A secure lightweight authentication mechanism for IoT devices in generic domain

Sanaz Kavianpour
Abdul Razaq
Gavin Hales

Proc. of the International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME 2023)

19-20 July 2023, Tenerife, Canary Islands, Spain

A Secure Lightweight Authentication Mechanism for IoT Devices in Generic Domain

Sanaz Kavianpour
School of Design and Informatics
Abertay University
Dundee, Scotland, UK
s.kavianpour@abertay.ac.uk

Abdul Razaq
School of Design and Informatics
Abertay University
Dundee, Scotland, UK
a.razaq@abertay.ac.uk

Gavin Hales
School of Design and Informatics
Abertay University
Dundee, Scotland, UK
gavin.hales@abertay.ac.uk

***Abstract*— The Internet of Things prompt deployment enhances the security concerns of these systems in recent years. The enormous exchange of sensory information between devices raises the necessity for a secure authentication scheme for Internet of Things devices. Despite many proposed schemes, providing authenticated and secure communication for Internet of Things devices is still an open issue. This research addresses challenges pertaining to the Internet of Things authentication, verification, and communication, and proposes a new secure lightweight mechanism for Internet of Things devices in the generic domain. The proposed authentication method utilizes environmental variables obtained by sensors to allow the system to identify genuine devices and reject anomalous connections.**

Keywords*— Internet of things, lightweight authentication, port switching for authentication, server port forwarding

I. INTRODUCTION

The Internet of Things (IoT) is one of the most emerging technologies nowadays. IoT is a network of various physical devices, which perform individual tasks for a specific purpose. The non-standard computing devices that are connected to a network wirelessly and can transmit data are known as IoT devices [1]. IoT devices can interact and communicate over the Internet. There are three main categories of devices comprising consumer, enterprise, and industrial. Consumer devices include smart TVs, speakers, toys, wearables, and smart appliances. Enterprise devices are used as edge devices by a business, and they have a variety such as smart locks, smart thermostats, smart lighting, and smart security. Although these devices have various abilities, they tend to sustain and enhance operational efficiency. Industrial devices are used in industrial environments such as factories. These devices are mainly sensors that are used to monitor the manufacturing process and proper running. These sensors can also predict which parts of the device need to be changed to preclude sudden downtime. Devices perform ubiquitous and pervasive computing. IoT's goal is to enable devices to get connected to anything and anyone anywhere via any path, network, and service.

The increase in the number of IoT devices presents broader attack surfaces of the cybersecurity vulnerabilities as typically these devices do not have adequate mechanisms of computing platforms and because of wireless communication, they are vulnerable to network attacks, including data thefts, phishing attacks, spoofing and denial of service attacks. In addition, with the growth of demands of user applications, there is a rise in the number of device connections [2].

Because of the communication of many devices and sensors, a huge amount of data is generated and transferred over the Internet, which requires safe and secure storage and further analysis for decision-making in real time. Gathering this huge amount of data being communicated raises privacy and security concerns [3]. The transmitted data between devices can be intercepted by malicious parties and result in sensitive information leakage. One of the issues from a privacy perspective is that there are various privacy policies for different IoT devices communicating with each other, which require each device to verify the privacy policies of other devices before transmitting the data [4]. Although there are possible security controls such as encryption to protect data in transit, isolation of the network where devices reside, and privileged remote access to segmented networks that can mitigate the attack surfaces, there is still a gap in the security and privacy of IoT systems that requires to be addressed to preclude threats and attacks to each layer of IoT architecture.

Inadequate authentication and authorization, integrity, confidentiality, non-repudiation, availability, privacy, weak transport layer encryption, insecure software, hardware, and web interface are some of the significant concerns. For example, insufficient authentication mechanisms in the devices can provide unlimited access to IoT systems for malicious parties and insider actors. Various authentication schemes including two-factor authentication, biometrics, etc have been employed and adopted for devices in diverse domains as reviewed based on the literature. However, these schemes have some drawbacks and have delineated that further research is required to address the gap to provide efficient and secure authentication mechanisms between devices. Hence, the focus of this paper is on providing a secure authentication mechanism to establish communication between trusted parties and provide a secure exchange of data between IoT

979-8-3503-2297-2/23/$31.00 ©2023 Crown

devices to mitigate privacy and security concerns. This paper's contributions are as follows.

- Reviewing the authentication schemes for IoT devices to provide a preliminary understanding of authentication in IoT architectures and summarize the existing drawbacks of these schemes.
- Proposing a secure lightweight authentication solution for IoT devices in a generic domain.

