Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
1	Sarah Dill	Proximity based IoT device authentication	Approved	Jiansong Zhang, Zeyu Wang, Zhice Yang, Qian Zhang	IoT, Move2Auth, RSS, proximity, authentication	Internet of Things (IoT) devices are largely embedded devices which lack a sophisticated user interface, e.g., touch screen, keyboard, etc. As a consequence, traditional Pre-Shared Key (PSK) based authentication for mobile devices becomes difficult to apply. For example, according to our study on home automation devices which leverage smartphone for PSK input, the current process does not protect against active impersonating attack and also leaks the Wi-Fi password to eavesdroppers, i.e., currently these IoT devices can be exploited to enter into critical infrastructures, e.g., home networks. Motivated by this real-world security vulnerability, in this paper we propose a novel proximity-based mechanism for IoT device authentication, called Move2Auth, for the purpose of enhancing IoT device security. In Move2Auth, we require user to hold smartphone and perform one of two hand-gestures (moving towards and away, and rotating) in front of IoT device. By combining (1) large RSS-variation and (2) matching between RSS-trace and smartphone sensor-trace, Move2Auth can reliably detect proximity and authenticate IoT device accordingly. Based on our implementation on Samsung Galaxy smartphone and commodity Wi-Fi adapter, we prove Move2Auth can protect against powerful active attack, i.e., the false-positive rate is consistently lower than 0.5%.	IEEE INFOCOM 2017 - IEEE Conference on Computer Communications	A*	2017	There is a big issue regarding authentication of IoT devices. The goal was to create a method of authentication that would work for IoT devices while still maintaining properties of widely used and accepted authentication techniques.	N/A	The paper proposes "a proximity based mechanism for smpartphone to authenticate IoT devices, called Move2Auth". Through this solution, users perform a hand gesture generated by the smartphone in order to authenticate.	The solution was implemented on a Samsung Galaxy smartphone, and 5 users were asked to test the solution.	J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity based IoT device authentication," IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1-9, doi: 10.1109/INFOCOM.2017.8057145.	@INPROCEEDINGS{8057145, author={Zhang, Jiansong and Wang, Zeyu and Yang, Zhice and Zhang, Qian}, booktitle={IEEE INFOCOM 2017 - IEEE Conference on Computer Communications}, title={Proximity based IoT device authentication}, year={2017}, volume={}, number={}, pages={1-9}, doi={10.1109/INFOCOM.2017.8057145}}	https://drive.google.com/file/d/1X6Dpm1ZoRmy8Ay5asmaviGRtRWj6rLlf/view?usp=sharing	This paper details a method of proximity based authentication, which can be further researched in other papers and is highly relevant to the topic.
	Edwin Liu	PIANO: Proximity-Based User Authenticaiton on Voice-Powered Internet-of-Things Devices	Approved	Neil Zhenqiang Gong, Altay Ozen, Yu Wu, Xiayu Cao, Richard Shin, Dawn Song, Hongxia Jin, Xuan Bao	IoT, authentication, proximity, Voice-Power devices	Voice is envisioned to be a popular way for humans to interact with Internet-of-Things (IoT) devices. We propose a proximity-based user authentication method (called PIANO) for access control on such voice-powered IoT devices. PIANO leverages the built-in speaker, microphone, and Bluetooth that voice-powered IoT devices often already have. Specifically, we assume that a user carries a personal voice-powered device (e.g., smartphone, smartwatch, or smartglass), which serves as the user's identity. When another voice-powered IoT device of the user requires authentication, PIANO estimates the distance between the two devices by playing and detecting certain acoustic signals; PIANO grants access if the estimated distance is no larger than a user-selected threshold. We implemented a proof-of-concept prototype of PIANO. Through theoretical and empirical evaluations, we find that PIANO is secure, reliable, personalizable, and efficient.	2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)	A*	2017	An attacker can compromise a user's security and privacy via unauthorized physical access to the user's IoT devices. Specifically, many IoT devices store various private information of the devices' owners. The goal s to implement an authentication method that is secure, reliable, personalizable, zero-interaction, and efficient.	Distance Estimation protocols. Determining proximity using Ambient signals.	The goal s to implement PIANO (proximity-based user authentication method) on IoT devices as it has several promising features: secure, reliable, personalizable, zero-interaction, and efficient.	The protocol needs an authenticating device and a vouching device. It follows these steps: 1) The auth device constructs 2 snippets of acoustic signals (A and V) - "reference signals" 2) The auth device transmits the 2 signals to vouching device via bluetooth - is secure so attacks cannot eavesdrop 3) Both devices record acoustic signals using a microphone. Auth device plays A, vouching device plays V. 4) Both devices detect when the 2 signals are recorded and denote the timestamps for the 2 (AA and VV). 5) The vouching device transmits the time difference to auth device using bluetooth 6) The auth device calculates the distance.	N. Z. Gong et al., "PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2212-2219, doi: 10.1109/ICDCS.2017.68.	@INPROCEEDINGS{7980172, author={Gong, Neil Zhenqiang and Ozen, Altay and Wu, Yu and Cao, Xiaoyu and Shin, Richard and Song, Dawn and Jin, Hongxia and Bao, Xuan}, booktitle={2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)}, title={PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices}, year={2017}, volume={}, number={}, pages={2212-2219}, doi={10.1109/ICDCS.2017.68}}	https://ieeexplore.ieee.org/abstract/document/7980172/authors#authors	This paper details a method of proximity based authentication, which can be further researched in other papers and is highly relevant to the topic.
	Alison Nakai-Lackey	Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices	Approved	Prosanta Gope, Biplab Sikdar	Authentication, Servers, Internet of Things, Protocols, Cryptography, Integrated circuits	Device authentication is an essential security feature for Internet of Things (IoT). Many IoT devices are deployed in the open and public places, which makes them vulnerable to physical and cloning attacks. Therefore, any authentication protocol designed for IoT devices should be robust even in cases when an IoT device is captured by an adversary. Moreover, many of the IoT devices have limited storage and computational capabilities. Hence, it is desirable that the security solutions for IoT devices should be computationally efficient. To address all these requirements, in this paper, we present a lightweight and privacy-preserving two-factor authentication scheme for IoT devices, where physically uncloneable functions have been considered as one of the authentication factors. Security and performance analysis show that our proposed scheme is not only robust against several attacks, but also very efficient in terms of computational efficiently.	IEEE Internet of Things Journal (Volume: 6, Issue: 1, February 2019)	Not explicitly found in list for "IEEE", IEEE journals generally have a A* - B score.	2018	In this section, we present a practical anonymous authentication scheme, which consists of two phases: 1) setup and 2) authentication. The operations of the setup phase are carried out over a secure channel.	Fuzzy Extractor, Physically Uncloneable Function, System Model	To provide two-factor authentication to IoT devices, in addition to a password or a shared secret key as the first authentication factor, this paper proposes the use of physically uncloneable functions (PUFs) as the second authentication factor.	The proposed solution has no outline for actual implementation, rather, it exists as a series of theorems and proofs surrounding their concept.	P. Gope and B. Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 1, pp. 580-589, Feb. 2019, doi: 10.1109/JIOT.2018.2846299.	@ARTICLE{8382158, author={Gope, Prosanta and Sikdar, Biplab}, journal={IEEE Internet of Things Journal}, title={Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices}, year={2019}, volume={6}, number={1}, pages={580-589}, doi={10.1109/JIOT.2018.2846299}}	https://ieeexplore.ieee.org/abstract/document/8382158/keywords#keywords	This paper explores a novel IoT MFA technique, which may be used in exploring existing MFA techniques and/or as a comparison to existing techniques.
	Andrea Pallotta	A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication	Approved	Peng Hao, Xianbin Wang, Weiming Shen	Authentication, Cryptography, Collaboration, Radio frequency, Communication system security, Wireless communication	Nowadays, Internet of Things (IoT) devices are rapidly proliferating to support a vast number of end-to-end (E2E) services and applications, which require reliable device authentication for E2E data security. However, most low-cost IoT end devices with limited computing resources have difficulties in executing the increasingly complicated cryptographic security protocols, resulting in increased vulnerability of the virtual authentication credentials to malicious cryptanalysis. An attacker possessing compromised credentials could be deemed legitimate by the conventional cryptography-based authentication. Although inherently robust to upper-layer unauthorized cryptanalysis, the device-to-device physical-layer (PHY) authentication is practically difficult to be applied to the E2E IoT scenario and to be integrated with the existing, well-established cryptography primitives without any conflict. This paper proposes an enhanced E2E IoT device authentication that achieves seamless integration of PHY security into traditional asymmetric cryptography-based authentication schemes. Exploiting the collaboration of several intermediate nodes (e.g., edge gateway, access point, and full-function device), multiple radio-frequency features of an IoT device can be estimated, quantized, and used in the proposed PHY identity-based cryptography for key protection. A closed-form expression of the generated PHY entropy is derived for measuring the security enhancement. The evaluation results of our cross-layer authentication demonstrate an elevated resistance to various computation-based impersonation attacks. Furthermore, the proposed method does not impose any extra implementation overhead on resource-constrained IoT devices.	IEEE Access (Volume: 6)	Not present on portal. IEEE-published journals usually have a A*-B score	2018	The current implementation of Device-to-Device PHY authentication is difficult to integrate with pre-existing cryptography primitives and to scale to E2E systems due to how complicated IoT cryptographic protocols are. The Elliptic Curve Cryptography (ECC)-based authentication methods, one of the recently suggested solutions, aims to solve the computational overhead by shortening the encryption key length. However, exhaustive search approaches, which constantly shorten in execution time due to the rapidly growing processing power of attackers, can compromise the cryptographic credentials of IoT devices with limited resources available.	D2D PHY authentication and characteristics, Elliptic Curve Cryptography, E2E Service Model (Nodes), MAMO	The proposed PHY-aided authentication scheme aims to integrate D2D PHY fingerprints with asymmetric E2E IoT-device authentications, enhance security with a closed-form expression for the PHY entropy, and resist computational-based authentication attacks without imposing additional computational overhead on IoT devices with limited resources.	The proposed authentication method can applies to any typical E2E IoT system, where two ends are a source node (e.g. IoT devices) and a destination node (e.g. Internet host). The paper discusses the proposed solution through a series of algorithms, mathematical proofs, and simulations.	P. Hao, X. Wang and W. Shen, "A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication," in IEEE Access, vol. 6, pp. 42279-42293, 2018, doi: 10.1109/ACCESS.2018.2859781.	@ARTICLE{8419693, author={Hao, Peng and Wang, Xianbin and Shen, Weiming}, journal={IEEE Access}, title={A Collaborative PHY-Aided Technique for End-to-End IoT Device Authentication}, year={2018}, volume={6}, number={}, pages={42279-42293}, doi={10.1109/ACCESS.2018.2859781}}	https://ieeexplore.ieee.org/document/8419693	This paper explains the current issues with implementing PHY-based authentication in E2E IoT services and proposes an alternative authentication technique, relavant to the research topic.
