Al-Rafidain Journal of Computer Sciences and Mathematics (RJCM)

www.csmj.mosuljournals.com

Lightweight Authentication for Devices in Internet of Thing Environment: A Survey

Sameera Abbas Fadhel [1], *Dr. Ahmed S. Nori [2]

Department Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq[1]
Department Cyber Security, College of Computer Science and Mathematics, University of Mosul, Mosul/Iraq[2]
**Corresponding author. Email: sameeraabbasfadhel@uomosul.edu.iq*

Article information

Article history:
Received: 17/4/2023
Accepted: 25/9/2023
Available online:

Abstract

Internet of Thing (IoT)" is a major and emerging technology where different devices are associated together to operate smartly deprived of human's intervention. IoT has a great effect on economic, social and commercial life. The extremely large number of associated devices together through different protocols make it vulnerable to be threatened by several types of attacks, such as; Unauthorized Access and Authentication Attacks, Network Attacks, Data Privacy and Integrity Attacks, and Supply Chain Attacks. Building and developing lightweight authentication systems for IoT devices are indeed crucial due to several compelling reasons, including; Resource Constraints, Security Concerns, Scalability, Bandwidth Efficiency, Latency Considerations, Cost Reduction, Long Lifecycle and the overall User Experience. Blockchain and "Machine Learning (ML)" are emerging technologies that may be exploited in solving different security problems. This paper presents a survey of lightweight authentication protocols and schemes that are adopted and applied for IoT environment. The security issues in IoT environment are also discussed besides the different types of attacks that may face the network. The paper held a comparison between the selected works and studies in terms of different criteria including the benefits, the results, the used applications and technologies or methods.

Keywords:
Internet of Things, Machine Learning, Security, Lightweight Authentication, IoT Applications..

Correspondence:
Author: Sameera Abbas Fadhel
Email: sameeraabbasfadhel@uomosul.edu.iq

I. INTRODUCTION

The "Internet of Thing (IoT)" are a worldwide connected networks, that are connected to each other through the internet and capable to collect and share electronic information [1]. While the devices number within the network increases, then IoT is growing accordingly [2]. The internet likelihood is broadening through IoT and hence it made unavoidable [3]. Actually, IoT is considered nowadays one of the newest, most essential and fastest spreading tools in communication field. IoT includes set of smart device and integrated sensors which are connected with internet via "Wireless sensor Networks (WSNs)". This in turns open the door for adopting new approaches to exchange the data between the devices efficiently [4]. Practically, the communication environment of IoT is employed in different applications including; smart homes, "smart health care", "smart traffic monitors", etc. [5]. Within IoT environment, the sensor nodes have their particular limitations including; low capacity of storage, limited computing capability and battery. The involved data within IoT ecosystem includes information with great deal of sensitivity that need high confidentiality [6][7]. The security of the transmitted data is the most essential concern in IoT environment, which can be guaranteed through establishing a secure channel among different devices [8][9]. This in turns requires a set of security operations including; data integrity, authorization and authentication. There are different cryptography algorithms that are obtainable to be used in data security such as asymmetric and symmetric algorithms, such as;

AES, DES, 3-DES, RSA, etc. [8][9]. However, the used in IoT are not sufficiently strong to process these set of encryption methods, it also could not store additional data on it. Alternatively, lightweight algorithms that support a smaller bits' number at a time could be adopted and applied. This is why lightweight cryptography on IoT is on a great deal of importance [10][11][12].

IoT devices have essential roles in commercial and industrial activities, they are classified as industrial application devices and home automation devices[13]. Due to the growing dependence on IoT devices, the cyber security issue has become on a great deal of importance and sensitivity. Consequently, different types of attacks that the IoT device may expose should be considered and addressed. The security analysis should also recognize the strengths and the weaknesses of the system on order to design highly secured and high quality IoT system [13].

In fact, there are different protocols and schemes that were proposed in the literature to achieve secure authentication for IoT devices. This survey paper presents and investigates these studies and held a comparison between these studies in terms of different criteria. The first section from this paper presented an introduction to IoT. The rest of this paper is organized as follows: section II discusses the security issues in IoT environment, section III is the literature review part, section IV compares the presented studies and finally the conclusion is presented in section V.

