Device Authentication Schemes in IoT: *A Review*

Omphulusa Lucia, Bassey Isong, Naison Gasela
Computer Science Department
North-West University
Mafikeng, South Africa
omphulusalucia@gmail.com, isong.bassey@ieee.org,
naison.gasela@nwu.ac.za

Adnan M. Abu-Mahfouz
Council for Scientific and Industrial Research
(CSIR)
Pretoria, South Africa
a.abumahfouz@ieee.org

***Abstract*— Internet of Things (IoT) is one of the most promising technologies and has wide spread application areas in the information technology for future products and services. Developments in IoT have given rise to device proliferation which in turn increase IoT challenges such as security. One of the security challenges is the authentication of heterogeneous devices in the network. Due to the unique nature of these devices, traditional security schemes proposed and developed over the years have been rendered inept and infeasible for IoT application. However, several lightweight solutions have also been proposed for IoT application, but are far from being efficient. Therefore, this paper performed a review on some of these studies in order to comprehend the challenge, identify some of the approaches offered, and provide recommendations for future research. We reviewed about 9 articles and our analysis shows authentication is still an open issue in IoT and there is no generic approach to authenticate devices**.

Keywords— IoT, Security, Authentication Schemes, Devices

I. INTRODUCTION

Internet of Things (IoT) is a technology model that has shown rapid growth in the past recent years. It simplifies things for people by ensuring that data interchange between people/devices is simple and faster. IoT refers to the interconnected global network of physical objects that contain embedded technology based on communication, sensory, processing and networking, which enables them to interact within themselves or the external environment [1]. These devices range from small "things" like smart watches, smartphones, chips, routers to several other devices with great computational power [2]. IoT main objective is to provide a network infrastructure with interoperable communication protocols and software to allow connections [3][4]. Thus, the development of IoT has resulted to the unlimited number of devices that can connect to the network at any time [5]. Accordingly, it has been predicted that the number of devices that will be online would reach 26 billion by 2025 and consequently, more data will be generated on an hourly or daily basis. However, IoT is currently confronted with many challenges ranging from data management, lack of standardized architecture, data mining, and security to many others [6]. These challenges are exacerbated by the nature of IoT devices often characterized as resource-limited which have subjected existing traditional communication protocols and security approaches inept for IoT [7]. Moreover, the proliferation of the number of connected devices to the network has significantly contributed to security challenges faced by IoT world which has been deemed alarming.

Nonetheless, the failure, success, and growth of IoT completely depends on the security which in turns depend on the type of application served [8]. In the same vein, confidentiality, integrity, authentication as key security requirements also are dependent on the application [7]. If proper security schemes are in place, both devices and data will be secured and the data trusted to make informed decision. Lack of effective security makes it easier for attackers to gain access to the network to compromise integrity, confidentiality, nonrepudiation and availability of both devices and data and in some cases, life-threatening [7]. For instance, compromising a single node may maliciously lead to complete network failure. Thus, issue of security should be taken as a priority ahead of data management, storage, and processing.

In recent years, several security solutions have been proposed and developed. However, some of these solutions are inept, infeasible, and not applicable in the IoT landscape due to the unique nature. A particular case is authentication which is a key security requirement. To properly address security challenges in IoT, the different layers has to be considered. IoT has three layers: the perception, network and application layers and each has specific challenges associated with it. The application layer, which is the closest to consumers/user and the pressing issue is the authentication of the heterogeneous devices into the network [7]. Authentication is the standard protocol for any network and every connected device has to be authenticated to make sure the right device has the right access in the right place. In addition to sensitive data, IoT is capable of controlling both physical and virtual environment, thus, the security of the network, system and user privacy protection have to be taken seriously.

Recent studies have shown that devices are able to get in and out of the network without authentication. IoT has many unlimited devices, which are heterogeneous in nature, connected, and differ in sizes, shapes, storage, and computational power and battery life. With such number connected to the network, tracing back the device who does what, when, where and so on, constitute a tedious work. Several researches have also shown that due to the diversity of devices connected, it is hard to authenticate devices. Moreover, communication spans from small device to large devices or small device to small devices. Thus, to solve this

challenge, several authentication schemes have been proposed and developed for IoT device [7] such as authentication in IoT cloud federation based on two schemes [9], a robust lightweight scheme [10] and a lightweight authentication and authorization framework [4]. Therefore, this paper performed a comprehensive analysis on some of these authentication schemes with the objective of understanding the authentication challenge, identifying their approaches as well as opportunities for future research.