	Niklas Bernardo Correa	MTRA: Multiple-Tier Remote Attestation in IoT Networks	Approved	Hailun Tan, Gene Tsudik, Sanjay Jha	Multiple-Tier Remote Attestation, program integrity verification, IoT	Large numbers of Internet of Things (IoT) devices are increasingly deployed in many aspects of modern life.Given their limited resources and computational power, verifying program integrity in such devices is a challenging issue. In this paper, we design MTRA, a Multiple-Tier Remote Attestation protocol, by exploiting differences in resources and computational power among various types of networked IoT devices.More powerful devices equipped with a Trusted Platform Module (TPM) are verified through trusted hardware while others are verified through software-based attestation.MTRA is a flexible means of program integrity verification for heterogeneous IoT devices.	2017 IEEE Conference on Communications and Network Security (CNS)	Not found on conference portal. IEEE seems to have A*-B score mostly	2017	There are two stages for the proposed attestation protocol: • Offline (preparation stage), when none of the devices have been deployed for operations and related additional hardware (i.e., TPMs) is initialized and installed on the computationally powerful devices. As no network has not been established, no adversary can launch an attack. • Online (operative stage), when all devices have been deployed and are operational. The remote attestations are performed and an adversary can launch attacks.	We assume that an IoT network contains three types of device. The first is a trusted third party that issues attestation challenges to the rest of the network (i.e., base-station). The device, directly controlled by the network administrator, has unlimited computational power and cannot be compromised by an adversary. There is only one such device in a network. The second type of device could accommodate tamper-proof hardware (e.g., TPM) but is vulnerable to some forms of network attacks. The third type has limited resources and lacks tamper-proof hardware	Our contributions are: • A new two-tier attestation protocol for heterogeneous IoT networks: In prior work [6], [8], [15], [16], [19], protocols were not designed in the context of heterogeneous IoT networks. • Countermeasures against rainbow and interference attacks: In the challenge-response attestation protocol, the adversary attempts to send an arbitrary challenge to probe the response from the prover, which can be exploited for the Time-Of-Use to Time-Of-Check (TOUTTOC) attack without manipulating the prover's firmware. This is rainbow attack. In addition, an adversary can interfere with the challenge-response attestation protocol as a Man-In-The-Middle [17]. To the best of our knowledge, we are the first to adopt a one-way hash chain to defend against rainbow attacks. Each hash key is updated after the challenge is successfully completed. Therefore, the hash key used for one challenge is different from the key for the next challenge. This is further analyzed in Section V.• Defense against wormhole attacks: The wormhole attack is a notorious network attack that can allow an adversary to retrieve information earlier than expected for other types of attack [12]. In our approach, a local one-way hash chain is proposed to invalidate the efforts of wormhole attacks. Section V-B details how our approach can defend against it. To the best of our knowledge, we are the first to defend against wormhole attacks in remote attestation. • New approach to detect Time-Of-Check-To-Time-Of-Use (TOCTTOU) attacks: An adversary might have the correct firmware to respond to attestation challenges and have malware running in another period in a TOCTTOU attack. We deploy an online-offline notification mechanism to defend against TOCTTOU attacks in Section V-C.	The paper proposes 3 different algorithms to be used in different stages. These are written in pseudo-code in page 4.	Tan, H., Tsudik, G., &amp; Jha, S. (2017). MTRA: Multiple-Tier Remote Attestation in IoT Networks. 2017 IEEE Conference on Communications and Network Security (CNS).	@article{tan_tsudik_jha_2017, title={IEEE CNS 2017 SPA: 2017 IEEE Conference on Communications and Network Security (CNS): SPA — program}, DOI={10.1109/cns.2017.8228614}, journal={2017 IEEE Conference on Communications and Network Security (CNS)}, author={Tan, Hailun and Tsudik, Gene and Jha, Sanjay}, year={2017}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8228638	This paper was somewhat tangential to the topic at hand. However, it provided insight into hardware based techniques for verifying IoT devices as well as software based when the device is not powerful enough to mae use of a TPM.
	Sarah Dill	Noisy Vibrational Pairing of IoT Devices	Good, Approved	S Abhishek Anand, Nitesh Saxena	IoT, Authentication, vibrations, IoT pairing	Internet of Things (IoT) is embodied by smart network-enabled devices that utilize computing power, networking, and miniaturization to enable richer and improved user experience. Due to their interconnectedness, ubiquitous nature and low computational power, trustworthy and secure communication between IoT devices has become a security concern. To authenticate the devices, “pairing” may be secured by the use of an auxiliary channel such as audio, visual and vibrations for sharing the key or keying material between the IoT devices. In this paper, we evaluate the security of vibration channel, susceptible to an acoustic eavesdropper, that can capture audio leakage from the vibrations of the transmitting IoT device. We propose a noisy vibration scheme for cloaking vibration sounds during pairing against such attacks. The scheme only requires a speaker for emitting the masking sound during key transmission. We evaluate the scheme in proximity, co-located and remote settings with an eavesdropping attacker. We also study motion sensor exploits against this scheme and compliment it with additional measures to mask vibration effects on motion sensors. Our scheme is user transparent and requires only a speaker (that may already be present on the device), so it can be readily implemented in the IoT setting, smart wearables, and other commodity gadgets.	IEEE Transactions on Dependable and Secure Computing	A	2019	Common IoT pairing protocols that use audio have been proved to be susceptible to eavesdropping by a dedicated adversary. The goal of this research was to find a secure way to use audio signals for pairing devices.	N/A	The paper proposed a secure "noisy" vibrational pairing scheme to use with common IoT devices.	The authors test their solution against eavesdropping and suggest different methods to prevent these attacks from being successful (e.g. adding low frequency tones to mask the signal).	S. A. Anand and N. Saxena, "Noisy Vibrational Pairing of IoT Devices," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 3, pp. 530-545, 1 May-June 2019, doi: 10.1109/TDSC.2018.2873372.	@ARTICLE{8478315, author={Anand, S Abhishek and Saxena, Nitesh}, journal={IEEE Transactions on Dependable and Secure Computing}, title={Noisy Vibrational Pairing of IoT Devices}, year={2019}, volume={16}, number={3}, pages={530-545}, doi={10.1109/TDSC.2018.2873372}}	https://drive.google.com/file/d/1uL6XThQfcvF44dwprYMupq4qpDj_7LI8/view?usp=sharing	The paper presents a possible secure solution to the IoT pairing issue. While more research would need to be done to test this solution, it is a step in the right direction and provides insight to other methods besides the commonly used and insecure methods that are often used today (WiFi, Bluetooth, RFID, etc.)
	Edwin Liu	PUF based IoT Device Authentication Scheme https://ieeexplore.ieee.org/abstract/document/8939751	Approved	Byoungkoo Kim; Seoungyong Yoon; Yousung Kang; Dooho Choi	IoT, Authentcation, PUF, more secure device authentication	This paper propose a PUF(Physical Unclonable Function)-based IoT(Internet of Things) device authentication scheme to minimize the risk of authentication key exposure and the load of authentication server. The proposed technique can be realized by storing and updating only a single CRP(Challenge-Response Pair) through interaction with the device to be authenticated, unlike the existing technique of storing all the CRPs that can be generated by the PUF technology in the authentication server. In addition, it enables more secure device authentication through authentication message encryption by using the secret key generated from the CRP	2019 International Conference on Information and Communication Technology Convergence (ICTC)		2019	Most IoT devices are operated with software-based security technologies. This means the security system can easily be hacked into. Sensitive things that could be leaked woud be the device's secret key for authentication and encryption.This allows the hacker to pair and access the person's IoT device and take control of it. This is a huge privacy issue and could put the user at risk.	N/A	The paper proposed a new technology called "PUF" that helps the IoT device have unique characteristics and a lowere chance of gettign hacked into.	The authors test their solution by applying the PUF technique to IoT devices. PUF store and updates only a single CRP through interaction between the authentication server and the device. Since the secret key generated based on the CRP is used for message encryption, more secure device authentication can be assured.	B. Kim, S. Yoon, Y. Kang and D. Choi, "PUF based IoT Device Authentication Scheme," 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 1460-1462, doi: 10.1109/ICTC46691.2019.8939751.	@INPROCEEDINGS{8939751, author={Kim, Byoungkoo and Yoon, Seoungyong and Kang, Yousung and Choi, Dooho}, booktitle={2019 International Conference on Information and Communication Technology Convergence (ICTC)}, title={PUF based IoT Device Authentication Scheme}, year={2019}, volume={}, number={}, pages={1460-1462}, doi={10.1109/ICTC46691.2019.8939751}}	https://ieeexplore.ieee.org/abstract/document/8939751	This paper "works" but is not the best.
