Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment

Ali Shahidinejad, Mostafa Ghobaei-Arani, Alireza Souri, Mohammad Shojafar, and Saru Kumari

***Abstract*— Due to the ever-growing use of active Internet devices, the Internet has achieved good popularity at present. The smart devices could connect to the Internet and communicate together that shape the Internet of Things (IoT). Such smart devices are generating data and are connecting to each other through edge-cloud infrastructure. Authentication of the IoT devices plays a critical role in the success of the integration of IoT, edge, and cloud computing technologies. The complexity and attack resistance of the authentication protocols are still the main challenges. Motivated by this, this paper introduces a lightweight authentication protocol for IoT devices named *Light-Edge* using a three-layer scheme, including IoT device layer, trust center at the edge layer, and cloud service providers. The results show the superiority of the proposed protocol against other approaches in terms of attack resistance, communication cost, and time cost.**

I. INTRODUCTION

Internet of things (IoT) is a network of interconnected devices such as tags, sensors, and smartphones over the Internet. IoT devices can collect and generate data and communicate with each other. However, these devices have some limitations, such as a low battery, low power, and low memory. The IoT devices and their data are overgrowing; therefore, storing, computing, and analyzing IoT data is an important issue. To handle this, there should be enhanced technologies such as edge/cloud computing to manage the storing and computation issues. Currently, cloud servers, including public and private ones, are providing different services such as Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a Service (SaaS). The edge computing paradigm has developed to bring resource capabilities at the edge of the network and closer to consumers' location for reducing service latency and network traffic. In all edge/cloud applications, authenticating the consumers before accessing their demanded services is essential. Various techniques have been proposed in the literature to authenticate the consumers, which vary based on computation cost, speed, and robustness against attacks [1]. The existing authentication protocols are not safe against vulnerabilities, and also, in most of them, the high complexity is a major problem. To overcome high complexity and vulnerability issues, this paper proposes a lightweight authentication protocol for IoT devices using a three-layer scheme, including IoT device layer, trust center at the edge layer, and cloud service providers. The main contributions of the paper are listed as follows:

- We propose a lightweight authentication protocol for IoT devices in an edge environment that we name it *Light-Edge*.
- We enhance consumers' security against different types of attacks, such as eavesdropping, and Denail of Service (DoS).
- We evaluate the proposed Light-Edge protocol in terms of attack resistance, communication cost, and time cost required for the authentication process.
- We provide a future vision for the enhanced version of realizing the authentication schemes in future networks such as fifth generation or sixth generation network (5G/6G).

II. RELATED WORK

Providing security for Internet services and their applications is the key to earn the trust of users. They must be assured of the Internet's safety, its applications, and connected equipment against online threats. In the following, we review the background of the authentication schemes applied for IoT devices.

Username-password authentication scheme was first introduced by [2], where authors used a secure one-way function to encrypt the password. However, this protocol is dependent on the encrypted password table that is threatened by the stolen-verifier attack [3]. Various authentication techniques based on username and password have been proposed. Li et al. [4] proposed a multi-server authentication technique based on the neural network; however, the complexity of the protocol was high. Kalra et al. [5] have proposed a mutual authentication protocol to enhance the communication security of IoT devices and cloud service providers using HTTP cookies and elliptic curve cryptography (ECC). Their proposed protocol consists of three phases, namely registration, pre-computation, and authentication, to guarantee the security requirements include confidentiality, forward secrecy, mutual authentication, and anonymity. Their security analysis results indicated that their proposed protocol is robust against man-in-the-middle, cookie theft, offline dictionary, and replay attacks.

Amin et al. [6] have designed an extended authentication scheme for IoT devices in geo-distributed cloud systems. They studied the protocol in [7] and indicated that it is not resisted against session key discloser and user impersonation attacks, and it is not provided with some of the security requirements such as user anonymity. Therefore, they proposed a framework according to the geo-distributed cloud system to store and retrieval all confidential information from the private cloud servers. They demonstrated that it protected against security attacks, including user impersonation, offline password guessing, privileged insider, session key discloser, and replay attacks. Amin et al. [6] and Xue et al. [7] proposed authentication protocols for multi-server distributed cloud systems, while the authentication protocol in this paper is applicable for edge-cloud systems.