The rest of the paper is organized as follows: Section II is the related works, Section III analyzes some of the current works on device authentication, and Section IV presents the paper discussions and summary while Section V is the paper conclusion.

II. Related Works

This section highlights some existing related works on survey or reviews in the perspective authentication in IoT. Helmi *et al.* [6] surveyed on the different challenges that affects IoT such as the creation of digital divides, IPV6 and force sensors and so on. Hossain *et al.* [8] also reviewed on the security challenges in IoT. They focused on different attack surfaces, threat models, and security issues and so on. In addition, the study provided open problems in security and privacy to assist researchers in addressing them. Mardiana [11], performed a survey on IoT security where they highlighted on the status of IoT research and evaluated the challenges of applying security mechanisms. They also discussed several solutions or models used for solving security challenges. Similarly, Antonopolous [12] surveyed on block-chain based IoT security solution. They outlined the different tools used to authenticate devices, how block chain authenticates devices and how information is kept on storage. Accordingly, El-hajj *et al.* [7] presented a comprehensive survey of authentication protocols in the IoT field. The employed multi-criteria classification, compared and assessed different authentication schemes proposed. Their aim was to provide a direction to researchers and developers to improve on IoT device authentication.

Qi Jing *et al.* [13] also conducted a survey with a focus on three layers of IoT and the analysis of the security challenge faced in each. They identified device authentication as the main challenge confronting the application layer. They recommended the use of lightweight security methods as a solution and also discussed several open issues relating to security. In the same vein, Maire O'Neil [14] surveyed on insecurity design on today's IoT network. The study explained how unlimited number of devices connected to IoT network without proper authentication is creating security problems. Moreover, physical unclonable function (PUF) was proposed for device authentication. According to [14], PUF will create both authentication and identification of device in IoT. In [15], a review on authentication and authorization of IoT mobile devices using biometric features was performed. Several literatures were reviewed different with a focus on the use of biometric features and highlighted their limitations as well as provided future directions on implementing biometric for mobile IoT devices.

In all these related works [6-8, 11-15], only the work in [7] is similar to this research. Though [7] did a comprehensive review using multi-criteria classification, our work is based on recent works and is basically to understand the nature of the challenge and the different approaches offered in order to propose a new solution.

III. Analysis of Current IoT-based Authentication Schemes

As stated above, authentication is a key requirement for an IoT network to ensure confidentiality and integrity of information transmitted [7]. However, the nature of IoT devices makes traditional authentication schemes unsuitable for IoT application. This is because the traditional networks are not designed to accommodate countless devices unlike the IoT counterpart. In particular, traditional authentication schemes like the cryptographic-based ones were designed for main powered, high processing and or large memory capacitated devices and are inept for IoT environment due to the resource constrained nature of participating devices [7]. Consequently, several lightweight authentication schemes have been developed in this regard.

Therefore, this section presents some of the proposed and developed schemes of authenticating devices in the IoT network, their implementation, and challenges. We discuss each based on the category they belong to.

A. Authentication Factor/Public Key Based Scheme

This category of authentication scheme is based one party presenting information to the other party to authenticate itself. It also known as identity-based authentication and uses a combination of hash, symmetric and asymmetric algorithms. Accordingly, they include physiological or biometric information based on individual characteristics e.g. finger print, hand geometry, retinal scans etc. Others involved behavioral characteristics of individual e.g. voice ID, gait analysis [7]. Some of the existing approaches under this scheme are discussed as follows:

Musale *et al.* [17] focused on authentication of devices in IoT using a lightweight gait-based technique. The objective is to address the infeasibility of traditional-based authentication methods in IoT, due to small devices in IoT that are resource constrained. Thus, using the knowledge-based authentication in IoT increases energy consumption and computational power for some of these devices. This challenge is address in [17] by proposing a Li-GAIT (Lightweight Gait Authentication) to authenticate smartphone users in which arm swing patterns in their walk is analyzed.