II. IOT SECURITY ISSUES

The benefits of IoT systems have their effect on the adaption of smart technology to facilitate human life through applying it in different places including; offices, homes, etc. [14]. Through IoT emergence, new opportunities were brought up in different fields like; smart homes, industry, farming, healthcare, transportation, etc. [14]. The security threats in IoT environment are required to be addressed due to the rapid development and adoption of IoT devices in our daily life [14]. Authentication in IoT involves verifying access capabilities or credentials, securing access to operational devices and identified users in network communications. This section explores authentication requirements, existing schemes, technologies, and key management in IoT [4]. There are different types of attacks that threaten the IoT environment. Different possible attack types are briefly discussed in this section [14].

The first type is the physical attack that is related to the network hardware devices and it affects the system physical functionality [14]. The second type is the side-channel attack that occur in case that a security exploit collects information from the program execution influence through measuring or exploiting the system indirect effect rather than directly targeting the program [14]. The Cryptanalysis attacks is the third possible type where the attacker employs various methods to break the network cryptosystem. The last one is the data attack, where the attackers employ intelligent systems to obtain knowledge about the vulnerabilities of the system and the network. However, this type of attack may result in different types of serious attacks [14].

Blockchain and "Artificial Intelligence (AI)" are considered trending technologies that are adopted for both heavier and lightweight networks to achieve high end security. The blockchain, which was discover by Satoshi Nakamoto in 2008 [15] is a paradigm used for secure and decentralized storage for the data after suitable authentication and verification. Blockchain is considered highly secure and could not be easily hacked to achieve control through the transactions, the attacker should authenticate itself to all dynamic block within the chain and achieve legitimate hashes to all blocks [16]. ML and "Deep Learning (DL)" are emerging technologies that may be exploited in solving different security problems by leveraging their abilities to analyze data, detect patterns, and make predictions. It comes in to three major types, which are; supervised learning, unsupervised learning and 'Reinforcement Learning (RL)". Supervised learning methods works using labeled dataset, it is employed in IoT networks for spectrum detection, channel estimation, determining location and for adaptive filtration. Two major process are included in this type of learning, which are; classification and regression. Some of the common classification techniques are; "Naïve Bayes (NB)", "Decision Tree (DT)", "Support vector machine (SVM)", and "Random Forest (RF)". While logistic regression and polynomial regression are the two commonly adopted regression techniques. Unsupervised learning methods in turns cope with unlabeled data and the input data is heuristically used in learning the pattern of the input data. Hierarchal clustering and K-mean are two common examples for unsupervised learning [17]. Sybil and anomaly attacks of communication layer are usually detected using unsupervised learning techniques. RL in turns learn through discovering different actions in particular environment and then discover the optimal action sets so that the reward is being maximized. Q-learning is a common RL technique [17].

III. LITERATURE REVIEW

A lightweight encryption scheme was suggested and designed in [18], this model corresponds with the restricted and inadequate resources that IoT devices have including the memory and the power. This proposed scheme offers a high security level for the data transmitted between two IoT devices via continuously changing the key used for encrypting the IoT transmitted data. Furthermore, the robustness of the model is increased through using an enough large key so that it could not be broken by attackers. The experiments confirmed the effectiveness of the proposed lightweight model with encryption time of 170.7ms on average for 80bits key size, which is considered relatively large, with 7.7 PSNR in comparison with different algorithms. The continuous adoption for IoT services particularly in E-health applications will in turn increase the challenges of security, like the authentication for the exchanged data and different connected devices [4]. The authenticity aspect in e-health applications is considered one of the most essential challenges that should be effectively addressed. Consequently, a robustness authentication scheme is required for E-heath applications so that the data transfer and

exchange between the base station and the sensor nodes could be protected. They proposed a new lightweight, efficient and secure authentication system to be used for E-health applications within IoT environment to set up secure channels and authenticate the data exchanged between the sensor nodes and the base station [4]. The model characterizes with the group-based node feature and hence it reduces the consumed energy and distance, therefore has lower communication costs. It also robustness since it is capable of resisting the hackers through employing the "elliptic curve cryptography (ECC)" [4].