Kumar et al. [8] have proposed a secure authentication scheme to support key exchange between cloud servers and RFID tags in vehicular cloud computing networks. They used ECC to provide secure communication with anonymity attributes. They illustrated that it is safe against man-in-the-middle and replay attacks. Their performance analysis results on their proposed work also provided good performance in terms of computation and cost compared with the existing approaches.

Butun et al. [9] presented a cloud-centric authentication as a service approach that addresses time constraints and scalability. Aghili et al. [10] proposed an energy-efficient and secure protocol for E-Health Systems in IoT. Their proposed protocol provides both key agreement and authentication for preserving the privacy of patients and doctors.

Zhang et al. [11] proposed an edge computing-based authentication protocol for vehicular networks. They used a fuzzy logic controller to select an edge computing vehicle, and then they provided a mutual authentication between the vehicles and edge computing. However, in this paper, we use the fuzzy controller for IoT decive's trust computation.

Nevertheless, none of the aforementioned protocols can preserve a lightweight authentication for general IoT applications in a three-layer IoT scheme. Interestingly, in this work, we propose a lightweight protocol for the edge-cloud environment, which provides secure authentication, and it can be used for various IoT applications.

III. Light-Edge : Proposed Protocol

In here, we introduce our lightweight authentication protocol (Light-Edge). The main elements of the proposed approach are devices, trust center, and cloud servers. The general procedure includes registering the devices into the trust center to communicate with the cloud server and request services. By doing so, a unique identifier and password are assigned to each device, which is used for login into the network and authenticating. A unique identifier is also assigned to each server. After authentication, the trust center encrypts messages and communications between devices and cloud servers using the designed cryptography algorithm. In the trust center, in addition to securing applications and authentications, we define request time and delay thresholds. Also, we measure the reliability level of each device to determine its level of access.

Figure 1 shows the sequence diagram of the proposed protocol. Table I represents the used variables in the sequence diagram.

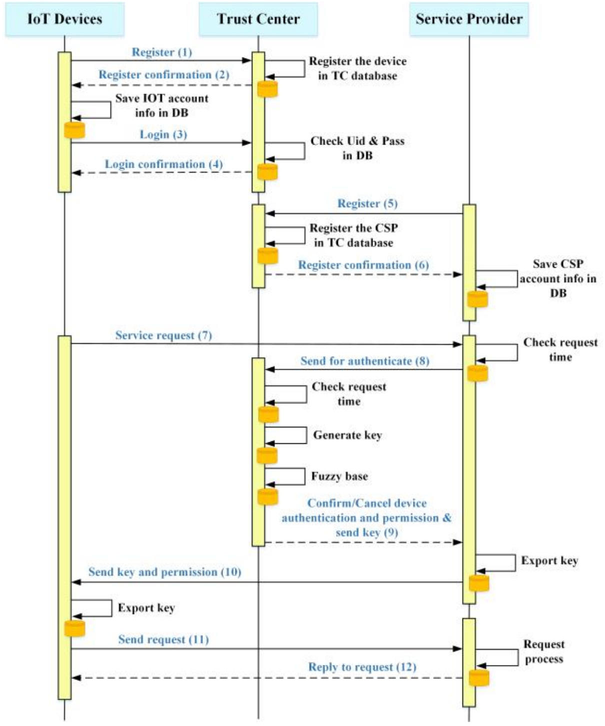
IoT Devices
Trust Center
Service Provider
Register (1)
Register the device in TC database
Register confirmation (2)
Save IOT account info in DB
Login (3)
Check Uid & Pass in DB
Login confirmation (4)
Register (5)
Register the CSP in TC database
Register confirmation (6)
Save CSP account info in DB
Service request (7)
Check request time
Send for authenticate (8)
Check request time
Generate key
Fuzzy base
Confirm/Cancel device authentication and permission & send key (9)
Export key
Send key and permission (10)
Export key
Send request (11)
Request process
Reply to request (12)

Fig. 1. Sequence diagram of the proposed authentication protocol, DB:= database; CSP: cloud service provider;

TABLE I. Variables and their definitions

Variable	Definition
TC	Trust Center
CSP	Cloud service provider
SP_j	Service provider j
UID_I	ID of device or group i
p_I	Password of device i
SID_J	ID of server j
b_I	Random number chosen by device i
d_J	Random number chosen by server j
H (.)	Unilateral hash function
TS	Time sticker
X	Security number of trust center for devices' communications
$\oplus$	XOR operator
+	Adjoint operator
ΔRT	Threshold of the distance of sending devices' requests to a server
ΔT	Threshold of delay

Step 1: Each device registers in the trust center so that its information gets stored. Each device sends $(UID_i \,.\, A_i \,.\, b_i)$ to TC, where $A_i = H(P_i + b_i)$.