This paper is organized in the following sections. Section II discusses the literature review. The intended system is explained in Section III, followed by the implementation in Section IV. Section V summarizes the paper and briefly outlines the planned scheme for future research.

II. LITERATURE REVIEW

A. IoT Security Challenges

In designing and developing IoT devices, security and privacy are one of the main challenging issues [5]. Secure communication, application security, and physical device security are required for IoT devices security to ensure data ownership and devices' trustworthiness via their operational cycle. The connection of IoT devices should be secure; otherwise, they will be vulnerable to attacks. The manufacturer, developers, and users are responsible for avoiding any exposure that leads to potential harm. The possible security threats to IoT devices in an unprotected environment are eavesdropping attacks, impersonation attacks, denial of service attacks, parallel session attacks, password change attacks, offline guessing attacks, stolen smart device attacks, gateway node bypassing attacks, and man-in-the-middle attacks. One of the main security challenges of IoT devices is authentication. Each device should be able to identify and authenticate all other devices which interact with it in the system. However, authentication of the vast number of devices is not without drawbacks. For instance, the performance of the IoT system may be decreased as the authentication process requires a vast amount of network communication known as mass node authentication [6]. Furthermore, there are various users for each application which means users require separate permission and access control. In an IoT system, different devices from different manufacturers can be connected. This means various authentication schemes need to be employed, which can be challenging for data privacy. Data should be transferred through trusted and secured protocols. With the ubiquitous intelligence integrated with IoT devices and the diffusion of data and information among these devices over the Internet, privacy concerns have arisen for users. Various devices such as a sensor or RFID tags have different capabilities for computation, memory, and embedded software, which require a lightweight authentication scheme. Although various mechanisms have been developed and used to ensure the users' confidence and self-assurance in using IoT devices, there is still a gap. This paper reviewed and summarised some of the relevant research that has been done for IoT device authentication.

B. Related Work on IoT Authentication Schemes

In 2022, Trinka et al. assessed and categorized current practices related to IoT security solutions, commonly involved technologies, and standards for authentication and authorization [7]. Based on the review in [8], four types of authentication schemes for IoT devices are cloud-based IoT authentication, lightweight authentication, decentralized blockchain-based authentication, and biometrics-based remote user authentication schemes (multifactor authentication). Based on the analysis of the results, although various schemes could provide authentication for devices, they have some drawbacks. For instance, the proposed authentication scheme with the dynamic identity concept for the cloud-based IoT devices was vulnerable to forgery attacks [9]; or the schemes that employed the smart cards as a secure dynamic remote authentication method were vulnerable to offline password guessing attacks [10, 11]. An authentication scheme based on the edge–fog–cloud was proposed that captured the dynamic facial pattern from the edge of the IoT devices. Although this scheme enhances the robustness of the presentation attack, it could not provide mutual authentication and it was not secure enough and had no key agreement [12]. One proposed lightweight authentication scheme based on numerical series cryptography for IoT environments was proposed to provide mutual authentication and session key agreement for IoT devices [13]. According to an informal security review, this approach was resistant to known security attacks and applicable Wireless Sensor Networks (WSNs) IoT applications. However, this approach requires further research in terms of efficiency to data and communication security besides the communication overhead considering other existing protocols. The schemes that provide lightweight remote attestation employing Physical Unclonable Functions (PUFs) to connect software attestation to remotely identifiable hardware delineated high computation and storage overhead. Furthermore, they were not robust against modelling attacks by machine learning techniques, and security protocols were unsafe [14,15]. The mechanisms that integrated blockchains into IoT lack security requirements consideration [16,17] and create identification issues [18]. The developed schemes based on biometrics-based remote user authentication could not provide mutual authentication and were vulnerable to server spoofing attacks [19, 20]. And the mechanism which proposed user authentication and key agreement for WSNs was susceptible to denial-of-service and man-in-the-middle attacks [21]. Table I summarizes the relevant authentication schemes that have been implemented for generic applications. The proposed scheme in this research is comparable to research in [13] considering the efficiency of data and communication security.

III. THE PROPOSED SYSTEM

The system is always defined within the parameters of its domain. Processes in the system will be possibilities of a function in the defined behavior. A system with random possibilities can offer a perfect opportunity to disguise a unique process.