Authors in [19] stated that the gateway/sink is required to be trusted by IoT devices in order to provide a secure communication with the remainder of the network. Consequently, The IoT device requires a method for sink authentication and vice-versa. They proposed a new key exchange and lightweight authentication protocol for IoT devices in wireless environment. Two unique keys are assigned at the configuration time to each devices' pair, initial session key and master key. The session key is changed continuously and it is employed for data exchange throughout a particular session. This protocol is good to be used with disconnected IoT environment.

A trust-aware security scheme is proposed in [20] to be used by "digital applications (DApps)" in order to increase the privacy and the security in case of associating huge IoT services. Industrial data is generated by sensing units through a dedicated network in order to focus the structure of the application service. They used the blockchain as a part from the IoT system in order to improve the security of the network. Their proposed model improved the active users' number through delivering more packets and hence more mobility is achieved.

A new lightweight "Group Authentication Scheme (GAS)" was proposed in [21] in order to be used in authenticating the data of IoT devices in wireless media. This model offers 80% energy saving compared to the current solutions. It can also prevent man-in-the-middle and replay attacks types. It can be employed for both decentralized and centralized authentication scenarios.

Authors in [22] proposed a new protocol for secure communication and lightweight authentication for embedded and IoT devices. The main building block of this protocol is "Physically Unclonable Functions/ Random Number Generators (TRNGs/PUFs)". They aimed at illustrating the potentials of authentication and securing communication for the embedded system employing TRNG and PFU for generating keys deprived of the need to save the keys on the device itself. By this way, the key management problem on microcontrollers and hardware devices is simplified while secure communication is permitted.

Authors of [23] stated that there are different drawbacks for employing pre-defined keys and passwords in authenticating different IoT applications, such as smart office and smart hotel. Actually, they didn't offer short-term access within these reservation systems and hence adopting the password techniques for user's authentication is not reasonable. They presented a new authentication technique for IoT devices called "Token-Based Lightweight User Authentication (TBLU", which depends on a token method for the purpose of improving the authentication robustness. The security strength of the presented model was confirmed through security analysis in terms of "Perfect Forward Secrecy (PFS)" and token security. The performance analysis results also confirmed that this technique is strong competitor compared to current authentication techniques for IoT devices.

A new "Decentralized Lightweight Group Key Management architecture for Access Control in the IoT environment (DLGKM-AC)" was presented in [24]. According to a hierarchical structure that consists from one "Key Distribution Center (KDC)" and some "Sub Key KDCs(SKKDCs)", the presented model improves the subscribers' group management and reduces the KDC rekeying overhead. They also introduced a novel master token protocol that manages the dissemination of keys through a set of subscribers. By adopting this protocol, the storage, communication overhead throughout leave/join events and computation are being reduced. The scalable IoT architecture is accommodated through this presented approach. This in turn alleviates the single failure point through reducing the load results from rekeying process at the core network. Secure group communication is guaranteed in DLGKM-AC through guaranteeing backward/forward Secrecy and avoiding collusion attacks. The results of the conducted simulation confirmed the effectiveness of the proposed scheme with substantial resource gain in terms of communication, computation and storage overheads.

Authors in [25] stated that there are a lot of studies that have been recently conducted in the certificate-based authentication field. These schemes were not efficient in communication, storage and computation, which are extremely vital in IoT. In their work, they presented a new lightweight authentication technique depending on consortium blockchain besides designing a digital token that resembles cryptocurrency. They also manipulated the tokens' amount to perform the management of trust lifecycle. They performed a comprehensive evaluation and analysis to confirm the robustness of the proposed scheme against different types of attackers. They also confirmed that this scheme is efficient and competes the state-of-art schemes in terms of authentication, storage and communication costs.

Authors of [26] presented a new cross-domain authentication technique for IoT environment that based on identity called IRBA. Blockchain was used in this scheme as a decentralized anchor of trust rather than using the traditional authority certificate. Furthermore, the scheme adopted "identity-based self-authentication" method in place of the old-style "public key infrastructure (PKI)" authentication method. They implemented a prototype for their scheme and evaluated its effectiveness. Smart contracts are used in IRBA for implementing the process of authorization so that the authorization process credibility is guaranteed. The authorization results are saved in IRBA by using blockchain so that these results are authenticated. The results show that this scheme is efficient, has low computing overhead and good

processing performance.