To evaluate the effectiveness of the approach, Android Operating System was used to test its accuracy. Three phases were involved: data collection, feature extraction and authentication phases. Motorola G4 Plus Android Phone was used to collect data about the user which is sent to the Li-GAIT system for features extraction. During the authentication, the model employed machine learning to learn the features and understand the pattern based on the stored data collected and the data collected while the user is walking. The model was tested on 12 different users and the results

showed that using this model, it saves both battery and computation power.

Alharbi and Alhazmi [18] also proposed an authentication scheme to combat the risk of data confidentiality posed by devices without authentication. The proposed lightweight local user authentication scheme uses Near Field Communication (NFC) technology and Chaskey hashing [18]. It operates in three phases: verification, registration, and authentication. The verification phase deals with the verification of the IoT network where a valid user the phone as an identity to access the network. In this case, the phone is passed to the trusted device which passes the user identity to the IoT gateway for identity verification without revealing the sensitive data. However, in the registration phase, the phone of the user is passed to trusted device connecting the IoT gateway to generate the user identity-based secret key while in the authentication phase, the identity of the user is encrypted with the secret key using Chaskey hash function and create the session key. However, the scheme has not been implemented.

Ashibani and Mahmoud [19] proposed IoT device authentication approach based on behavioral usage pattern. They argued that traditional authentication schemes based on knowledge-based were fasting becoming infeasible as passwords or pre-defined keys could be stolen. For instance, smartphones used to access IoT networks could be stolen or lost and if hacked, the hacker could continuously perform authenticate on the network and have access to user sensitive information. As a solution, [19] authentication model employs ML which utilizes the user's dataset and learns their previous access patterns and then authenticate them based on the app-access profiling. The ML model monitors the app's access logs on the end user's device before a request sent and while sent. This detect any deviation from the normal pattern that could happen. If any deviation is experienced, authentication is rejected. The model was built on Panda's library and uses dataset extracted from Android Operating System. There are two categories of dataset: the management activity data and the network trace data. To assess its performances, result obtained shows users could be authenticated based on their app usage pattern.

B. Token-based Scheme

This scheme is based on the usage of identification tokens to authenticate user or device which is created by a server such as OAuth2 protocol or open ID [7]. The only study considered in this paper under this scheme is discussed as follows:

Bhuwiyuga *et al.* [20] focused on the communication between devices in the IoT environment. The objective was to address the weak authentication form (password and username) for devices used by Message Queue Telemetry Transport Protocol (MQTT). It was argued that, an attacker can easily access the credentials using a wireless sniffing mechanism due to the single channel for authentication in MQTT. To address this challenge, [20] developed a token-based scheme of MQTT protocol having four components: publisher, subscriber, MQTT Broker, and token authentication server. The protocol operates by the publisher sending a request to the token authentication server to get a token. This is performed before a token is generated and when a token has expired. On receipt, the server verifies the credentials against the database and if matched, token is generated and sent back to the publisher to store the token for later or further authentication. To evaluate the scheme, both functional testing and performance testing were performed. For functional testing, a valid token and the invalid token were performed. With valid token both server and the broker authenticated each other while invalid token did not. Moreover, performance testing shows a fluctuation.

C. Procedural-based Scheme

This category of authentication scheme occurs three ways which are either 1-way, 2-way or 3-way [7]. In particular, the 1-way authentication occur when two parties wish to communicate with each other. In this case, one party will authenticate itself while the other remains unauthenticated for the duration of the communication. The 2-way authentication on the other hand, involved two parties authenticating one another and remain authenticated for the duration of the communication. A failure of one party one to authenticate results to communication not being established. For the 3-way authentication, there is a central authority like a server or any device that helps the two parties wishing to communicate to actually authenticate themselves. Some of the existing studies under this category include:

Nasir *et al*. [21] also proposed an authentication approach to guard against disclosure attack on mutual authentication using RFID Tag in IoT. This is because existing mutual authentication protocol using RFID are prone to disclosure attacks which makes easy to obtain the secrete key computed between RFID tag and the reader. Such attacks are inevitable because messages sent as plain text. As a solution, [21] proposed a scheme that uses both symmetric encryption and hashing to improve the existing mutual authentication protocol to improve security against attack disclosure. It operates by first encrypting the messages using 128 bit for secret key on AES algorithm and then transmit it through the insecure channels. When intercepted by an attacker, it makes no and each session have a different key to ensure the secrecy of the communication. No implementation was performed.