TABLE I. AUTHENTICATION SCHEMES

Reference	Scheme	Strength	Drawbacks
[22]	A lightweight two-factor authentication scheme employing XOR operation and unidirectional hashing	• Resistance to threats such as insider attacks, forgery, user tracking or offline estimations	• Lack of regard for Denial of Service (DoS) and Distributed DoS attacks • High computational cost
[23]	A blockchain based authentication scheme called Bubbles-of-Trust in which the communication between devices is managed by the public block-chain implemented using Ethereum	• Adequate security analysis	• Require additional fees for each transaction because of a public block-chain • Time-consuming for real-time applications
[24]	An authentication scheme based on PUF using Linear Feedback Shift Register (LFSR)	• Possibility for password or biometric updates	• Does not address the potential for machine learning attacks • Inadequate security analysis • Complicated architecture
[25]	An Elliptic curve and symmetric cryptography based authentication and key management scheme	• Provide a mutual confirmation between the Network Control Center (NCC) and the user • Consideration of preserving privacy • Resistance to attacks such as replay, impersonation, stolen verifier, Denial of Service, and offline estimations	• Not efficient regarding computation
[26]	The Two-step verification scheme consists of using secret key or password in the first step and using PUF in the second step	• Resistance to impersonation and physical attacks • Low computation cost	• Does not address machine learning attacks and variations in environmental factors
[27]	GLARM, which is a group-based light-weight authentication and key agreement scheme	• Resistant to Man-in-the-Middle and Denial of Service attack	• No consideration of identity and location privacy
[28]	Speaker-to-microphone (S2M), which is an efficient device validation procedure	• Resistance to various attacks such as audio replay, varying distances, and similar device attacks • Low error rate	• No consideration of location privacy
[29]	Hardware-based fingerprint scheme with PUF and presenting machine learning-based attacks on PUF which creates a software model of the PUF	• Proof-of-concept of how to manage machine learning attacks	• Inadequate consideration of environmental conditions variation
[30]	PUF-based elliptic curve algorithm utilising error correction codes (ECC)	• Using ECC for PUF to manage machine learning threats Handled environmental variations	
[31]	The application of a Symmetric Encryption Algorithm (AES) will hide the modelling process for the PUF	• Resistance to modelling, physical, and side channel attacks	• Environmental variations are not taken into account.
[32]	A multi-tier authentication scheme using credentials with a predetermined physical context	• Resistant to replay type attacks	• No consideration for Denial of Service attacks
[33]	An authentication scheme using Advanced Encryption Standard (AES) for encryption of registered devices and Diffie–Hellman for encryption of unregistered devices on different servers	• Handle timing, brute-force, and MITM attacks • Store cryptography and authentication data on different servers	• No performance evaluation
[34]	Authentication utilizing a triple-factor mechanism including either a fingerprint or iris scan, combined with the use of a smart card and a password.	• Resistance to inside system attacks	• Could not change the credentials
[35]	A customised data encapsulation	• Decrease computation and communication overhead	
[36]	A two-way IoT authentication scheme employing the Datagram Transport Layer Security (DTLS) protocol based on the RSA certificates exchange	• Minimal computational and communication overhead with a high degree of interoperability	• Potentially unreliable because of UDP over DTLS
Proposed Approach	A secure lightweight authentication scheme	• Allow secure authentication to be added to even very simple and low-power devices	

Let there be an independent device. The device is IoT compatible with remote connection and dedicated functionality. A typical IoT device can sense the surrounding environment such as gusts, heat, altitude, etc. Accordingly, a device with a method to quantify these traits with a scope of typical behavior should reveal a key identity on its own. Hence, this research proposes a system that takes advantage of behavioral changes to translate into a secure transaction to construct a device to provide a secure environment for the devices to operate. The change in the device or surrounding environment is considered an anomaly; thus, identifying the entity.

Natural quantities of IoT device sensors are delineated in Table II, and the employed notations have been described in Table III, respectively.

TABLE II. NATURAL QUANTITIES

IoT Device Sensors		
Index	**ID**	**Medium**
1	t	Temperature
2	s	Sound
3	l	Light
4	aq	AirQuality
5	ar	AirPressure
6	h	Humidity
7	p	Proximity
8	ap	Air Pollution

TABLE III. NOTATIONS

Notation	**Description**
m	Medium from one of the Natural Quantities
p	TCP/IP Port
S_p	Source/Listening/Server TCP/IP Port
D_P	Destination/Connecting/Client TCP/IP Ports
T	A single HTTP transaction
nc	New correlation - new activity
sc	Shared correlation - same activity
v	variant correlation - x is to reflect the degree of variation from sc
node	A digital system to monitor