Authors of [27] presented a new efficient mechanism called "blockchain-assisted secure device authentication mechanism (BASA)" to be applied and used with cross-domain industrial applications in IoT environment. Precisely, they introduced the consortium blockchain for the purpose of constructing the trust between different domains. They also utilized the "Identity-based signature (IBS)" throughout the authentication process. To protect the device privacy, they designed an identity management technique that could realize that the devices are still anonymous despite of being authenticated. The subsequent communications were secured through the negotiation on the session keys among two parties. They performed Extensive experiments to verify the efficiency and the effectiveness of the proposed scheme.

Authors of [28] discussed the disadvantages for old-style IoT in security protection and identity authentication and they proposed and implemented a new security and authentication model based on blockchain technology to be adopted in IoT environment. Hyperledger Fabric was used in implanting the system prototype and verify its effectiveness. A unique ID was assigned to each single device and then recorded within a blockchain in order to perform the authentication among each other deprived of central authority. Furthermore, they designed a data protection technique through hashing essential data within blockchain so that any data change could be immediately detected. The results confirmed the effectiveness of the proposed security mechanism.

Authors in [29] discussed the requirements for multi-domain authentication in IoT environment. The presented a cross-domain authentication technique besides a model for distributed joint authentication factors through employing the structure of double blockchain. They also presented the cross-chain technology within multi-domain IoT authentication process. They also designed a block data construction for the purpose of improving the access authentication function. They depend on the cross-chain technology besides the distributed consensus technique, the authentication process was realized using intelligent contract.

Authors of [30] discussed the importance of authentication protocols as the first line of defence against different types of attacks in "vehicular ad hoc networks (VANETs)". They stated that cryptography-based or public key infrastructure are usually employed in the traditional schemes. However, these methods have very high storage and computational costs. They depend on the consortium blockchain to propose a privacy-preserving authentication method for VANETs. The vehicle authenticity is represented through its capability of transaction on blockchain in place of cryptographic key certificate. A new data structure was designed depending on "unspent transaction output (UTXO)" together with a group of online operations including query, issue, revocation and transfer. Therefore, the authentication among two entities is performed through corresponding communication and on-chain verification. A set of privacy and security analysis were performed besides prototype implementation using Hyperledger Fabric platform in order to estimate the efficiency and the effectiveness of the proposed system.

Authors of [31] presented a privacy-aware authentication technique to be used for multi-server 'Cloud-Edge IoT(CE-IoT" schemes. The proposed scheme combined the blockchain and Physical Unclonable Functions (PUFs) techniques. The" challenge-response pairs (CRPs)" CRPs real correlations were double-encoded to "mapping correlations (MCs)" through keyed-hash and one-time physical identity function. They took the benefit of the blockchain in storing the MCs, efficiently synchronizing them and join the multi-receiver encryption so the physical identity is being shared securely. They used a random oracle model to prove the security of their model and verified its ability in resisting different attacks. They also implemented a prototype for their proposed protocol and verified that CE-IoT systems could be accommodated by this protocol.

Authors of [32] stated that the current decentralized protocols require power and computing resources more than the ability of IoT devices. Therefore, distributed consensus platform could not be fully adopted in IoT setting. They presented an implementation of lightweight "proof-of-work (PoW)" mining besides the reconfigurable hardware alternatives. Through replacing the cryptographic and hash functions in the conventional blockchain protocol with efficient and secure hardware implementations, the proposed scheme could considerably reduce the power and hardware resources overheads for PoW mining. They also presented an anti-spoofing solution to be used for GPS navigation between IoT devices. The proposed protocol utilized PUFs besides "configurable nonlinear feedback shift register (CNLFSR)" and substitute "secure hash algorithm (SHA-256)" and "elliptic curve digital signature algorithm (ECDSA)" in blockchain-PoW mining. the presented 'PUF-CNLFSR-Blockchain (PCBChain)" attained a similar functionality to that of blockchain-PoW mining with low power consumption and hardware costs. The proposed scheme achieved 97% resource saving and (50×) performance boost compared to the conventional blockchain.