Gupta *et al.* [12] also proposed a user authentication and key establishment scheme which is lightweight and anonymous in nature for wearable devices. This is to address the challenge of several devices being resource constrained in the IoT involving authenticating themselves before data is being sent and received. The proposed lightweight scheme uses five steps for authentication. The user initiates the authentication step by communicating or contacting the required wearable device. Both the device and terminal then establish a session key using a trusted server. The scheme uses hash functions and XOR operations. It also makes use of random nonce and current timestamps to resist any strong attacks. To assess its performance, the approach was tested using BAN-Logic to prove it generates secured keys between terminal and wearable devices. In terms of security, AVISA was used to show that it can resist strong attacks.

Dahya and Bohra [22] focused on the methods used for encryption for device authentication. Since the authentication of devices in the network relies on encryption protocol, the objective of this paper is to address the challenge of weak encryption which are vulnerable to attacks while complex methods delay encryption. Moreover, well-known single channel authentication where a single device has to authenticate its self to the other has been deemed insufficient for IoT network as many heterogeneous network domains are involved. As a solution, [22] proposed a robust, quick and complex encryption model called parallel partial model (PPM). PPM was designed with the combination of two algorithms: Improved Advanced Encryption Standard (iAES) and Modified Elliptic Encryption Curve Cryptography (mECC) to secure and achieve high efficiency on complex encryption. To evaluate its performance, the model was analyzed based on the execution time and found to be efficient in all cases.

D. Hardware-based Scheme

This scheme employs the use of hardware physical characteristics for device authentication in the IoT. This include implicit hardware physical characteristics to enhance the authentication such as PUF or true random number generator [7] and the explicit hardware itself such as trusted platform module such as TPM, chips that stores and process the keys for authenticating devices. Some of the studies under this scheme category include:

Maire O'Neil [14] proposed a physical unclonable function (PUF) for device authentication which is a lightweight solution. PUF is used to create both authentication and identification of device in the IoT world by generating a unique digital fingerprint using silicon chips' process variations. There are tampered proof and capable of effectively detecting devices that were cloned.

Hasan and Qureshi [23] proposes an authentication algorithm for IoT devices based on chip serialization. The scheme was aimed at addressing the challenges posed by devices in executing complex authentication algorithms due to resource constraint since existing authentication algorithms are not universally applicable to IoT devices. They proposed a lightweight algorithm and primitives for efficient and high-level security with minimum resource utilization. It has two phases: pre-registration and authentication phase. Pre-registration phase uses secure channels to guard against eavesdropping without communicating device identity in its original form, while the authentication phase ensures that the correct device can only generate the hash of the device ID. Furthermore, the design assumed that every IoT device is embedded with a serialization/device identification chip which provides an unclonable unique device identification. Maxim DS2411 has been considered the most appropriate identification chip that can be embedded into IoT devices and is recommended for all IoT devices that requires no passwords input.

TABLE I. SUMMARY OF LIGHTWEIGHT AUTHENTICATION SCHEMES

Ref.	Challenge Addressed	Proposed Solution	Approach	Tools
[21]	Authentication protocols using RFID prone to disclosure attacks	Preventing disclosure attack on authentication using RFID tag	AES algorithm to create 128 bit secret key for encrypting texts/messages	N/A
[18]	Growing number of devices make authentication complex	Local user authentication scheme that is lightweight in nature based on NFC technology	-3 steps using NFC based on Bluetooth, ZigBee. -using hash function (chaskey) to message authentication	-NFC Technology
[12]	Passwords and pre-defined keys not feasible in IoT network	Lightweight user authentication based on tokens generation for IoT devices	Use tokens to create additional security layer of authentication	N/A
[23]	Current authentication protocols not universally applicable for Io devices	Authentication scheme using hardware serialization	Use of chip embedded in device to generate unique device identification	Maxim DS24II
[20]	MQTT use single channel authentication, easy to attack	Authentication scheme for resource constrained IoT devices based on architectural tokens generation	-publisher, subscriber, MQTT broker and server to generate a toke	N/A
[22]	Weak encryption, delayed encryption in IoT	Robust, secure hybrid parallel model for authentication in IoT	Using iAES and mECC to secure and provide encryption	N/A
[19]	Traditional authentication schemes not feasible for IoT environment	Behavioral profiling model based on app usage	Use machine learning to utilize user's dataset and learn the patterns	PANDA
[17]	Traditional authentication schemes not feasible enough in IoT environment	Lightweight gait authentication scheme using subconscious level activities	-collect data from user's phone -perform features extraction on dataset collected -machine learning to learn patterns and authenticate users	Motorola G4 Plus
[24]	Difficulty in highly constrained IOT devices to load cryptographic credentials.	Two novel authentication deployment schemes. LISA and LISAT	-Devices must be close to each other -use one-way visible light channel (VLC) of multitouch screens to initialize sensor devices -use photodiode BPW34 and 1M resistor to detect signals transmitted	GSM Module, Arduino Pro Mini, Android Smartphone