A set of natural quantities supported by the IoT device, can be presented as Equation (1).

$$m = \{t, s, l, aq, ar, h, p, ap\} \quad (1)$$

The members of natural quantity can be expanded to include more relevant and primitive quantities that are more suitable for the enabling environments. However, the quantities depend on the given capability of the device and the environment. For example, a more sophisticated device could host a gyroscope, image sensor, or electromagnetic sensors to capture the right surrounding. The inclusion of these media quantities will also depend on the cost factor and deployed application scope. The proposed architecture is capable of hosting and accommodating these possible expansions. The TCP/IP ports use 16 bits for decimal presentation. Thus, 216 results in 65535 ports available in the system. The proposed system employs a set of ports assigned randomly to the client and server at the compile time. For example, Equation (2) presents a range of ports the server (D_P) and clients (S_P)will utilize to make HTTP transactions such as GET or POST methods. These ports will be shared with all the connecting clients and the server. As proof of concept and for simplicity, we propose to generate this random set of ports at compilation time. However, it can be dynamically generated and shared with all the connecting nodes.

$$S_P = \{500 \geq p \leq 1000\} \Longleftrightarrow D_P = \{500 \geq p \leq 1000\} \quad (2)$$

A function of ports with a pair of connecting and listening can be derived as presented in Equation (3).

$$f(p) = \{S_P , D_P\} \quad (3)$$

All the HTTP transactions would use the predefined ports given in Equation (4). Thus, proving a function of transaction with a function of ports as described in Equation (5).

$$T = \{p_1 , p_2 , \dots , p_n\} \quad (4)$$

$$f(T) = f(p) \quad (5)$$

The transaction function can be further expanded to include media along with the port number. A single transaction can include a single medium or several entities from the medium. The arrangement of such pseudo randomness in the medium query will ensure a further security blanket to achieve true anonymity of the data exchange from the devices.

TABLE IV. MEDIUM AND PORTS

	Medium							
Ports	**t**	**s**	**l**	**aq**	**ar**	**ap**	**h**	**p**
0	0	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0
2	0	1	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0
4	0	0	0	1	0	0	0	0
5	0	0	0	0	1	0	0	0
6	0	0	0	0	0	1	0	0
7	0	0	0	0	0	0	1	0
8	0	0	0	0	0	0	0	1
...	x	x	x	x	x	x	x	x
255	1	1	1	1	1	1	1	1

The transaction presented in Equation (5) can be further enhanced with Table IV (Medium and ports). In Table IV, every row presents a set of unique natural quantities on the unique port. The uniqueness of a transaction provides a pseudo-random process to acquire device data and provides real-time information. An anomaly in either of these processes will trigger the alarm and activate the contingency methods.

$$f(T) = (m, p) \tag{6}$$

$$f(T_k) = (m_i, p_j) \tag{7}$$

$$f(T_{k+1}) = (m_{i+1}, p_{j+1}) \tag{8}$$

IV. IMPLEMENTATION

The proposed system is implemented as follows, shown in Fig.1.

A. Lightweight Protocol

The Lightweight Protocol (LWP) is designed with two major requirements: speed and lightweight. This LWP is executed at low-end IoT devices with limited CPU power and storage. This simple yet secure protocol provides robust communication because of its simple design.

B. System Design

A structure of three data members consists of TCP/IP port numbers, sensor data, and the type used to store data. The entries are represented in components of port, sensor type and quantity. For example, 2@64 will point to the second entry of the 3 with *p* value holding the port number, and *m* for sensor type, *s* entry will be populated with new data from the required sensors. The size and type of structure can be adjusted based on the target device. A two-dimension word (2 bytes = 8x8 matrix) array should be sufficient to hold TCP/IP ports and medium data. However, the type of medium entity can be replaced with an integer data type to accommodate more accuracy of sensor data.

```
/*
Start with tx from the first index Or reset the index
if it is the l as t one Tx return with the next index
Rx starts from the index returned by tx Rx_i return with the next index
*/
struct table
  {
      unsigned short p;   /* ports */
      unsigned char m;   /* sensor types */
      unsigned   int d;   /* sensor data */
} ;
     int table [8] [8]; /* Double array to hold ports and medium*/
      generate a table with ports and medium data placeholders.
```

Fig. 1. Listing 1: System Abstraction.