According to [33], the secure authentication of IoT devices among adversaries that have much higher computational capability and power still form a challenge even for wireless security and cryptographic protocols. They proposed a new classifier based on deep learning that could learn the hardware imperfections for radios of low power that could not be easily emulated also for adversaries of very high power. They constructed a "Long Short Term Memory (LSTM)" framework particularly sensitive to signal imperfections that last through long durations. This framework utilized the deep "Neural Network (NN)" in learning the imperfections of wireless hardware. the LSTM classifier utilized the temporal correlation among wireless signal I/Q streams for the purpose of identifying the transmitters with low-power among adversaries of high power regardless of the transmitted data. They used 30 low-power nodes to test and evaluate the performance of their framework and they confirmed its effectiveness in resisting progressive software attackers.

IV. COMPARISON

Table 1 below summarized the presented researches and studies in the previous section. The comparison is perfumed according to the used application, contribution, used algorithms and technologies, benefits and finally the results. By comparing research studies based on these criteria, readers can make informed decisions about which studies are most relevant to their interests, which ones offer the most promising solutions, and which ones have demonstrated concrete results and benefits within the context of IoT authentication.

Table 1. Summary of Presented Researches

Study	Contribution	Used algorithms, technologies, simulators	Results
[4]	A new efficient and lightweight authentication scheme for E-health applications in IoT environment. Secure channels are established and authenticated between sensor nodes and base station.	ECC Authenticated Key Agreement (AKA) protocol. Group Node concept. Contiki simulator used in evaluation. Different scenarios were considered including mobility and non-mobility, without and with GN.	Reduced distance Reduced costs of communication Lower consumed energy Resists different attacks types Protection of data use, transfer and exchange among sensor nodes and base station. Improve network usage.
[18]	A new lightweight encryption algorithm that fulfill with the restricted IoT devices resources. A large enough, strong and continuously changed key is used to prevent attackers from breaking this key.	Lightweight and robustness encryption and decryption algorithms.	Less memory space and processing time compared to other methods. High security level for the transmitted data. Saves the processor time and memory space and consumes less power. High security level Very fast cryptography algorithm
[19]	Presenting a new protocol for the purposes of providing lightweight, secure, space and energy efficient key exchange and authentication for IoT devices in wireless media without using TTP.	HMAC based HKDF symmetric-key cryptography	Efficient protocol in terms of required computation, energy usage and memory. Lightweight, efficient and secure. Doesn't need any "Trusted Third Party (TTP)" The keys are secret and do not exchanged explicitly over the network. Works also when gateway and IoT device are disconnected from the remainder of the network.
[20]	A new authentication and privacy preserving system was proposed MAC verification and hash evaluation were used.	Blockchain MAC verification. Python and Raspberry Pi for simulation.	Reduced communication and processing expenses. Delivery ratio, security and privacy issues could be addressed. Seamless authentication and trust-awareness protocol.
[21]	A lightweight authentication scheme for key agreement and authentication in sensing layer was proposed. The protocol depends on GAS in combating the problems of scalability that occur in case of increasing the components number within IoT network.	Omnet++ simulator GAS	Can attack both man-in-the-middle and replay attacks. 80% energy saving. Improved energy efficiency Many-many authentication solutions.
[22]	A new protocol is proposed for secure communication and lightweight authentication within IoT devices. Single circuit was proposed to be employed in key generation using TRNG and PUF as the main building block. The secrets are not required to be stored on the device itself and hence the key management problem is simplified.	TRNGs / PUFs	Simplifying the key management problem. Secure communication is achieved. Secure communication Lightweight authentication.
[23]	Lightweight authentication scheme is proposed to be used for IoT devices. Depends on a token technique rather than using password-based mechanisms.	Symmetric cryptography.	Efficient and lightweight solution. Mutual authentication is confirmed among communication parties. Reduced computation overhead. Energy of authenticating devices is saved.
[24]	A novel lightweight decentralized architecture for distributing keys. A new master token management algorithm.	GKM	DLGKM-AC is effective in terms of improved security, reduced overhead and increased scalability. The scheme reduces the KDC rekeying overhead. Improves the subscribers' group management. Security requirements were ensured. Robustness enough to resists the collusion attack.