Perkovic *et al.* [24] approach focused on multichannel key deployment scheme for WSN which requires the presence of light source devices like smartphones or tablets. The objective is to address the challenge of securing large number of inter-connected wireless devices involving initializing cryptographic credentials into large number of devices which are considered of low-cost and highly interface constrained devices lacking usual wired interfaces, displays, keypads, and alike. Two novel multichannel key schemes: LISA and LISAT were employed which requires that devices be present or be closed to each other geographically. Moreover, both are secret-key based and make use of the visible light channel of touch screens to adjust sensor devices in a secure, usable, and scalable way. Accordingly, LISA protocol was implemented on the Arduino Pro Mini platform and the results obtained show the device and the smartphones can actually authenticate and communicated with each other when in a close contact.

IV. Discussions

In this paper, we have performed analysis of some of the proposed and developed lightweight solutions for devices authentication in the IoT. Based on the analysis, findings show that authentication is a serious security challenge to IoT devices and is developing. There are unlimited number of connected devices and of different sizes. These devices are also communicating from different network domain and there is no standardized architecture of security that handles all these devices. Thus, authentication poses a challenge because some of these devices do not have to authenticate themselves on the network and yet may carry sensitive data that could be exploited at any time.

In this paper, we also identified some of the solutions that have been proposed and developed. However, these approaches are of different forms and there is no generic scheme in place that can authenticate all devices. Each proposed is designed to address specific challenge. Table I presents the summary of some of the lightweight schemes considered in this paper which are under the categories of public key based [21, 24, 25], token based [9], procedural-based [7, 18, 22] and the hardware-based [8, 17, 20]. For instance, the scheme proposed by [17] allows devices to authenticate one another when physically close. It is done by placing a sensor on top of a smartphone and using VLC for authentication. However, solution by [17] is not effective since it does not work on geographically dispersed devices. IoT devices communication should be both physically close and geographically dispersed. Moreover, some of the proposed scheme for authentication amongst light source devices e.g. smart watches requires no passwords usage to communicate with each other. The issue with such solution is that, IoT devices are of different sizes and communicating with each other can be between small to small devices, big to small devices or vice versa and big to big devices. Also, [22] proposed the use of symmetric encryption and hashing to improve on the current authentication protocol. However, the approach wasn't implemented just like in [21] and no results shown to evaluate their performance.

In all the proposed solutions analyzed in this study, it is clear that authentication still needs great attention. As more are added the network, robust authentication mechanism is indispensable that have the ability to authenticate all devices regardless of the sizes and network domains to ensure data integrity, confidentiality, and availability.

V. Conclusion

This paper reviewed and presented analysis of some of the existing authentication schemes for IoT devices. The analysis is based on the challenges addressed, the solution offered and the authentication method applied. Based on this analysis, we found that device authentication is a serious security challenge in the IoT realm. Moreover, several solutions have been offered with each having its unique approach, strength, and weakness. However, there is no generic approach to authenticate the growing heterogeneous devices in the network. Thus, there is the needs for a robust and generic scheme to authenticate all devices in IoT from all domains regardless of the sizes. This is important as all these devices play a huge role in generating, processing, and storing data for business or personal use. Therefore, our future work is to design and develop a generic lightweight authentication scheme for the IoT network.

Acknowledgment

This research was supported by the Department of Computer Science at the North West University Mafikeng campus and the CSIR, South Africa.

References

[1] Abidoye, Ademola & Obagbuwa, Ibidun. Models for Integrating Wireless Sensor Networks into the Internet of Things (MIWIT). IET *Wireless Sensor Systems*. 7. 10.1049/iet-wss.2016.0049.