V. CONCLUSION

This paper presents a novel lightweight authentication method specifically designed for use in IoT and embedded systems to address some of the disadvantages of existing mechanisms. Upon reviewing existing literature, existing authentication mechanisms are subject to issues such as high complexity when implemented in the IoT and embedded systems domain. The proposed mechanism allows for the authentication of IoT devices in a way which is lightweight, allowing secure authentication to be added to even very simple and low-power devices.

The proposed authentication method utilizes environmental variables obtained by sensors to allow the system to identify genuine devices and reject anomalous connections. As the system is likely to have multiple co-located devices, it can identify which values to expect. If an unauthorized device is connected to the system from a remote location, the environmental variables used for authentication will be detected as anomalous and will be rejected. A limitation of this system is that some of these environmental variables could possibly be found by an attacker and used to appear genuine. For example, if the temperature variable alone was used, then an attacker may query a weather service to find the correct value if they know the location of the IoT system they are attacking. This is simple to derive by querying the location of the system based on its IP address. The proposed system addresses this using multiple environmental factors which when combined, would be challenging to derive from a remote location. For example, although the temperature of a location is often published online, the current light level is more challenging to find remotely. When combined with other frequently changing factors such as sound level, this makes it increasingly more difficult to spoof the expected values.

The future work of this project will explore lightweight transport security mechanisms which complement the proposed lightweight authentication protocol. Implementing such a mechanism can ensure that the authentication protocol here is resistant to man-in-the-middle attacks while maintaining a low computational overhead. This work will also look to develop a proof-of-concept open-source library for implementation in IoT projects. This will allow for real-world experimentation and peer review of the proposed lightweight authentication protocol in-situ. Additionally, there is the possibility for machine learning to be implemented in the authentication process to allow anomalous connections to be detected with minimal user intervention, and for a mesh architecture to be designed which will allow the system and machine learning algorithm to build a consensus of what is genuine and anomalous, using environmental variables sourced from many closely located IoT devices.

REFERENCES

[1] K.K. Patel, S. Patel, and C. Salzar, “Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges,” IJESC, 6(5), 2016. DOI 10.4010/2016.1482.

[2] R. Hassan, F. Qamar, M. Kamrul Hasan, A.H. Mohd Aman, and A. Sid Ahmed, “Internet of Things and Its Applications: A