	Alison Nakai-Lackey	Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications	Approved. But be careful to the difference between apply MFA to IoT applications and MFA-based IoT device authentication	Aleksandr Ometov; Vitaly Petrov; Sergey Bezzateev; Sergey Andreev; Yevgeni Koucheryavy; Mario Gerla	Authentication, Drones, Smart cities, Fingerprint recognition, Internet of Things, Reliability, Internet of Things, Smart devices	The unprecedented proliferation of smart devices together with novel communication, computing, and control technologies have paved the way for A-IoT. This development involves new categories of capable devices, such as high-end wearables, smart vehicles, and consumer drones aiming to enable efficient and collaborative utilization within the smart city paradigm. While massive deployments of these objects may enrich people's lives, unauthorized access to said equipment is potentially dangerous. Hence, highly secure human authentication mechanisms have to be designed. At the same time, human beings desire comfortable interaction with the devices they own on a daily basis, thus demanding authentication procedures to be seamless and user-friendly, mindful of contemporary urban dynamics. In response to these unique challenges, this work advocates for the adoption of multi-factor authentication for A-IoT, such that multiple heterogeneous methods - both well established and emerging - are combined intelligently to grant or deny access reliably. We thus discuss the pros and cons of various solutions as well as introduce tools to combine the authentication factors, with an emphasis on challenging smart city environments. We finally outline the open questions to shape future research efforts in this emerging field.	IEEE Network (Volume: 33, Issue: 2, March/April 2019)	A*	2019	This paper advocates for the adoption of multi-factor authentication for A-IoT, such that multiple heterogeneous methods - both well established and emerging - are combined intelligently to grant or deny access reliably. The pros and cons of various solutions are discussed, as well as tools are introduced to combine the authentication factors, with an emphasis on challenging smart city environments	N/A	...We propose a novel approach to construct reliable authentication solutions for A-IoT devices by intelligently combining multiple potentially unreliable methods, which follows the multi-factor authentication (MFA) paradigm.	There's no solution outlined here, rather a comparison of different methods of A-IoT, such as: Hardware Tokens, Memorable Passwords/PINs, Fingerprint/Palm/Eye Scanner, Facial Recognition, Voice Recognition, Data from Wearables, and Behavioral Patterns.	A. Ometov, V. Petrov, S. Bezzateev, S. Andreev, Y. Koucheryavy and M. Gerla, "Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications," in IEEE Network, vol. 33, no. 2, pp. 82-88, March/April 2019, doi: 10.1109/MNET.2019.1800240.	@ARTICLE{8675176, author={Ometov, Aleksandr and Petrov, Vitaly and Bezzateev, Sergey and Andreev, Sergey and Koucheryavy, Yevgeni and Gerla, Mario}, journal={IEEE Network}, title={Challenges of Multi-Factor Authentication for Securing Advanced IoT Applications}, year={2019}, volume={33}, number={2}, pages={82-88}, doi={10.1109/MNET.2019.1800240}}	https://ieeexplore-ieee-org.ezproxy.rit.edu/document/8675176	This paper works for understanding MFA with IoT applications. Probably not the best considering we're looking at device authentication, but still something interesting to consider/know of.
	Andrea Pallotta	A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks	Approved. But be careful to stick to IoT device authentication.	Chien-Lung Hsu; Tuan-Vinh Le; Chung-Fu Lu; Tzu-Wei Lin; Tzu-Hsien Chuang	Edge computing, Protocol, Servers, Authentication, Computer architecture, Smart cards, Password	Edge computing has played an important role in enabling 5G technology which supports a great number of connected narrow-band IoT devices. In an edge computing architecture enabled with global mobile network, edge or IoT devices are wirelessly connected to the edge of the network. Data acquisition and processing will be handled at or close to the edge of the network in a distributed way. Since edge computing is a heterogeneous distributed interactive system with multiple domains and entities, it might suffer from potential attacks and threats. To provide a trusted edge computing, there must have a robust scheme that allows all participants to mutually authenticate in a secure and privacy-preserved way. With the rapid development of IoT technologies, mobile networks and edge computing architecture, single server has been unable to meet the needs of users. In this paper, we propose a privacy-preserved end-to-end password-based authenticated key exchange protocol for multi-server architecture in edge computing networks. Our protocol allows an end user to use an easy-to-remember password to login to the server, then through foreign agent compute a shared key with another end user for specific use of services. The proposed protocol provides strong user anonymity during communication process. Besides, the proposed protocol is proved to be secure using BAN logic and AVISPA tool. Furthermore, performance analysis shows that the proposed protocol gains stronger security and better computational efficiency. Providing lightweight computation with short key size of ECC, our work is a solution to lower latency and improve efficiency in edge computing networks.	IEEE Access (Volume: 8)	Not present on portal. IEEE-published journals usually have a A*-B score	2020	With the rapid progression of IoT technologies, single server users have not been able to keep up with the users' needs. Traditional centralized cloud models fail and will inefficiently support IoE-based applications. Data acquisition and processing in edge computing architecture will be handled at the network in a distributed way. However, this could cause potential security issues and challenges in processing massive data due to the nature of edge computing architecture, due to its nature. Edge computing architecture is, in fact, a heterogenous distributed system with multiple domains and entities.	Gope and Hwang's Scheme, Bellovin and Merritt's protocol, Sood's protocol, Elliptic Curve Cryptography (ECC)	This paper proposes a privacy-preserved end-to-end authenticated key exchange protocol for multi-server architecture in edge computing networks. The proposed protocol is implemented with single sign-on (SSO) property and multi-server architecture. While preserving user privacy during the communication process, the proposed protocol, compared with previous works, gains stronger security and better efficiency.	The proposed protocol is implemented with a user-controlled Single Sign-On (SSO). There are four phases to the implementation: 1. Smart Card Registration Phase: the user creates an account with identity d0540011. 2. Smart Card Login Phase: the user logs in using the smart card. 3. Server Creation Phase: after the user logs into the system, servers are created using the smart card's identity and password. 4. Account Registration Phase: the user uses ID, password, and arbitrary IDs to register accounts for multiple servers. The password for each account is automatically generated by the SSO system. Subsequently, system interfaces for authentication and key exchange, and password updates are being developed to be available for the user.	C. -L. Hsu, T. -V. Le, C. -F. Lu, T. -W. Lin and T. -H. Chuang, "A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks," in IEEE Access, vol. 8, pp. 40791-40808, 2020, doi: 10.1109/ACCESS.2020.2976431.	@ARTICLE{9016184, author={Hsu, Chien-Lung and Le, Tuan-Vinh and Lu, Chung-Fu and Lin, Tzu-Wei and Chuang, Tzu-Hsien}, journal={IEEE Access}, title={A Privacy-Preserved E2E Authenticated Key Exchange Protocol for Multi-Server Architecture in Edge Computing Networks}, year={2020}, volume={8}, number={}, pages={40791-40808}, doi={10.1109/ACCESS.2020.2976431}}	https://ieeexplore.ieee.org/document/9016184	This paper is somewhat related to IoT authentication

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
2 To connect the two types of work together, we can say sth like device pairing enables two mobile devices to authenticate each other	Niklas Bernardo Correa	Survey and Systematization of Secure Device Pairing		Mikhail Fomichev, Flor Álvarez, Daniel Steinmetzer, Paul Gardner-Stephen, Matthias Hollick	Security, Internet of Things, taxonomy, authentication, communication channels, physical layer, human computer interaction, privacy	Secure device pairing (SDP) schemes have been developed to facilitate secure communications among smart devices, both personal mobile devices and Internet of Things devices. Comparison and assessment of SDP schemes is troublesome, because each scheme makes different assumptions about out-of-band channels and adversary models, and are driven by their particular use-cases. A conceptual model that facilitates meaningful comparison among SDP schemes is missing. We provide such a model. In this paper, we survey and analyze a wide range of SDP schemes that are described in the literature, including a number that have been adopted as standards. A system model and consistent terminology for SDP schemes are built on the foundation of this survey, which are then used to classify existing SDP schemes into a taxonomy that, for the first time, enables their meaningful comparison and analysis. The existing SDP schemes are analyzed using this model, revealing common systemic security weaknesses among the surveyed SDP schemes that should become priority areas for future SDP research, such as improving the integration of privacy requirements into the design of SDP schemes. Our results allow SDP scheme designers to create schemes that are more easily comparable with one another, and to assist the prevention of persisting the weaknesses common to the current generation of SDP schemes.	IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 1, FIRST QUARTER 2018	I was not able to locate the ranking of this particular journal, but IEEE journals in CORE are all above a C rank, with most being within the A* to B range.	2018	The authors identify that there is a lack of a conceptual model that can be use to meaningfully compare secure pairing schemes since each scheme makes it own assumptions and is designed to suit its particular circumstances. The authors intend to provide a taxonomy that can be used to compare existing schemes to each other and identify systemic weakenesses that require further research.	several surveys have investigated different aspects of SDP. Kumar et al. [8] presented the first comparative study to quantify usability and security of various pairing schemes. Our work reveals that quantitative comparison of different SDP schemes is questionable due to the previously taken design decisions, and we qualitatively address the design aspects of SDP to enable meaningful comparison of different SDP schemes. Two other studies from Kobsa et al. [12] and Kainda et al. [11] focused more closely on usability and the role of user actions to achieve security in SDP. Our work has wider scope, because we consider the role of the user as one of the fundamental design aspects of SDP, in addition to physical communication media and particular use cases. The work of Mirzadeh et al. [10] provided an extensive survey on security and performance of different cryptographic protocols used in various SDP schemes, in addition to presenting classification of OOB channels. In our work we devise a more fine-grained classification of communication channels in SDP by differentiating between PHY and HCI channels, and focus on security issues of those channels instead of cryptographic protocols. In their survey Chong et al. [13] presented different modes of user interaction for SDP and analyzed a vast number of SDP schemes using this taxonomy. We refine their findings to classify HCI channels and, additionally, present a set of common security and usability properties to coherently analyze those channels and the SDP schemes relying on them, which has not been done before.	