			Computational, communication and storage overheads were minimized.
[25]	A lightweight authentication technique. The LiIDCoin is utilized in representing the identity trust of IoT device.	Consortium Blockchain Lightweight IDentity Coin HyperLedger Fabric platform	Reduces the costs of storage, computation and communication. Reduces the efforts of lifecycle management. Cryptocurrency-like scheme.
[26]	"Identity, Recognize, Blockchain, and Algorithm (IRBA)" was proposed.	identity-based self-authentication method. Blockchain.	The authorization process credibility is guaranteed. Decentralized storage for the results of access authorization is achieved. Low computing overhead. Good processing performance. Suitable for different IoT scenarios.
[27]	BASA mechanism was proposed and evaluated. Identity management technique was proposed. Key agreement technique was also proposed.	Blockchain IBS	The efficiency and security of BASA was confirmed through evaluation. Flexible design for identity management technique. Entities from diverse administrative domains could authenticate each other deprived of knowing the actual identity.
[28]	A blockchain-based scheme was proposed for security protection and identity authentication. Hyperledger Fabric was used in implementing the system prototype.	Blockchain Raspberry Pi Hyperledger Fabric platform. "Practical Byzantine fault tolerance (PBFT)".	Further security protection is provided by the proposed scheme between diverse trust domains. Generic nature. Simplicity. Low costs of implementation.
[29]	The traditional PBFT consensus technique is improved using identity-based secret-sharing method so that group authentication is achieved for access requests.	PBFT Private key and public key encryption. Blockchain technology.	The single failure problem is reduced. The overload is decreased. good system stability and high security. Can be deployed directly within current systems. Well-matched with local systems.
[30]	Consortium blockchain was applied to the VANETs authentication service. The authenticity of the trusted authority could be improved through launching a transaction. A novel data structure was designed together with techniques based on UTXO.	VANETs Blockchain Hyperledger Fabric platform. UTXO	The proposed scheme is efficient and secure. Certificate is not required to verify the authenticity of the trusted authority.
[31]	a privacy-aware authentication technique was proposed to be used for multi-server CE-IoT schemes. The proposed scheme combined the blockchain and PUFs techniques.	CE paradigm Blockchain PUFs multi-receiver encryption hash function.	The adversary break probability for this protocol is very small. Key security properties are provided. The protocol resists different passive and active attacks. Suitable for multi-server environment. Single point failure problem was solved. The protocol is scalable and efficient. CE-IoT systems were accommodated.
[32]	the CNLFSR and PUF solution is developed to build novel hardware-based cryptographic alternatives and permit resource-efficient mining and authentication considering reconfigurable levels of security. GPS spoofing and PCBChain solutions were implemented practically.	Blockchain PUFs CNLFSR GPS spoofing	97% resource saving and (50×) performance boost compared to the conventional blockchain. An improved security level. low power consumption and hardware costs.
[33]	● A classifier that based on deep learning is presented. ● LSTM framework is constructed.	● Machine Learning. ● NNs.	● LSTM is effective in resisting progressive software attackers. ● Good resistance to multipath and adversaries of high power

V. Conclusion

IoT resulted in a revolution on different systems and the way of interaction between the human and communication and computing systems. Achieving secure and efficient authentication for IoT devices is on a great deal of importance. Blockchain and AI are considered trending technologies that are adopted for both heavier and lightweight networks to achieve high end security. In this survey paper, we presented some of the studies conducted in the literature with topics related to lightweight authentication of IoT devices through using different emerging technologies like, ML, DL and blockchain. The paper presented an extensive comparison between these studies in terms of different criteria. The security issues in IoT environment are also discussed besides the different types of attacks that may face the network.

Acknowledgement

The authors would like to thank the Department of Computer Science and Department of Cyber Security in the College of Computer Science and Mathematics at the University of Mosul for their help in completing this paper.

References

[1] Chanal, P. M., & Kakkasageri, M. S. "Security and privacy in IOT: a survey." Wireless Personal Communications, Vol. 115, No.2, pp. 1667-1693, 2020

[2] Tournier, J., Lesueur, F., Le Mouël, F., Guyon, L., & Ben-Hassine, H. "A survey of IoT protocols and their security issues through the lens of a generic IoT stack." Internet of Things, Vol .16, pp. 100264.,2001.