Comprehensive Survey," Symmetry 2020, 12 (10), 1674. DOI:10.3390/sym12101674.
[3] S. Kumar, P. Tiwari, and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review, " Journal of Big Data, 6(111), 2019.
[4] X.Wu, F. Ren, Y. Li, Zh. Chen, X.Tao, "Efficient Authentication for the Internet of Things Devices in Information Management Systems," Efficient Authentication for the Internet of Things Devices in Information Management Systems, vol.2021. https://doi.org/10.1155/2021/9921036
[5] L.Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT Privacy and Security: Challenges and Solutions," Applied Sciences, 2020.
[6] I. Inayat Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," International Journal of Computer Science and Information Security (IJCSIS), vol. 14(8), 2016.
[7] M. Trnka, A. Abdelfattah, A. Shrestha, M. Coffey, and T. Cerny, "Systematic Review of Authentication and Authorization Advancements for the Internet of Things," Sensors, 2022.
[8] S.Kavianpour, B. Shanmugam, S. Azam, M. Zamani, G. Narayana Samy, and F. De Boer, " A Systematic Literature Review of Authentication in the Internet of Things for Heterogeneous Devices," Journal of Computer Networks and Communications, vol. 2019. https://doi.org/10.1155/2019/5747136.
[9] C. Lee, T.H.; Lin, and R.X. Chang, "A secure dynamic id-based remote user authentication scheme for the multi-server environment using smart cards," Expert Systems with Applications, vol. 38 (11), 2011, pp. 13863–13870.
[10] S. Shunmuganathan, R.D. Saravanan, and Y. Palanichamy, "Secure and efficient smart-card-based remote user authentication scheme for the multi-server environment," Canadian Journal of Electrical and Computer Engineering, vol. 38 (1), 2015, pp. 20–30.
[11] T. Maitra, S.K.H. Islam, A. Amin, D. Giri, M.K. Khan, and N. Kumar, "An enhanced multiserver authentication protocol using password and smart card: Cryptanalysis and design," Security and Communication Networks, vol. 9(17), 2016, pp. 4615–4638.
[12] A. Castiglione, M. Nappi, and S. Ricciardi, "Trustworthy Method for Person Identification in IIoT Environments by Means of Facial Dynamics", IEEE Transactions on Industrial Informatics, vol. 17(2), 2021, pp. 766–774.
[13] M. Aladdin, K. Nagaty, and A.Hamdy, "Secure authentication scheme based on numerical series cryptography for the Internet of Things," Journal of Theoretical and Applied Information Technology, vol.100 (23), 2022.
[14] R. Amin, N. Kumar, G.P. Biswas, R. Iqbal, and V. Chang, "A lightweight authentication protocol for IoT-enabled devices in a distributed cloud computing environment," Future Generation Computer Systems, vol.78, 2018, pp. 1005–1019.
[15] J. Kong, F. Koushanfar, P.K. Pendyala, A.R. Sadeghi, and C. Wachsmann, " PUFatt: embedded platform attestation based on novel processor based PUFs," In Proceedings of the 51st ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, June 2014.
[16] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, 2016, pp. 2292–2303.
[17] Q. Xu, K.M.M. Aung, Y. Zhu, and K.L. Yong, "A blockchain-based storage system for data analytics on the internet of things," In New Advances in the Internet of Things, Springer, Berlin, Germany, 2018, pp. 119–138.
[18] A. Dorri, S.S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: the case study of a smart home," in Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, March 2017.
[19] Y.P. Liao and C.M. Hsiao, "A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol," Ad Hoc Networks, vol.18, 2014, pp. 133–146.
[20] Y.An, "Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards," Journal of Biomedicine and Biotechnology, vol. 2012, 2012.
[21] L. Chen, F. Wei, and C. Ma, "A secure user authentication scheme against smart- Card loss attacks for wireless sensor networks using symmetric key techniques," International Journal of Distributed Sensor Networks, vol. 11(4), 2015, pp. 63–73.
[22] L. Zhou, X. Li, K.H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstances," Future Generation Computer Systems, vol. 91, 2019, pp. 244–251.
[23] M.T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol.78, 2018, pp. 126–142.
[24] B.Srinivasu, P. Vikramkumar, A. Chattopadhyay, and K.Y. Lam, " CoLPUF: A Novel Configurable LFSR-based PUF," In Proceedings of the 2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26-30 October 2018, pp. 358– 361.
[25] M.Qi, J. Chen, and Y. Chen, "A secure authentication with key agreement scheme using ECC for satellite communication systems," International Journal of Satellite Communications and Networking, 2018.
[26] M.N. Aman, K.C. Chua, and B. Sikdar, "Mutual Authentication in IoT Systems Using Physical Unclonable Functions," IEEE Internet of Things Journal, vol. 4 (5), 2017, pp. 1327–1340.
[27] C. Lai, R. Lu, D. Zheng, H. Li, and X.S. Shen, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine-to-machine communications," Computer Networks, 2016; vol. 99, 2016, pp. 66–81.
[28] D. Chen, N. Zhang, Z. Qin, X. Mao, Z. Qin, X. Shen, and X. Li, " S2M: A Lightweight Acoustic Fingerprints based Wireless Device Authentication Protocol," IEEE Internet Things Journal, vol. 4, pp. 88–100.
[29] D. Mukhopadhyay, "PUFs as Promising Tools for Security in Internet of Things," IEEE Design & Test, vol. 33 (3), 2016, pp.103–115.
[30] J.R. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22-24 August 2016.
[31] M. Barbareschi, P. Bagnasco, and A. Mazzeo, "Authenticating IoT Devices with Physically Unclonable Functions Models," In Proceedings of the 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Krakow, Poland, 4-6 November 2015.
[32] A. Singh and K. Chatterjee, "A secure multi-tier authentication the scheme in cloud Computing environment," In Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 19-20 March 2015.
[33] F.F.Moghaddam, S.G.Moghaddam, S.Rouzbeh, S.K. Araghi, N.M. Alibeigi, and S.D. Varnosfaderani, "A scalable and efficient user authentication scheme for cloud computing environments," In Proceedings of the 2014 IEEE REGION 10 SYMPOSIUM, Kuala Lumpur, Malaysia, 14-16, April 2014.
[34] J.Z. Lu, T. Chen, J. Zhou, J. Yang, and J. Jiang, "An enhanced biometrics-based remote user authentication scheme using smart Cards," In Proceedings of the 2013 6th International Congress on Image and Signal Processing (CISP), Hangzhou, China, 16-18 December 2013.
[35] Y.L. Zhao, "Research on Data Security Technology in the Internet of Things," Applied Mechanics and Materials, vol. 433-435, 2013, pp.1752–1755. http://dx.doi.org/10.4028/www.scientific.net/AMM.433-435.1752.
[36] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11 (8), 2013, pp. 2710–2723.