The paper makes the following proposals: • A system model and consistent terminology that facilitates precise description and reasoning about SDP schemes, by considering the three components: – Physical (PHY) channels; – Human-computer interaction (HCI) channels; and – Application classes. • Classification of the existing SDP schemes using this model. • Identification and analysis of systemic security weaknesses commonly found in such schemes, revealing areas where future SDP research is required. • Revelation of the rarity with which privacy is considered among current SDP schemes. • Principles for designing robust SDP schemes	N/A	Fomichev, M., Álvarez, F., Steinmetzer, D., Gardner-Stephen, P. Hollick, M. (2018). Survey and Systematization of Secure Device Pairing. IEEE Communications Surveys & Tutorials, 20(1), 1–6. https://doi.org/10.1109/comst.2018.2802707	@article{ fomichev_álvarez_steinmetzer_gardner-stephen_hollick_2018, title={Survey and Systematization of Secure Device Pairing}, volume={20}, DOI={10.1109/comst.2018.2802707}, number={1}, journal={IEEE Communications Surveys &amp; Tutorials}, author={ Fomichev, Mikhail and Álvarez, Flor and Steinmetzer, Daniel and Gardner-Stephen, Paul and Hollick, Matthias}, year={2018}, pages={1–6}}	https://ieeexplore-ieee-org.ezproxy.rit.edu/stamp/stamp.jsp?tp=&arnumber=8023969	The authors provide a concise way of organzing pairing schemes in IoT. I was only considering specific authentication algorithms, and whether they were robust against attackers able to sniff traffic or spoof/control a device being paired and whether or not it was feasible to implement the algorithms in limited IoT hardware. But the authors argue the importance of considering the context under which the pairing is occuring, such as whether a human user can provide input during the process or if devices must be able to pair by themselves unassisted. The author's decision to organize schemes according to how they employ physical communication channels (wifi, bluetooth, ...), human-device interactions (reading input from a screen, performing gestures, ...), and the context of the pairing (does user control all devices, just one device, is pairing with help of other use or 3rd party infrastructure, ...) is interesting, and makes sense to me. I will have to acquaint myself with more schemes and more taxonomies to determine its usefulness.
3	Sarah Dill	Listen!: Audio-based Smart IoT Device Pairing Protocol	Good, approved	Shijia Mei, Zhihong Liu, Yong Zeng, Lin Yang, Jian Feng Ma	Authentication, IoT, Device Pairing, Audio-based	Context-based zero-interaction has become the trend for smart IoT device pairing. In this paper, we propose a secure and usable mechanism to authenticate devices co-located in smart home scenario, and build a secure communication channel between legitimate devices by utilizing on-board microphones to capture a common audio context. After receiving randomly generated sound signals, smart IoT device uses the time intervals between salient sound signals to derive audio fingerprint which can be matched among co-present devices and then be used to bootstrap trust of the devices. The protocol is based on the idea that devices co-located within a physical security boundary (e.g., single family house) can hear similar sounds, and the devices outside would miss parts of sound signals due to the attenuation when sounds pass through the wall. To accelerate the generation rate of audio fingerprint, an extra sound source is introduced. We implement our protocol on Android devices, and the experiment results show that the protocol can distinguish the malicious devices outside from the legitimate devices located inside a security boundary and can quickly establish a strong secret-key between legitimate devices.	2019 IEEE 19th International Conference on Communication Technology (ICCT)	Not found on conference portal. IEEE seems to have A*-B score mostly	2019	IoT devices are using wireless communication techniques in order to transmit data; however, because this data in many cases is sensitive (such as health data), we need a better way to secure these communications. Other methods of pairing (such as entering a password) don't work on IoT devices with no user interface. The authors came up with an audio-based solution that works around these issues.	N/A	The authors designed a secure IoT device pairing solution (*Listen!*) that is entirely based on sound and a security boundary. The idea behind this is that an adversary trying to eavesdrop cannot do so effectively unless they are physically close to the source of the sound.	The proposed solution can be implemented with smart IoT devices (smartphones) and must be installed. The solution works best with no ambient noise, and the success rate drops as the ambient noise increases in volume.	S. Mei, Z. Liu, Y. Zeng, L. Yang and J. F. Ma, "Listen!: Audio-based Smart IoT Device Pairing Protocol," 2019 IEEE 19th International Conference on Communication Technology (ICCT), 2019, pp. 391-397, doi: 10.1109/ICCT46805.2019.8947178.	@INPROCEEDINGS{8947178, author={Mei, Shijia and Liu, Zhihong and Zeng, Yong and Yang, Lin and Ma, Jian Feng}, booktitle={2019 IEEE 19th International Conference on Communication Technology (ICCT)}, title={Listen!: Audio-based Smart IoT Device Pairing Protocol}, year={2019}, volume={}, number={}, pages={391-397}, doi={10.1109/ICCT46805.2019.8947178}}	https://ieeexplore.ieee.org/abstract/document/8947178	This paper aligns well with "Proximity based IoT device authentication": both propose effective solutions and align similarly in their backgrounds. This paper focuses on smart IoT devices in particular.
	Edwin Liu	Pairing-Based Cryptography on the Internet of Things: A Feasibility Study https://link.springer.com/chapter/10.1007/978-3-030-02931-9_18	approved	Ioanna Karantaidou, Spyros T. Halkidis, Sophia Petridou, Lefteris Mamatas & George Stephanides	Pairing-based Cryptography, Internt of things, Identity-based encryption, Short signatures	Pairing-based cryptography (PBC) has recently received much attention, since the mathematical building block of pairings paved the ground for devising efficient cryptographic protocols exploiting an old inspiration, i.e., to produce the public key of an entity based on its identity. The so-called Identity-Based Cryptography (IBC) simplifies key management procedures, since it does not require certificate-based infrastructures. Moreover, it is an elliptic curve cryptosystem which entails that it offers the same security levels as other public key systems with much smaller key lengths. The above characteristics make it an attractive solution for resource-constrained environments such as the Internet of Things (IoT), where strong confidentiality and signature schemes are necessary. In this article, we conducted feasibility tests of pairing-based cryptography for middle-class IoT devices, such as the Raspberry Pi 3 platform.	WWIC 2018: Wired/Wireless Internet Communications	B	2018	In this article, the authors conduct feasibility tests of pairing-based cryptography for middle-class IoT devices, such as the Raspberry Pi 3 platform. They are trying to search for IoT pairing authentication methods with strong confidentiality and signature schemes.	Boneh, Lynn and Shacham's (BLS) shor tsignautre scheme. Boneh and Franklin's identity-based encryption (IBE) protocol.	Their experiments tested the feasibility of fundamental PBC (Pairing-Based cryptography) and believe it can be fully adopted into IoT resource-constrained devices. They implemented the *Fulldent* IBE scheme and compared it to *BasicIdent*. It seems like the BLS algorithm was approximately equivalent to ECDSA (Elliptic Curve Digital Signature Algorithm) in the signing process, but was more time and energy consuming in the verification process,	1. we conducted real experiments to measure the resource requirements of fundamental pairing-based crytposystems in terms of CPU time, memory and energy; 2. we implement the FullIdent IBE scheme inside the Relic-Toolkit library; 3. we compare the performance of BasicIdent and FullIdent IBE schemes, as well as of BLS and ECDSA signature schemes for different security levels; 4. we tested the feasibility of pairing-based algorithms for middle-class IoT devices, such as the Raspberry-Pi 3 platform.	Karantaidou, I., Halkidis, S.T., Petridou, S., Mamatas, L., Stephanides, G. (2018). Pairing-Based Cryptography on the Internet of Things: A Feasibility Study. In: Chowdhury, K., Di Felice, M., Matta, I., Sheng, B. (eds) Wired/Wireless Internet Communications. WWIC 2018. Lecture Notes in Computer Science(), vol 10866. Springer, Cham. https://doi.org/10.1007/978-3-030-02931-9_18	@InProceedings{10.1007/978-3-030-02931-9_18, author="Karantaidou, Ioanna and Halkidis, Spyros T. and Petridou, Sophia and Mamatas, Lefteris and Stephanides, George", editor="Chowdhury, Kaushik Roy and Di Felice, Marco and Matta, Ibrahim and Sheng, Bo", title="Pairing-Based Cryptography on the Internet of Things: A Feasibility Study", booktitle="Wired/Wireless Internet Communications", year="2018", publisher="Springer International Publishing", address="Cham", pages="219--230", }	https://link.springer.com/chapter/10.1007/978-3-030-02931-9_18	
	Alison Nakai-Lackey	Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems	approved	Hassan N. Noura; Reem Melki; Ali Chehab	Authentication, Cryptography, Internet of Things, Cryptographic protocols, Servers	Authentication is critical for any digital system as it represents the first step towards accessing data and resources. Authentication of entities, especially devices in the Internet-of-Things (IoT) system, is one of the most important security challenges that needs to be addressed; otherwise, it will hinder the deployment of IoT applications. The most widely used authentication mechanisms in IoT are based on one-factor cryptographic techniques. These techniques are often not sufficient in the context of IoT due to the limited computational power of IoT devices and the severity of security concerns, especially that these devices are physically not well protected. Consequently, any weakness in the identification/authentication schemes would allow a compromised entity to perform dangerous attacks. To overcome the above-mentioned limitations and achieve high authentication accuracy, we propose an efficient two-factor lightweight mutual authentication scheme for IoT entities, which can be deployed at various levels; device, control, aggregation node, gateway, and server. The first factor is based on a cryptographic protocol which employs a configurable Physically Unclonable Function (PUF) along with a nonce extracted from the physical channel. The second factor is an entity-based fingerprint that uses specific information (i.e., features that can be extracted from various layers of the communication protocol) to construct a unique fingerprint for each entity. The proposed scheme is designed to require the minimum possible overhead in terms of computation and communication overhead, and ensure maximum security resilience against authentication attacks.	2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)	B	2019	The proposed scheme is designed to require the minimum possible overhead in terms of computation and communication overhead, and ensure maximum security resilience against authentication attacks.	The first factor is based on a cryptographic protocol which employs a configurable Physically Unclonable Function (PUF) along with a nonce extracted from the physical channel. The second factor is an entity-based fingerprint that uses specific information (i.e., features that can be extracted from various layers of the communication protocol) to construct a unique fingerprint for each entity.	To overcome the above-mentioned limitations and achieve high authentication accuracy, we propose an efficient two-factor lightweight mutual authentication scheme for IoT entities, which can be deployed at various levels; device, control, aggregation node, gateway, and server.	Proposed scheme is not given technical experiments, rather a series of theorized ways the scheme would thwart modern known security issues with existing MFA techniques. A few known limitations are issued: the proposed approach introduces a low communication overhead for each authentication cycle, since IoT devices should exchange few additional messages with the server, and IoT devices should extract certain physical channel parameters which requires additional resources and computation overhead.	H. N. Noura, R. Melki and A. Chehab, "Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1-7, doi: 10.1109/VTCFall.2019.8891082.	@INPROCEEDINGS{8891082, author={Noura, Hassan N. and Melki, Reem and Chehab, Ali}, booktitle={2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)}, title={Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems}, year={2019}, volume={}, number={}, pages={1-7}, doi={10.1109/VTCFall.2019.8891082}}	https://ieeexplore.ieee.org/abstract/document/8891082	
