorization and a writing audit of validation in the IoT setting. The examination of an enormous range of validation conventions/plans prompts recognize various necessities and open issues that ought to be thought about by scientists and engineers while growing new confirmation plans for IoT organizations and applications.

A RFID-based arrangement that empowers recognizability and validation of IoT gadgets across the production network called ReSC-2[15]. Contrasted and existing methodologies, ReSC-2 has the accompanying benefits: (1) By restricting the RFID tag and the recognized gadget along with a coordinated planning, likely split assaults (i.e., isolating tag from item, trading labels, and so forth) can be distinguished; (2) By consolidating two strategies (i.e., balanced planning between label character and control chip personality, one of a kind label follow made out of marks of perusers on the conveyance way) together, ReSC-2 can address the greater part of safety and protection challenges for IoT production network; (3) The manufacture cost is very low since by far most of parts (e.g., voltage controller, control chip with implanted SRAM, and so on) in this plan as of now exist in numerous advanced IoT gadgets.

A Lightweight Authentication with Two-manner Encryption for Secure Transmission in CoAP Protocol (LATEST) [16] that gives a stable transmission among the server and IoT devices. This mutual authentication mechanism makes use of ROT 18 Cipher with XoR operation and 128-bit AES primarily based totally encryption for securing the data transmission. The ROT18 Cipher is a monoalphabetic substitution cipher, that is a aggregate of ROT13 and ROT5. The proposed scheme employs symmetric encryption in each client and server for making sure stable authentication and mutually verify every different identity. In addition, the proposed scheme guarantees confidentiality and integrity with the aid of using being resistant to replay attacks, impersonation attacks, and change attacks.

A green saving strength method[17] to steady end-to-end (E2E) communications primarily based totally on the compression of the IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) header for HIP DEX packets is proposed. The solution is put in an IoT primarily based totally-WSN over Constrained Application Protocol (CoAP) withinside the software layer and Routing Protocol for Low electricity and lossy networks (RPL) withinside the routing layer. The paper additionally endorse a singular distribution version that minimizes the variety of signaling messages. Both proposed compression and distribution fashions for HIP DEX combined with an authentic implementation of an opportunistic affiliation established order of the handshake, represent an green protection answer for IoT. We known as our answer Lightweight Compressed HIP DEX withinside the IoT (LC-DEX).

Paper [18] describes P-HIP, that safeguards the character security of an IoT gadget by empowering the gadget to figure and utilize remarkable host identifiers from organizations to organizations and meetings to meetings. To make the HIP reasonable for asset obliged IoT gadgets, P-HIP gives techniques that unburden IoT gadgets from calculation escalated tasks, for example, measured exponentiation, associated with validation and meeting key trade. Also, P-HIP limits the correspondence overheads for trading authentications in lossy organizations. P-HIP can lessen calculation costs, correspondence overheads, and the meeting key foundation timewhen involved by low-fueled gadgets in a lossy organization.

3. DISCUSSION

The Internet of Things (IoT) changes our lives through savvy mechanization and has turned into a vital piece of numerous exercises. The primary components that have empowered inescapable IoT reception are the fast advances in programming, systems administration, sensors and computerized reasoning. In this paper, a survey on features of CoAP protocol, its security issues and vulnerability iissues and techniques for adding the uprightness to the CoAP protocol is proposed. Since IoT devices are constrained by various limitations, there is a necessity for lightweight device authentication techniques which prevents entry of malicious nodes and which consumes less power and which can fit for constrained devices.

REFERENCES

1. Oscar Garcia-Morchon, Ronald Rietman, Sahil Sharma, Ludo Tolhuizen, and Jose Luis Torre-Arc.: A comprehensive and lightweight security architecture to secure the IoT throughout the lifecycle of a device based on HIMMO. Philips Group Innovation, Research, Eindhoven, The Netherlands
2. Sana Abdelaziz bkheet, Johnson I. Agbinya.: A Review of Identity Methods of Internet of Things (IOT). In: Advances in Internet of Things Vol.11 No.4(2021).
3. Ruizhong Du, Jingze Wang, Shuang Li.: A Lightweight Flow Feature-Based IoT Device Identification Scheme. Hindawi Security and Communication Networks Volume 2022 ,Article ID 8486080 (2022).
4. John Carter, Spiros Mancoridis, Erick Galinkin.: Fast, Lightweight IoT Anomaly Detection Using Feature Pruning and PCA. In: Association for Computing Machinery. ACM ISBN 978-1-4503-8713-2/22/04(2022).
5. Shahid Raza.: Lightweight Security Solutions for the Internet of Things in: Copyright c Shahid Raza, ISSN 1101-1335 ISRN SICS-D–64–SE Printed by Malardalen University,Sweden(2013).
6. Tenzin Kunchok, Prof. Kirubanand V.: A lightweight hybrid encryption technique to secure IoT data transmission. In: International Journal of Engineering & Technology, 7 (2.6) (2018) 236-240(2018).
7. K. Sambasiva Rao, M. Kameswara Rao.: A Lightweight Digital Signature Generation Mechanism for Authentication of IoT Devices. In: International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6(2019).

8. S. Gladson Oliver1, and T. Purusothaman.: Lightweight and Secure Mutual Authentication Scheme for IoT Devices Using CoAP Protocol. In: Computer Systems Science & Engineering, vol.41, no.2(2022).
9. Crown https://github.com/DADABox/revisiting-iot-device-identification(2021).
10. Dan Garcia-Carrillo , Rafael Marin-Lopez.: Lightweight CoAP-Based Bootstrapping Service for the Internet of Things. In: https://www.mdpi.com/journal/sensors Sensors, 16, 358; doi:10.3390/s16030358(2016).
11. Ashwani Kumar, Deena Nath Gupta, Rajendra Kumar.: Hash Constructions for CoAP under an IoT Environment. In: International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON) Pune, India. Oct 29-30(2021).
12. Ali Tufail.: A Lightweight Pairing Protocol for IoT Devices in Smart Homes. In: IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.4,(2019).
13. Prof Vijay Varadharajan, Dr Uday Tupakula and Kallol Karmakar.:Lightweight Authentication Mechanism and OAuth Protocol for IoT Devices In: Technical Report TR2: ISIF ASIA Funded Project, The University of Newcastle(2018).
14. Mohammed El-hajj, Ahmad Fadlallah , Maroun Chamoun , Ahmed Serhrouchni 3,: A Survey of Internet of Things (IoT) Authentication Schemes. In: www.mdpi.com/journal/sensors Sensors 2019, 19, 1141; doi:10.3390/s19051141(2019).
15. Kun Yang, Domenic Forte, and Mark M. Tehranipoor.: Protecting Endpoint Devices in IoT Supply Chain. In: IEEE 978-1-4673-8388-2/15(2015).
16. Pritam S. Salankar, Vinay Avasthi, Ashutosh Pasricha.: Lightweight Coap Based Authentication Scheme by Applying Two-Way Encryption for Secure Transmission. In: International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-6(2020).
17. Balkis Bettoumi,Ridha Bouallegue.: LC-DEX: Lightweight and Efficient Compressed Authentication Based Elliptic Curve Cryptography in Multi-Hop 6LoWPAN Wireless Sensor Networks in HIP-Based Internet of Things . In: https://www.mdpi.com/journal/sensors Sensors 2021, 21, 7348. https://doi.org/10.3390/s21217348.
18. Mahmud Hossain, Ragib Hasan.: P-HIP: A Lightweight and Privacy-Aware Host Identity Protocol for Internet of Things. In: : IEEE Internet of Things Journal, DOI 10.1109/JIOT.2020.3009024,(2020).