[3] Palanivelu, R., & Srinivasan, P. S. S. "Safety and security measurement in industrial environment based on smart IOT technology based augmented data recognizing scheme." Computer communications, Vol.150, pp. 777-787,2020

[4] Almulhim, M., Islam, N., & Zaman, N. "A lightweight and secure authentication scheme for IoT based e-health applications." International Journal of Computer Science and Network Security, Vol. 19, No. 1, pp. 107-120,2019.

[5] Wazid, M., Das, A. K., Shetty, S., JPC Rodrigues, J., & Park, Y. "LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment." Sensors, Vol. 19, No. 24, pp. 5539, 2019.

[6] Karthikeyan, B., Sasikala, T., & Priya, S. B. "Key exchange techniques based on secured energy efficiency in mobile cloud computing", Applied Mathematics & Information Sciences, Vol. 13, No. 6, pp. 1039-1045,2019.

[7] Ambeth Kumar, V. D., Malathi, S., Kumar, A., & Veluvolu, K. C. "Active volume control in smart phones based on user activity and ambient noise." Sensors, Vol. 20, No. 15, pp. 4117, 2020.

[8] Li, C., & Yang, C. "(WIP) authenticated key management protocols for internet of things." In 2018 IEEE International Congress on Internet of Things (ICIOT), pp. 126-129, 2018.

[9] Neelakandan, S., & Anand, J. G. "Trust based optimal routing in MANET's." In 2011 International Conference on Emerging Trends in Electrical and Computer Technology, pp. 1150-1156,2011.

[10] Subbulakshmi, P., & Prakash, M. "Mitigating eavesdropping by using fuzzy based MDPOP-Q learning approach and multilevel Stackelberg game theoretic approach in wireless CRN." Cognitive Systems Research, Vol. 52, pp. 853-861, 2018.

[11] Patel, C., & Doshi, N. "Cryptanalysis of ecc-based key agreement scheme for generic IoT network model." In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-7,2019.

[12] Mohan, P., & Chelliah, S."An authentication technique for accessing de-duplicated data from private cloud using one time password." In Cloud Security: Concepts, Methodologies, Tools, and Applications, pp. 435-445,2019.

[13] Ambili, K. N., & Jose, J. "A secure software defined networking based framework for IoT networks." Cryptology ePrint Archive.

[14] Attkan, A., & Ranga, V. (2022). "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security." Complex & Intelligent Systems, pp. 1-33,2020.

[15] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, pp. 21260.,2008.

[16] Bach, L. M., Mihaljevic, B., & Zagar, M. "Comparative analysis of blockchain consensus algorithms." In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO),pp. 1545-1550. 2018.

[17] Istiaque Ahmed, K., Tahir, M., Hadi Habaebi, M., Lun Lau, S., & Ahad, A. "Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction." Sensors, Vol. 21, No. 15, pp. 5122.,2021.

[18] Abbas Fadhil Al-Husainy, M., & Al-Shargabi, B. "Secure and lightweight encryption model for IoT surveillance camera." International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, No. 2, 1840-1847.,2020.

[19] Rabiah, A. B., Ramakrishnan, K. K., Liri, E., & Kar, K. "A lightweight authentication and key exchange protocol for IoT." In Workshop on Decentralized IoT Security and Standards, Vol. 2018, pp. 1-6., 2018.

[20] Ali, A., Noya, I. D., Rehman, A. U., Ahmed, M., Singh, A., & Anand, D. "A Lightweight Trust-less Authentication Framework for Massive IoT Systems." Creative Commons CC BY license, 2022.

[21] Aydin, Y., Kurt, G. K., Ozdemir, E., & Yanikomeroglu, H. "A flexible and lightweight group authentication scheme." IEEE internet of things Journal, Vol .7, No. 10, pp. 10277-10287, 2020.

[22] Buchovecká, S., Lórencz, R., Bucek, J., & Kodýtek, F. "Lightweight Authentication and Secure Communication Suitable for IoT Devices", In ICISSP, pp. 75-83.,2022.

[23] Dammak, M., Boudia, O. R. M., Messous, M. A., Senouci, S. M., & Gransart, C.. "Token-based lightweight authentication to secure IoT networks." In 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-4, 2019, January.

[24] Dammak, M., Senouci, S. M., Messous, M. A., Elhdhili, M. H., & Gransart, C. "Decentralized lightweight group key management for dynamic access control in IoT environments." IEEE Transactions on Network and Service Management, Vol. 17, No. 3, pp. 1742-1757.2020.