	Andrea Pallotta	Practical and Secure IoT Device Authentication Using Physical Unclonable Functions	Approved	John Ross Wallrabenstein	Internet of things, Protocols, PUF-based authentication protocol, Hardware, Cryptography, Authentication	Devices in the internet of things (IoT) are frequently (i) resource-constrained, and (ii) deployed in unmonitored, physically unsecured environments. Securing these devices requires tractable cryptographic protocols, as well as cost effective tamper resistance solutions. We propose and evaluate cryptographic protocols that leverage physical unclonable functions (PUFs): circuits whose input to output mapping depends on the unique characteristics of the physical hardware on which it is executed. PUF-based protocols have the benefit of minimizing private key exposure, as well as providing cost-effective tamper resistance. We present and experimentally evaluate an elliptic curve based variant of a theoretical PUF-based authentication protocol proposed previously in the literature. Our work improves over an existing proof-of-concept implementation, which relied on the discrete logarithm problem as proposed in the original work. In contrast, our construction uses elliptic curve cryptography, which substantially reduces the computational and storage burden on the device. We describe PUF-based algorithms for device enrollment, authentication, decryption, and digital signature generation. The performance of each construction is experimentally evaluated on a resource-constrained device to demonstrate tractability in the IoT domain. We demonstrate that our implementation achieves practical performance results, while also providing realistic security. Our work demonstrates that PUF-based protocols may be practically and securely deployed on low-cost resource-constrained IoT devices.	2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)	Not found on conference portal. IEEE seems to have A*-B score mostly	2016	The issue with other PUF-based authentication implementations is that they lack sufficiently large security parameters. For example, Wallrabenstein presented a contruction of the protocol based on Frikken et al's implementation of PUF-based protocols in the context of banking authentication. However, the issue with Wallrabenstein's contructs is that the security of the proof-of-concept implementation relies on the discrete logarithm problem over a 256-bit-modulus, which, as stated by the paper, is insecure.	Physical Unclonable Functions (PUFs), Physical Random Functions (PRFs), Frikken et al.'s PUF-based protocols for banking authentication, Wallrabenstein's PUF-based protocols, discrete logarithms. elliptic curve cryptography, ElGamal cryptosystem, PUF hardware aging	This paper proposed PUF-based elliptic curve cryptographyic implementation for device enrollment, authentication decryption, and digital signatures for IoT architectures. The protocol provides low-cost tamper protection for unsecured IoT devices and reduced computational and storage requirements while based on the secure 384-bit elliptic curve modulus.	Both the elliptic curve construction and Wallrabenstein's logarithm contruction (for comparison purposes) have been implemented on a small USB dongle containing a Xilinx Artix 7 FPGA and use a 384-bit modulus for an accurate performance comparison. Additionally, they have access to a wide ring ascillator PUF and a MicroBlaze processor. The performance experiments take into consideration the communication between the device and a server equipped with a 1.3 GHz Inter Core M processor and 8GB of RAM	J. R. Wallrabenstein, "Practical and Secure IoT Device Authentication Using Physical Unclonable Functions," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 99-106, doi: 10.1109/FiCloud.2016.22.	@INPROCEEDINGS{7575850, author={Wallrabenstein, John Ross}, booktitle={2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)}, title={Practical and Secure IoT Device Authentication Using Physical Unclonable Functions}, year={2016}, volume={}, number={}, pages={99-106}, doi={10.1109/FiCloud.2016.22}}	https://ieeexplore.ieee.org/abstract/document/7575850	This article is interesting because it explains in details a new implementation of PUF-based authentication and its benefits over elliptic curve cryptographic algorithms
	Niklas Bernardo Correa	Two-Factor Authentication for IoT With Location Information	Approved	Muhammad Naveed Aman, Mohamed Haroon Basheer, Biplab Sikdar	Authentication, Internet of Things (IoT), physically unclonable functions, received signal strength indicator	The number of Internet of Things (IoT) devices is expected to grow exponentially in the near future and produce large amounts of potentially sensitive data. The simple and low cost nature of IoT devices makes them an attractive target for spoofing or impersonation attacks. To solve this issue, this paper proposes a two-factor authentication protocol using physically unclonable functions and the characteristics of the wireless signal from an IoT device. The security analysis and results on MICAz motes shows that the proposed protocol can be used as an effective tool to secure IoT systems from spoofing as well as various other attacks. A performance analysis of the proposed protocol shows that it has a significantly lower computational overhead and energy consumption compared to existing techniques.	IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 2, APRIL 2019	Not found on conference portal. IEEE seems to have A*-B score mostly	2019	One of the major security requirements for the IoT isstrong authentication and controlling access to the network and resources. (...) A second concern with many IoT devices is that they are physically unprotected, i.e., they are installed in locations easily accessible to adversaries. Therefore, an adversary can easily capture these devices and subject them to physical and sidechannel attacks. To solve these issues, this paper uses two-factor authentication with the following two factors. 1) PUFs are used in place of secret keys or passwords to assign a hardware fingerprint to IoT devices. 2) The wireless channel characteristics in the form of received power [measured from the received signal strength indicator (RSSI)] and the link quality indicator (LQI) of the radio signal of the IoT device are used as wireless fingerprints to verify the current location of the IoT device	1) The proposed protocol uses light weight symmetric cryptography, making it suitable for resource constrained IoT devices. 2) This paper uses PUFs to safeguard IoT devices against physical and cloning attacks. 3) The proposed protocol uses the wireless channel characteristics such as RSSI and LQI values to establish the validity of the data gathered from a specific location. 4) Identifying the exact location of an IoT device may not be possible due to the dynamic nature of a wireless channel. Thus, this paper uses analytical models of the wireless channel to detect whether an IoT device is located within a specific area.	This paper focuses on the problem of authentication in IoT systems with the main innovations as follows. 1) An analytical model to detect the change in received power of an IoT node if it is moved beyond its designated location/area. 2) An analytical model based on the change of the probability distribution of LQI to detect if an IoT node has moved beyond its designated location/area. 3) An authentication protocol for IoT devices using two factors for authentication, namely hardware fingerprints in the form of PUFs and the location of an IoT device using the wireless channel characteristics. 4) Experimental results confirming the effectiveness as well as efficiency of the proposed protocol.	PART A - Device Registration: CRPs exchanged between IoT device and server using TOTP. Server stores a CRP, PID, and EID. The client stores PID and EID. PART B - Authentication: IoT begins auth by sending its PID + random nonce to server. If PID associated with CRP, server generates a random nonce and replys with MAC(PID,Challenge, (client nonce, server nonce, IoT ID). The client generates a response to the challenge with its PUF and verifies the MAC, then generates a new PID and replies with MAC (IoT ID, server nonce, client nonce). The wireless gateway relaying requests/responses uses RSSI and LQI measurements to locate the device and itself and forwards this information along with client's request. Server verifies MAC from client and location information and authenticates the device. PART C - Periodically verifiy location: Every time the server receives a new packet from IoT device, it checks the wireless gateway that forwarded it. PART D - Update CRP periodically to maintain freshness: Server initiates CRP update sending a challenge to the IoT device. IoT device verifies MAC and produces a response and sends it. Wireless gateway provides location information and forwards it to server along with client's response. Server verifies location information and MAC, old CRP replaced with new one.	Aman, M. N., Basheer, M. H., &amp; Sikdar, B. (2019). Two-Factor Authentication for IoT With Location Information. IEEE Internet of Things Journal, 6(2). https://doi.org/10.1109/jiot.2019.2792722	@article{aman_basheer_sikdar_2019, title={Two-Factor Authentication for IoT With Location Information}, volume={6}, DOI={10.1109/jiot.2019.2792722}, number={2}, journal={IEEE Internet of Things Journal}, author={Aman, Muhammad Naveed and Basheer, Mohamed Haroon and Sikdar, Biplab}, year={2019}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8542644	This paper brings together PUF based methods as well as location based methods for authentication, which are techniques discussed in other papers read by the group thus far. I found including the wireless gateway into the authentication scheme an interesting idea. On one hand it out-sources a potentially intensive computation away from the resource restrained IoT device and introduces yet another device an attacker would have to compromise to get his way. But on the other it limits aplicability of this protocol, as it would require the network infrastructure immediately around the IoT device to adequate iteself. Installing a new wireless gateway just wont be feasible in many scenarios.