Step 2: The TC assigns a unique identifier for each IoT device and calculates $PUID_i = H(UID_i + b_i)$, $M_i = H(PUID_i + X)$, $C_i = h(PUID_i + A_i)$, and $D_i = M_i \oplus C_i$. Then, TC registers the device in the TC database, and sends a registration confirmation to the device.

Step 3: The device saves the account information into its database and then log into the network using the given username and password.

Step 4: By evaluating the information stored in the database, device's entry is authorized by the trust center. Otherwise, it disconnects from the network.

Step 5: Servers must register in the trust center as well in order to serve the IoT devices. CSP send $\left(SID_j \,.\, d_j\right)$ to TC.

Step 6: TC assigns a unique identifier and password for each provider, and the CSP's information gets stored in the TC database. Then Tc sends register confirmation to CSP.

Step 7: After logging into the network, the device sends a request to the provider.

Step 8: Each request to the cloud provider requires the device to be authenticated. So, the server sends the device's information to TC in order to evaluate the device's entry and to concede a mutual key for connection. After evaluating time parameters including the gap between two adjacent requests of the device, which must not be less than the threshold of the time gap of sending a request to a provider ($TS_i^t - TS_i^{t-1} \geq \Delta RT$) and also the delay which must not override the threshold ($T_{SPj}^{cur} - TS_i < \Delta T$), the trust center proceeds to generate the key. Evaluating the reliability of devices and accordingly assigning accessibility is a vital task of the trust center, which is done by receiving device's performances from providers. The negative and positive bounds of the time frame are defined by $W_p = |Curr - Pos|$ and $W_n = |Curr - Neg|$, where Pos and Neg are approvable time frame boundaries, and $Curr$ represents the current time. If positive action is in the W_p bound, it is considered a positive one; otherwise, it is disqualified. The same story happens for a negative action in W_n bound.

The device's trust is computed through a fuzzy system by its number of positive and negative actions. The input variables of a fuzzy system are the number of positive and negative behaviors. A triangle membership function is used for both the number of positive and negative behaviors translated into linguistics variables (low, normal, and high).

Step 9: After confirming the device's authentication in step 8, the trust center sends the key to the cloud provider.

Step 10: The ability to send requests and receive services will be obtained by sharing the mutual key between the provider and the device. In this step, the cloud provider exports the mutual key to the IoT device.

Step 11: Using the issued key, the device can now communicate with the provider securely and request services. We use LEAIoT encryption to send messages securely, which stands for Lite Encryption Algorithm used for communications with the least delay in the IoT [12]. Compared with state-of-the-art encryption algorithms, LEAIoT was proved to have the lowest key generation time [12].

Step 12: The provider would reply to device's request.

IV. Simulation Results

In this section, the simulation results are discussed in order to investigate the performance of the proposed protocol (Light-Edge). The proposed approach is compared with *three* methods Amin et al. [6], Li et al. [4], and Xue et al. [7]. The main reason for choosing these methods is that they are the most widely used among all the available methods. Furthermore, these methods show different performances in terms of security and complexity, making the comparison more meaningful in the cloud-edge environment.

AVISPA software has been used to evaluate the protocol's validation, and MATLAB is used for evaluating the computation time cost and the average communications cost. The On-the-Fly Model Checker (OFMC) and Constraint-Logic-based ATtack SEarcher (CL-Atse) tools are used to formally validate the proposed approach. These tools analyze the security of cryptographic protocols efficiently and versatility. The formal security analysis results show that the Light-Edge and Amin et al. [6] are safe under both OFMC and CL-Atse tests, while Li et al. [4] approach is unsafe under the CL-Atse test, and Xue et al. [7] is unsafe under OFMC test.

To strengthen the security of a system, some security requirements should be assured in the authentication process, including (1) mutual authentication, denoted as *MA*, (2) confidentiality, denoted as *Conf*, (3) anonymity, denoted as Anon, (4) accessibility, denoted as Access and (5) scalability, denoted as *Scal*. Table II shows the performance of Light-Edge and counterpart approaches in terms of security requirements.