[25] Zhang, Y., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. "A Lightweight Authentication Scheme Based on Consortium Blockchain for Cross-Domain IoT." Security and Communication Networks, 2022.

[26] Jia, X., Hu, N., Su, S., Yin, S., Zhao, Y., Cheng, X., & Zhang, C. "IRBA: an identity-based cross-domain authentication scheme for the internet of things." Electronics, Vol. 9, No. 4, pp. 634,2020.

[27] Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. " Blockchain-assisted secure device authentication for cross-domain industrial IoT." IEEE Journal on Selected Areas in Communications, Vol. 38, No. 5, pp. 942-954,2020.

[28] Li, D., Peng, W., Deng, W., & Gai, F. (2018, July). " A blockchain-based authentication and security mechanism for IoT." In 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1-6.

[29] Li, D., Yu, J., Gao, X., & Al-Nabhan, N. "Research on multidomain authentication of IoT based on cross-chain technology." Security and Communication Networks, 2020.

[30] Zhang, Y., Tong, F., Xu, Y., Tao, J., & Cheng, G. "A privacy-preserving authentication scheme for VANETs based on consortium

blockchain." In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), pp. 1-6, 2020.

[31] Zhang, Y., Li, B., Liu, B., Hu, Y., & Zheng, H. "A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain." IEEE Internet of Things Journal, Vol. 8, No. 18, pp. 13958-13974,2021.

[32] Yan, W., Zhang, N., Njilla, L. L., & Zhang, X. "Pcbchain: Lightweight reconfigurable blockchain primitives for secure iot applications." IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 28, No. 10, pp. 2196-220, 2020.

[33] Das, R., Gadre, A., Zhang, S., Kumar, S., & Moura, J. M. "A deep learning approach to IoT authentication." In 2018 IEEE International Conference on Communications (ICC), pp. 1-6, 2018.

مصادقة خفيفة الوزن للأجهزة في بيئة انترنت الاشياء: دراسة استقصائية

سميرة عباس فاضل احمد سامي نوري
كلية علوم الحاسوب والرياضيات / جامعة الموصل
ahmed.s.nori@uomosul.edu.iq sameeraabbasfadhel@uomosul.edu.iq

تاريخ لاستلام:17/4/2023 تاريخ القبول: 25/9/2023

الملخص

إنترنت الأشياء (IoT) "هي تقنية رئيسية وناشئة حيث ترتبط الأجهزة المختلفة معًا للعمل بذكاء دون تدخل الإنسان. لإنترنت الأشياء تأثير كبير على حياتنا الاقتصادية والاجتماعية والتجارية. العدد الكبير جدا من الأجهزة المرتبطة معًا عن طريق البروتوكولات المختلفة تجعلها عرضة للتهديد من قبل عدة أنواع من الهجمات. ومع ذلك، لا يمكن تحسين أمان أجهزة إنترنت الأشياء نظرًا لمواردها المحدودة وقوتها الحسابية المحدودة ايضا. وبالتالي، لا تزال هناك حاجة ملحة لبناء وتطوير أنظمة مصادقة خفيفة الوزن لأجهزة إنترنت الأشياء لتحقيق أمان أفضل لشبكات إنترنت الأشياء. Blockchain و "التعلم الآلي (ML)" هما من التقنيات الناشئة التي يمكن استغلالها في حل مشكلات الأمان المختلفة. في هذا البحث يتم عرض ومراجعة بعضًا من أحدث بروتوكولات المصادقة خفيفة الوزن المقترحة والمخططات التي سيتم تطبيقها واعتمادها لبيئة إنترنت الأشياء، كما تم مناقشة قضايا الأمان في بيئة إنترنت الأشياء إلى جانب أنواع الهجمات المختلفة التي قد تواجه الشبكة. كما تضمن البحث مقارنة بين الأعمال والدراسات المختارة من حيث المعايير المختلفة بما في ذلك المحاسن والنتائج والتطبيقات المستخدمة، كذلك التقنيات أو الطرق المستخدمة.

الكلمات المفتاحية: انترنت الأشياء، التعلم الالي، الأمنية، مصادقة خفيفة الوزن، تطبيقات انترنت الأشياء.