	Sarah Dill	Internet of Things Device Authentication Scheme Using Hardware Serialization	Approved	Anum Hasan, KashifNaseer Qureshi	IoT, Authentication, Hardware	Devices in the Internet of Things (IoT) are often placed ubiquitously so that they can sense, process and communicate data in real time. IoT devices come in varying shapes and sizes with a range of features and resources. When devices are placed ubiquitously the importance of fundamental security goals like authentication increases considerably. Research has mostly studied various aspects of the IoT environment but often miss out on the essential authentication security goal. This paper first studies the latest methods through which authentication is achieved in the IoT. Analysis has shown that the devices lack resources to implement complex authentication algorithms. Another issue with many authentication algorithms is that they are not universally applicable to IoT devices. Based on these findings a novel authentication algorithm is proposed that is based on using device serialization chip. The designed algorithm resists a range of attacks like man-in-the middle, masquerading, device cloning and replay. The scheme is composed of lightweight security primitives that are universally applicable to different types of devices in the IoT for the provision of both authentication and session key generation. The paper presents a security analysis of the proposed scheme to show that the security primitives are a suitable fit and strongly support the system design goals.	2018 International Conference on Applied and Engineering Mathematics (ICAEM)	Not found on conference portal. IEEE seems to have A*-B score mostly	2018	The problem this paper addresses is authentication of IoT devices. Current authentication methods are poorly implemented security-wise or have vulnerabilities in their design.	N/A	The researchers propose a new authentication scheme that prioritiezes security and minimum resource demand. The authentication scheme is comprised of two parts: pre-registration and authentication. This is designed for smart IoT devices.	The scheme was designed to require minimum user intervention, but it does require some intervention when the IoT device is being registered. This solution was designed to be universally applicable to all IoT devices.	A. Hasan and K. Qureshi, "Internet of Things Device Authentication Scheme Using Hardware Serialization," 2018 International Conference on Applied and Engineering Mathematics (ICAEM), 2018, pp. 109-114, doi: 10.1109/ICAEM.2018.8536286.	@INPROCEEDINGS{8536286, author={Hasan, Anum and Qureshi, KashifNaseer}, booktitle={2018 International Conference on Applied and Engineering Mathematics (ICAEM)}, title={Internet of Things Device Authentication Scheme Using Hardware Serialization}, year={2018}, volume={}, number={}, pages={109-114}, doi={10.1109/ICAEM.2018.8536286}}	https://ieeexplore.ieee.org/abstract/document/8536286	The paper doesn't specifically list how their solution has been tested, but it has strong theory behind it.
	Edwin Liu	https://ieeexplore.ieee.org/abstract/document/9367500	Approved. Be careful workshop paper generally has low quality than the main conference. Eg. Globecom workshop vs Globecom	Xun Xiao, Fengyang Guo, Artur Hecker	Authentication, Prototypes, Blockchain, Performance gain, Internet of Things, Security, Machinery	Nowadays, electronic industry witnesses a massive explosion of offering Internet of Things (IoT) devices with cellular technology to the market for machinery type communication (MTC). Due to usually unmanned deployments, MTC requires authentication for security reasons before exchanging actual information. Today, IoT cross-domain authentication executed at a blockchain backend side is well studied. However, lightweight proximity-based authentication for cross-domain IoT devices is still lack of consideration. In this paper, we show the first attempt to solve this problem based on IOTA blockchain technology. Specifically, our solution benefits both from the advantages of IOTA blockchain and the capabilities of mobile edge computing (MEC) so that a lightweight authentication procedure can be achieved by reducing involvements of the heavy backend side. A small in-house prototype system is implemented in order to validate the feasibility of the proposed solution.	2020 IEEE Globecom Workshops (GC Wkshps	According to Professor low quality :(but isn't found	2020	Firstly, IoT devices are expected to work standalone without regular maintenance (e.g. in open and rural areas), thus easy to be damaged and/or hacked. Secondly, IoT devices are usually resource-constrained, which prevents IoT devices from running sophisticated mechanisms for self-protection. If IoT devices are compromised without notice, other participants in the system face security risks. Especially when cellular IoT(CIoT) devices come into the whole picture, there will be a significant number of devices deployed at a wild range without regular maintenance. Consequently, self-managed authentication for MTC is a prerequisite before the actual communication starts.	Preliminary techniques include Single Domain Authentication With Blockchain, Cross-Domain Authentication With Blockchain, and Integration of Blockchain and MEC.	The solution provided in the paper is a local authentication execution over bteween 2 devices, instead of them relying on heave backend procedures as of existing solutions. It also includes a lightweight blockchain - IOTA within MEC, which inherits the benefits of the featured technologies.	1) Device registration. Here one of the devices sends a registration request to its IoT service provider. THey check the attributes of the request and validate it. Concurrently, a transaction SPCert-Tx are submitted to an IOTA node deployed at MEC by the service provider. After successfully processed at IOTA, the results are returned. 2) Service Access and Proximity-Based Authentication. Now one of the devices sends a service request to another. The 2nd device parses the information sent from the 1st device. It then sends a read request to an IOTA node deployed by MEC to retrieve information of the corresponding service provider and certificate. Results are returned. If both pass, authentication is successful, otherwise failed. It replies back to device 1 with an "OK" to proceed. 3) Device Certificate Revoation. Service providers are able to revoke certificates when they become invalid.	X. Xiao, F. Guo and A. Hecker, "A Lightweight Cross-Domain Proximity-Based Authentication Method for IoT Based on IOTA," 2020 IEEE Globecom Workshops (GC Wkshps, 2020, pp. 1-6, doi: 10.1109/GCWkshps50303.2020.9367500.	@INPROCEEDINGS{9367500, author={Xiao, Xun and Guo, Fengyang and Hecker, Artur}, booktitle={2020 IEEE Globecom Workshops (GC Wkshps}, title={A Lightweight Cross-Domain Proximity-Based Authentication Method for IoT Based on IOTA}, year={2020}, volume={}, number={}, pages={1-6}, doi={10.1109/GCWkshps50303.2020.9367500}}	https://ieeexplore.ieee.org/abstract/document/9367500/keywords#keywords	

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
	Alison Nakai-Lackey	MAFIA: Multi-layered Architecture For IoT-based Authentication	Approved	Pranut Jain; Henrique Pötter; Adam J. Lee; Daniel Mósse	Authentication, Security, Usability, Energy consumption, Privacy, Face recognition, Complexity theory	Multi-factor authentication (MFA) systems are being deployed for user authentication in online and personal device systems, whereas physical spaces mostly rely on single-factor authentication; examples are entering offices and homes, airport security, and classroom attendance. The Internet of Things (IoT) growth and market interest has created a diverse set of low-cost and flexible sensors and actuators that can be used for MFA. However, combining multiple authentication factors in a physical space adds several challenges, such as complex deployment, reduced usability, and increased energy consumption. We introduce MAFIA (Multi-layered Architecture For IoT-based Authentication), a novel architecture for co-located user authentication composed of multiple IoT devices. In MAFIA, we improve the security of physical spaces while considering usability, privacy, energy consumption, and deployment complexity. MAFIA is composed of three layers that define specific purposes for devices, guiding developers in the authentication design while providing a clear understanding of the trade-offs for different configurations. We describe a case study for an Automated Classroom Attendance System, where we evaluated three distinct types of authentication setups and showed that the most secure setup had a greater usability penalty, while the other two setups had similar attributes in terms of security, privacy, complexity, and usability but varied highly in their energy consumption.	2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)	Not found on conference portal. IEEE seems to have A*-B score mostly. Conference is relatively new, 2022 would be its 4th year	2020	In MAFIA, we improve the security of physical spaces while considering usability, privacy, energy consumption, and deployment complexity. MAFIA is composed of three layers that define specific purposes for devices, guiding developers in the authentication design while providing a clear understanding of the trade-offs for different configurations	We propose a novel multi-layered architecture called MAFIA that defines how to utilize IoT devices to form an energy efficient CLUAS. We create the first model for different aspects of battery-operated CLUAS, such as energy efficiency, deployment complexity, usability, security, privacy, and present guidelines to compare different authentication setups. We demonstrate how our proposed architecture and models can be utilized to compare and select an IoT-based authentication system, using a case-study on Automated Attendance System (AAS) to automate event attendance.	In this paper, we propose both a novel architecture called MAFIA to leverage IoT devices efficiently and effectively in setting up a CLUAS, as well as models to quantify different aspects of a user authentication system. MAFIA defines three layers: (1) the Trigger Layer to make the authentication system energy efficient; (2) the Identification Layer to determine the identity of the user or subset of users attempting to authenticate, without compromising the usability of the authentication system; and (3) the Verification Layer to confirm the identity of the user, again while maintaining the usability of the system	Through a case study of an automated attendance system, MAFIA was applied to evaluate its security & privacy, usability penalty, and deployment complexity., and energy consumption.	P. Jain, H. Pötter, A. J. Lee and D. Mósse, "MAFIA: Multi-layered Architecture For IoT-based Authentication," 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 2020, pp. 199-208, doi: 10.1109/TPS-ISA50397.2020.00035.	@INPROCEEDINGS{9325348, author={Jain, Pranut and Pötter, Henrique and Lee, Adam J. and Mósse, Daniel}, booktitle={2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)}, title={MAFIA: Multi-layered Architecture For IoT-based Authentication}, year={2020}, volume={}, number={}, pages={199-208}, doi={10.1109/TPS-ISA50397.2020.00035}}	https://ieeexplore.ieee.org/abstract/document/9325348	Yet again another new architecture, but good to understand failings of current MFA practices.