[2] O. Khutsoane, B. Isong, and A. M. Abu-Mahfouz, "IoT devices and applications based on LoRa/LoRaWAN," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*, 2017, pp. 6107-6112: IEEE.

[3] M. Aazam, M. St-Hilaire, C. Lung and I. Lambadaris, "PRE-Fog: IoT trace based probabilistic resource estimation at Fog," *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, 2016, pp. 12-17.

[4] Fadele Ayotunde Alaba, Mazliza Othma, Ibrahim Abaker Targio Hashem, Faiz Alotaibi: Internet of Things Security. Journal of Network and Computer Applications. Vol.88, pp.10-28, 2017

[5] Gu X, Qiu J, Wang J, 2012: Research on trust model of sensors nodes in WSNs, *Procedia Engineering*, Vol. 29, pp.909-913, 2012

[6] O. Helmi et al. "The challenges facing with the internet of things". *International Journal of Scientific Study*. Vol 5. Issue 4., July 2017.

[7] El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors 2019,* 19, 1141.

[8] M. M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," *2015 IEEE World Congress on Services*, New York, NY, 2015, pp. 21-28.

[9] Barreto L., Celesti A., Villari M., Fazio M., Puliafito A. Security and IoT Cloud Federation: Design of Authentication Schemes. In: Mandler B. et al. (eds) Internet of Things. IoT Infrastructures. IoT360 2015. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 169. Springer, Cham, 2016

[10] M. S. Farash, M. Turkanovic´, S. Kumari, and M. Ho¨lbl, "An efficient user authentication and key agreement scheme for heterogeneous

wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Networks*, vol. 36, pp. 152–176, 2016.

[11] Mardiana binti Mohamad Noor, Wan Haslina Hassan: Current research on Internet of Things (IoT) security: A survey. Computer Networks, Vol. 148, Pp. 283-294, 2019

[12] Ankur Gupta, Meenakshi Tripathi, Tabish Jamil Shaikh, Aakar Sharma. "A Lightweight Anonymous User Authentication and Key Establishment Scheme for Wearable Devices" *Computer Networks*, Vol. 149, pp.29-42, February 2019.

[13] Jing, Q., Vasilakos, A.V., Wan, J. et al. "Security of the Internet of Things: Perspective and challenges" *Wireless Netw* (2014) 20: 2481.

[14] Maire O'Neill: "Insecurity by Design: Today's IoT Device Security problem" Engineering, pp.48–49, 2016.

[15] Mohamed Amine Ferrag, Leandros Maglaras, and Abdelouahid Derhab, "Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends," *Security and Communication Networks*, vol. 20, 2019.

[16] Jing, Q., Vasilakos, A.V., Wan, J. et al. "Security of the Internet of Things: Perspective and challenges" *Wireless Netw* (2014) 20: 2481.

[17] P. Musale, D. Baek and B. J. Choi, "Lightweight gait based authentication technique for IoT using subconscious level activities," *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018, pp. 564-567.

[18] M. H. Alharbi and O. H. Alhazmi, "Prototype: User Authentication Scheme for IoT Using NFC," *2019 International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2019, pp. 1-5.

[19] Y. Ashibani and Q. H. Mahmoud, "A Behavior Profiling Model for User Authentication in IoT Networks based on App Usage Patterns," *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, 2018, pp. 2841-2846.

[20] A. Bhawiyuga, M. Data and A. Warda, "Architectural design of token based authentication of MQTT protocol in constrained IoT device," *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, Lombok, 2017, pp. 1-4.

[21] H. Nasir, N. Kanwal and Musfirah, "Prevention of Disclosure Attack on a Mutual Authentication Protocol Using RFID Tag in IoT," *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, Taxila, 2018, pp. 136-139.

[22] S. Dahiya and M. Bohra, "Hybrid parallel partial model for robust & secure authentication in healthcare IoT environments," *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)*, Mathura, 2017, pp. 239-243.

[23] A. Hasan and K. Qureshi, "Internet of Things Device Authentication Scheme Using Hardware Serialization," *2018 International Conference on Applied and Engineering Mathematics (ICAEM)*, Taxila, 2018, pp. 109-114.

[24] Toni Perkovic, Mario Cagali, Tonko Kovacevic : "LISA: Visible light based initialization and sms based authentication of constrained IoT devices". *Future Generation Computer Systems.* Vol. 97, August 2019, Pages 105-118.