TABLE III. Security requirements comparison

	MA	*Conf*	*Anon*	*Access*	*Scal*
Light-Edge	✓	✓	✓	✓	✓
Amin *et al.* [6]	✓	✓	✓	×	×
Li *et al.* [4]	✓	×	×	×	×
Xue *et al.* [7]	✓	×	✓	×	×

Light-Edge provides all the security requirements, while other approaches do not satisfy all the security requirements. Given that the authentication is performed in both ends, i.e., the device and the cloud provider, it proves that Light-Edge meets the mutual authentication security requirement. The trust center uses encryption variables and random numbers for all the messages transferred between the device, the cloud provider, and the center. Also, the cloud provider and IoT devices sign up in the trust center, which illustrates that confidentiality has been ensured in the proposed method. Even if an attacker could bypass the initial authentication steps, he/she still cannot sabotage in steps of the time frame, and fuzzy system check and its session will get terminated as a fake device. Consequently, Light-Edge meets the anonymity security requirement. Since the device has access only to a certain set of resources, the access control security requirement is met. Finally, since the Light-Edge protocol is extensible and allows a new device entry to the network, and remains stable, the scalability security requirement is met.

Table III shows the performance of the proposed approach under different types of attacks such as eavesdropping (Eaves), duplication (Dup), offline password guessing (Off), authorized internal attack (Int), Man in the Middle (MITM), device impersonation (Imp), and Denial of Service (DoS), compared to other approaches.

TABLE IIIII. Attack resistance comparison, where ✓:= the method does not support the property, and ×:= the method supports the property

	Eaves	Dup	Off	Int	Imp	DoS	MITM
Light-Edge	✓	✓	✓	✓	✓	✓	✓
Amin *et al.* [6]	✓	✓	✓	✓	✓	×	×
Li *et al.* [4]	✓	×	×	×	×	×	×
Xue *et al.* [7]	✓	✓	×	×	×	×	×

Considering one device and one cloud server, Fig. 2 shows the computation time cost, including login time cost and authentication time cost for different approaches. As shown in the figure, the Light-Edge approach shows a better performance in terms of time cost than other approaches.

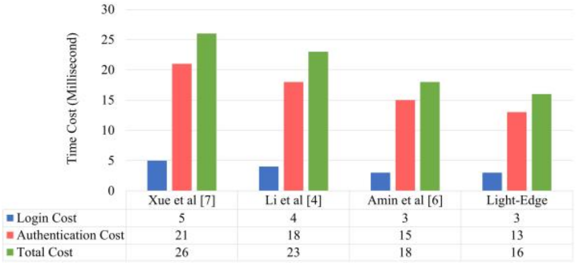

Fig. 2. Time cost comparison

Considering 100 to 1000 devices and ten cloud servers, Fig. 3 illustrates the average communication cost of authentication (CCA) and login (CCL) for different methods. It specifies that Light-Edge has more stability than the other techniques by adequately managing the devices, calculating the trust degree, and controlling the accessibility level. However, Light-Edge's communication cost is higher than Li et al. method; Light-Edge provides higher security, as shown in Tables II and III.

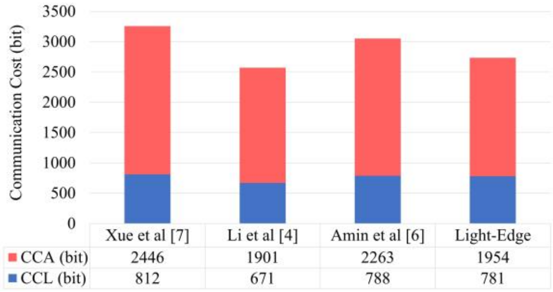

Fig. 3. Comparison of average communication cost

V. Challenges and Future Vision

Despite the promising prospect of future IoT applications and edge computing integration, some significant research challenges remain to be addressed in realizing the authentication schemes. Some of these challenges are as follows:

- Recently, many authentication schemes have been proposed for emerging computing paradigms such as edge/cloud to support IoT services. However, none of them considered the mobility of the device. In some IoT applications, such as the Internet of vehicular, users travel from the coverage of an edge or fog node to another. If each edge/fog node authenticates the devices independently, there will be an additional latency, which is not acceptable in real-time services. There should be a secure sharing of authentication decisions or cooperation among edge/fog nodes to authenticate the devices.
- Time-sensitive services have been widely projected for future 6G networks. Satisfying the demanded delay of these services increases the computation, which is beyond the capacity of the IoT devices. Offloading the computation to the edge devices provides the demanded computation and storage. However, some threats such as edge device compromise and privacy leaking might crash the security of the consumers. In this emerging paradigm, there is a need for secure and private mutual authentication.
- The next generation of the smart industry is highly dependent on the development of 5G/6G and Industrial IoT technologies. Without considering the privacy-preserving in such high-sensitive communication technologies, the configuration state can be modified or attacked. The security issues regarding the database of consumers in the cloud provider were not considered in this study. Therefore, a future study is to consider the privacy-preserving issues and test the authentication system under database threat.
- Edge/fog computing has a decentralized architecture, and it is not easy to gather and manage the behavior of IoT devices and evidence to compute the trust. Also, the trust management scheme should be designed according to the situations and types of services. Furthermore, the trust management scheme should support consistency and scalability when the network

condition changes by traffic patterns, scaling in or scaling out the edge/fog nodes, and the mobility of consumers. Because of these reasons, it is still challenging to realize efficient trust management.

VI. Conclusion

In this paper, we proposed Light-Edge, an authentication protocol for IoT devices where the trust center was responsible for the trust computation of devices connecting the cloud provider. To access the secured information in the cloud provider, we designed a three-layer lightweight authentication protocol and computed each device's trust value using a fuzzy logic-based controller. There were three main secure communications in this framework: (1) the devices and the trust center, (2) the cloud provider and the trust center, and (3) the devices and the cloud provider. Each of these communications was established if confirmed by the trust center. The obtained results showed that the proposed protocol is safe against different vulnerabilities, and also it is efficient in terms of complexity and time cost. We provided a technical report [13] wherein selected procedures, and additional simulation results are presented in more detail.

References

[1] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 616-644, 2020.

[2] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM,* vol. 24, no. 11, pp. 770-772, 1981.

[3] H. Song, G. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems*. Wiley Online Library, 2017.

[4] L.-H. Li, L.-C. Lin, and M.-S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," *IEEE Transactions on Neural Networks,* vol. 12, no. 6, pp. 1498-1504, 2001.

[5] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive and Mobile Computing,* vol. 24, pp. 210-223, 2015.

[6] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Generation Computer Systems,* vol. 78, pp. 1005-1019, 2018.

[7] K. Xue, P. Hong, and C. Ma, "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture," *Journal of Computer and System Sciences,* vol. 80, no. 1, pp. 195-206, 2014.

[8] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Vehicular Communications,* vol. 22, p. 100213, 2020.

[9] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Communications Magazine,* vol. 54, no. 4, pp. 47-53, 2016.

[10] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight Three-Factor Authentication, Access Control and Ownership Transfer Scheme for E-Health Systems in IoT," *Future Generation Computer Systems,* vol. 96, pp. 410-424, 2019/07/01/ 2019.

[11] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge Computing-Based Privacy-Preserving Authentication Framework and Protocol for 5G-Enabled Vehicular Networks," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 7, pp. 7940-7954, 2020.

[12] M. A. Habib, M. Ahmad, S. Jabbar, S. H. Ahmed, and J. J. Rodrigues, "Speeding Up the Internet of Things: LEAIoT: A Lightweight Encryption Algorithm Toward Low-Latency Communication for the Internet of Things," *IEEE Consumer Electronics Magazine,* vol. 7, no. 6, pp. 31-37, 2018.

[13] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, " A Technical Report for Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment," *ArXiv preprint arXiv:2101.06676,* 2021.

Ali Shahidinejad is an Assistant Professor at Qom Branch, Islamic Azad University. Contact him at a.shahidinejad@qom-iau.ac.ir.

Mostafa Ghobaei-Arani is an Assistant Professor at Qom Branch, Islamic Azad University. Contact him at m.ghobaei@qom-iau.ac.ir.

Alireza Souri is an Assistant Professor at Department of Computer Engineering, Haliç University, İstanbul, Turkey. Contact him at alirezasouri@halic.edu.tr.

Mohammad Shojafar is an Associate Professor at 6G innovation Centre (6GIC), University of Surrey, Guildford, United Kingdom. Contact him at m.shojafar@surrey.ac.uk.

Saru Kumari is an Assistant Professor at Department of Statistics, Chaudhary Charan Singh University, Meerut, India. Contact her at saryusiirohi@gmail.com.