	Andrea Pallotta	Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud	Approved	Mustafa A. Al Sibahee, Songfeng Lu, Zaid Ameen Abduljabbar, Erasmus Xin Liu, Yanli Ran, Ahmed Abdulelah Jasim Al-ashoor, Mohammed Abdulridha Hussain, Zaid Alaa Hussien	Authentication, Watermarking, Smart devices, Feature extraction, Biometrics (access control), Receivers, Cryptography	Document integrity and origin for E2E S2S in IoTcloud have recently received considerable attention because of their importance in the real-world fields. Maintaining integrity could protect decisions made based on these message/image documents. Authentication and integrity solutions have been conducted to recognise or protect any modification in the exchange of documents between E2E S2S (smart-to-smart). However, none of the proposed schemes appear to be sufficiently designed as a secure scheme to prevent known attacks or applicable to smart devices. We propose a robust scheme that aims to protect the integrity of documents for each users session by integrating HMAC-SHA-256, handwritten feature extraction using a local binary pattern, one-time random pixel sequence based on RC4 to randomly hide authentication codes using LSB. The proposed scheme can provide users with one-time bio-key, robust message anonymity and a disappearing authentication code that does not draw the attention of eavesdroppers. Thus, the scheme improves the data integrity for a users messages/image documents, phase key agreement, bio-key management and a one-time message/image document code for each users session. The concept of stego-anonymity is also introduced to provide additional security to cover a hashed value. Finally, security analysis and experimental results demonstrate and prove the invulnerability and efficiency of the proposed scheme.	2020 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)	Not found on conference portal. IEEE seems to have A*-B score mostly	2020	With the increment in IoT data trasmission, security and integrity have become a primary concern in fields that deal with confidential data, such as medicine, military, government, and e-commerce. Previously stipulated techniques, such as cryptographyic one-way hash functions and steganography, are vulnerable to replay and MITN attacks.	One-way hash function, steganography, MAC schemes (Castiglione et al., and Chen et al), watermark authentication schemes (Hsu and Wu proposal, and spatial domains), ECC algorithms	The paper presents a new and efficient authentication scheme with anonymity between pairs of smart devices for E2E communication. The scheme is based on extracting handwritten signature features to generate a symmetric one-time bio-key and it aims to prevent known attacks such as replay and MITN attacks. The efficiency of the scheme resides in the fact that it can hide bio-MAC in low-resolution images without high computational costs.	The scheme consists of two phases: - Registration Phase: the key components use public and private keys and ECC algorithm to secure the identities of the sender (S) and receiver (R), securely transmit hadwritten signatures to the cloud solution provider (CSP), and finally send a bio-shared vector from the CSP to S and R. - Authentication Phase: the phase is executed when the sender (S) wants to send a document (M) to the receiver (R). S uses the bio-shared vector from the registration phase to generate a one-time bio-key secret, used to computed a one-time bio-authentication key. To prevent replay attacks, the authentication code is randomly permuted.	M. A. A. Sibahee et al., "Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud," 2020 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2020, pp. 1-6, doi: 10.1109/ICSPCC50002.2020.9259519.	@INPROCEEDINGS{9259519, author={Sibahee, Mustafa A. Al and Lu, Songfeng and Abduljabbar, Zaid Ameen and Liu, Erasmus Xin and Ran, Yanli and Al-ashoor, Ahmed Abdulelah Jasim and Hussain, Mohammed Abdulridha and Hussien, Zaid Alaa}, booktitle={2020 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)}, title={Promising Bio-Authentication Scheme to Protect Documents for E2E S2S in IoT-Cloud}, year={2020}, volume={}, number={}, pages={1-6}, doi={10.1109/ICSPCC50002.2020.9259519}}	https://ieeexplore.ieee.org/document/9259519	Even if mostly theoretical, the paper sets a starting point for bio-authentication for cloud computing and IoT
4	Niklas Bernardo Correa	An Unlinkable Authentication Scheme for Distributed IoT Application - https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8620304		YOUSHENG ZHOU, TONG LIU, FEI TANG, MAGARA TINASHE	Authentication, IoT, privacy-preserving, security	The Internet of Things (IoT) is an enormous ubiquitous-network, which connects the objects through various sensors. The IoT technology promotes the interconnection and fusion between the physical world and information space, and it facilitates the day-to-day life of people. However, since a lot of equipped sensors are unattended and open, the IoT must face and overcome the main problems of security and privacy. Authentication is one of the paramount security concerns in the IoT environment, in which a user could directly access data from the sensors. Therefore, we propose an authentication and key agreement scheme providing unlinkability for the IoT environment based on bilinear pairings. The formal security proof demonstrates that the proposed protocol is unforgeable under the adaptively chosen message attack, and the session key exchange is semantic secure under the eCK model. In addition, the computation and communication costs of the proposed scheme are evaluated and compared with some existing similar schemes, which exhibits that it pleasantly addresses the needs of the IoT as far as security properties and computation expenses.	IEEE Access Journal	Not found,but IEEE journals are ranked A*-C, with most being in the A-B range	2019	The features of the proposed scheme are as follows: 1) Unlinkability property during authentication procedure to protect users' privacy. Any two or more messages from different sessions cannot be confirmed by any third party whether these messages come from the same entity. 2) Achieves anonymity. Since the real identity of user is randomized, it is kept hidden for any external unauthorized entities. 3) Ensures the forward secrecy. All transmitted messages have been randomized so that any attacker cannot derive the previous session key from the current session key. 4) Achieves conditional traceability to resolve possible disputes. If any dispute or misbehavior occurs during the authentication, the trusted third party can reveal the real identity of users with the exchanged authentication messages.	The paper sites numerous papers in the Related Works section that have proposed authentication schemes using a wide array of different techniques, not necessairly related to this paper's proposed solution. In the Preliminaires section, the paper introduces a model of the IoT network, notation used throughout the paper, as well as the definition of the elliptic curve discrete logarithm problem.	Propose an authentication and key agreement scheme providing unlinkability for the IoT environment based on bilinear pairings. The formal security proof demonstrates that the proposed protocol is unforgeable under the adaptively chosen message attack, and the session key exchange is semantic secure under the eCK model.	Consists of the following phases: 1) Initialization - genetrates public system parameters; 2) User Registration - creates public/private key pairs; 3) User Login; 4) User authentication and key agreement - where user and sensor node mutually authenticate. Initialization Phase 1) Trusted 3rd Party chooses EC additive group, three secure hash functions, a MAC code, and a bilinear pairing. 2) T3P selects a suitable private key and computes the associated public key. 3) T3P sets public parameters 4) Sensor node choses a suitable private key and computes its public key User Registration 1) User selects an identity and password, sends hash (password, identity) to T3P 2) T3P chooses random number and computes partial public and private keys, and a pseudonym for the user and returns these 3) The user then inputs the processed received data into his smart card 4) User selects a suitable random number as a private key and computes the corresponding partial key User Login and Request 1) User inserts smart card and inputs his ID and password, from which smartcard computes Hash(k,pw) 2) Smartcard picks a random number and sends it to the sensor node	ZHOU, Yousheng., LIU, Tong., TANG, Fei, &; TINASHE, Magara. (2019). An Unlinkable Authentication Scheme for Distributed IoT Application. IEEE Access, 6. https://doi.org/10.1109/ACCESS.2019.2893918	@article{zhou_liu_tang_tinashe_2019, title={An Unlinkable Authentication Scheme for Distributed IoT Application}, volume={6}, DOI={10.1109/ACCESS.2019.2893918}, journal={IEEE Access}, author={ZHOU, YOUSHENG and LIU, TONG and TANG, FEI and TINASHE, MAGARA}, year={2019}}		
	Sarah Dill	A Blockchain-Based Authentication and Security Mechanism for IoT	Approved!	Donging Li, Wei Peng, Wenping Deng, Fangyu Gai	IoT, Authentication, Security, Blockchain	The existing identity authentication of IoT devices mostly depends on an intermediary institution, i.e., a CA server, which suffers from the single-point-failure attack. Even worse, the critical data of authenticated devices can be tampered by inner attacks without being identified. To address these issues, we utilize blockchain technology, which serves as a secure tamper-proof distributed ledger to IoT devices. In the proposed method, we assign a unique ID for each individual device and record them into the blockchain, so that they can authenticate each other without a central authority. We also design a data protection mechanism by hashing significant data (i.e. firmware) into the blockchain where any state changes of the data can be detected immediately. Finally, we implement a prototype based on an open source blockchain platform Hyperledger Fabric to verify the proposed system.	2018 27th International Conference on Computer Communication and Networks (ICCCN)	B	2018	This paper focuses on the security of IoT, especially identitiy authentication and security protection, for IoT devices.	Uses existing blockchain technology	The paper suggests using blockchain in a multi-node network. Each device is a node in the blockchain, and each device ID, public key, hash of critical data, among other information is stored. This is paired with a periodic integrity check to ensure each node has not been tampered with.	The authors tested their solution on an IoT cluster, with devices including Raspberry Pis. They then defined different transactions that would be performed, generated key pairs, and tested data integrity verification.	D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-6, doi: 10.1109/ICCCN.2018.8487449.	@INPROCEEDINGS{8487449, author={Li, Dongxing and Peng, Wei and Deng, Wenping and Gai, Fangyu}, booktitle={2018 27th International Conference on Computer Communication and Networks (ICCCN)}, title={A Blockchain-Based Authentication and Security Mechanism for IoT}, year={2018}, volume={}, number={}, pages={1-6}, doi={10.1109/ICCCN.2018.8487449}}	https://ieeexplore.ieee.org/abstract/document/8487449	This solution does well in preventing malicious behavior. Ties in well with our research topic.
	Edwin Liu	https://ieeexplore.ieee.org/abstract/document/9795787	Approved, closely related	Ali Abdullah S. AlQahtani; Hosam Alamleh; Baker Al Smadi	Internet of Things, IoT, ad hoc, proximity, Beacon Frame, IoT Authentication	Internet of Things (IoT) is a distributed communication technology system that offers the possibility for physical devices (e.g., vehicles, home appliances sensors, actuators, etc.), known as Things, to connect and exchange data, more importantly, without human interaction. Since IoT plays a significant role in our daily lives, we must secure the IoT environment to work effectively. Among the various security requirements, authentication to the IoT devices is essential as it is the first step in preventing any negative impact of possible attackers. Using the current IEEE 802.11 infrastructure, this paper implements an IoT devices authentication scheme based on something that is in the IoT device's environment (i.e., ambient access points). Data from the broadcast messages (i.e., beacon frame characteristics) are utilized to implement the authentication factor that confirms proximity between two devices in an ad hoc IoT network.	2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)	Isnt listed	2022	The number of IoT devices have double from 2015 to 2020 (115 billion to 31 bllion devices). With this rise in IoT devices, that has been a large increase in IoT device attacks, such as DDoS and randsomware attacks. From 2016 to 2017, there was a 600% increase in these atacks, 6000 to 50000 reported. The authors proposed a technique to authenticate IoT devices in ad hoc networks to verify proximity. This way only devices within a certain distance from other authenticated IoT devices will be able to connect to the network.	Some authentication methods known are On-way authentication: in the case before two IoT devices start to communicate with each other, only IoT device authenticates itself to the other, while the other IoT device will not be authenticated. Two-way authentication: both IoT devices must authenticate themselves to each other prior to the communication.Three-way authentication: a service provider is involved in this type, which authenticates the two IoT devices and assists them to authenticate each other. Distributed: this method utilizes a distributed authentication technique between the IoT devices prior to the communication. Centralized: a trusted third end is utilized to distribute and manage the authentication certificates used. The methods for determining proximity could be GPS, bluetooth, or Wi-Fi	This paper proposes a technique to authenticate IoT devices in ad hoc networks to verify proximity. This is done in a way that only devices within a certain distance from other authenticated IoT devices will be able to connect to the network. Meanwhile, devices that are far from an authenticated device or not physically in the area will fail in the proximity authentication. The proposed system enforces security in ad hoc IoT networks. Also, it figures the more suitable device to connect to in an ad hoc network that would reflect the most suitable Radio frequency conditions to communicate. The experiment showed an adequate accuracy of proximity authentication that can be increased with configuring the tolerance in the threshold.	A. Two-device proximity authentication - In this experiment, two Raspberry Pis were placed within two meters of each other. Each Raspberry Pi scanned and collected the Wi-Fi beacon frames and RSSI in the area. The collected data was used to calculate the value of the threshold. In the experiment, the ten access points with the highest RSSIs were used in the equation. To test the proposed system, the two Raspberry Pis were placed at ten different locations around the building. Ten authentications were attempted at each location. Five of these attempts were conducted when the two devices were less than two meters apart. Then, five more times where the two devices are more than two meters apart. The data was collected for each attempt and the Euclidean distance was calculated. This distance was compared to the threshold to determine successful and failing authentications. B. Several nodes simulation - This experiment is to simulate the system's operations when several nodes are involved. The simulation was conducted utilizing python. The threshold calculated in the experiment above was considered. A function was written to perform the authentication following the steps above. The nodes in the simulation were configured with these Actual RSSI values at ten different locations collected in the experiment above. The simulation had each node to authenticate with the other through an iteration. Each node in the simulation would attempt to connect to the node where there are the nodes that meet the threshold and with the least Euclidean distance. In the simulation, each device is connected to a node with the least distance. The experiment returned authentication accuracy of 90%.	A. A. S. AlQahtani, H. Alamleh and B. Al Smadi, "IoT Devices Proximity Authentication In Ad Hoc Network Environment," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795787.	@INPROCEEDINGS{9795787, author={AlQahtani, Ali Abdullah S. and Alamleh, Hosam and Al Smadi, Baker}, booktitle={2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)}, title={IoT Devices Proximity Authentication In Ad Hoc Network Environment}, year={2022}, volume={}, number={}, pages={1-5}, doi={10.1109/IEMTRONICS55184.2022.9795787}}	https://ieeexplore.ieee.org/abstract/document/9795787	closely related
	Alison Nakai-Lackey	FPGA Implementation of ECC Enabled Multi-factor Authentication (E-MFA) Protocol for IoT Based Applications	Approved	S. Raja Sekar, S. Elango, Sajan P. Philip & A. Daniel Raj	Multifactor authentication Point multiplication FPGA E-Health IoT ECC application	IoT platform creates attractive opportunities for our daily lives which make us smarter and more comfortable. IoT offers an incredible guarantee in the e-healthcare field by enhancing the quality of service with limited time-bound. The connectivity provided for e-healthcare devices poses overwhelming security and privacy concerns in this area. In this work, the Elliptic Curve Cryptography (ECC) based Multi-Factor Authentication (MFA) is employed between two entities to enhance security. The authentication is achieved using the Point multiplication operation, which provides more randomness. The three-factor authentication protocol for IoT based E-health devices is presented in this work. The architecture is coded using Verilog HDL, synthesized using Xilinx Synthesis Technology (XST) and ported in Zynq FPGA device (XC7Z020CLG484–1). The results show that the proposed three-factor mutual authentication protocol provides better security.	International Conference on Microelectronic Devices, Circuits and Systems	Not found on conference portal	2021	One of the considered problems with the traditional way is to maintain the password database. If it is captured by the attackers, the probability of guesses with the speed limit of the hardware used nowadays, obviously it will be cracked. MFA is more efficient than the traditional way of using only username and password.	A proposed protocol designed using the ECC point multiplication architecture to produce the output values based on the design	The Elliptic Curve Cryptography (ECC) based authentication is proposed to provide better authentication and security. This paper's framework includes the proposed protocol design, analysis of the algorithm with the brief explanation of the sample problem, Finite State Machine (FSM), simulation result of the proposed protocol.	Theorized simulation was created to implement the protocol	Sekar, S.R., Elango, S., Philip, S.P., Raj, A.D. (2021). FPGA Implementation of ECC Enabled Multi-factor Authentication (E-MFA) Protocol for IoT Based Applications. In: Arunachalam, V., Sivasankaran, K. (eds) Microelectronic Devices, Circuits and Systems. ICMDCS 2021. Communications in Computer and Information Science, vol 1392. Springer, Singapore. https://doi.org/10.1007/978-981-16-5048-2_34	@InProceedings{10.1007/978-981-16-5048-2_34, author="Sekar, S. Raja and Elango, S. and Philip, Sajan P. and Raj, A. Daniel", editor="Arunachalam, V. and Sivasankaran, K.", title="FPGA Implementation of ECC Enabled Multi-factor Authentication (E-MFA) Protocol for IoT Based Applications", booktitle="Microelectronic Devices, Circuits and Systems", year="2021", publisher="Springer Singapore", address="Singapore", pages="430--442", abstract="IoT platform creates attractive opportunities for our daily lives which make us smarter and more comfortable. IoT offers an incredible guarantee in the e-healthcare field by enhancing the quality of service with limited time-bound. The connectivity provided for e-healthcare devices poses overwhelming security and privacy concerns in this area. In this work, the Elliptic Curve Cryptography (ECC) based Multi-Factor Authentication (MFA) is employed between two entities to enhance security. The authentication is achieved using the Point multiplication operation, which provides more randomness. The three-factor authentication protocol for IoT based E-health devices is presented in this work. The architecture is coded using Verilog HDL, synthesized using Xilinx Synthesis Technology (XST) and ported in Zynq FPGA device (XC7Z020CLG484--1). The results show that the proposed three-factor mutual authentication protocol provides better security.", isbn="978-981-16-5048-2" }	https://link.springer.com/chapter/10.1007/978-981-16-5048-2_34	

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
5	Andrea Pallotta	On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure	Approved	Ashok Kumar Das, Basudeb Bera, Mohammad Wazid, Sajjad Shaukat Jamal, Youngho Park	Servers, Security, Internet of Things, Authentication, Smart cards, Password	In recent years, the Internet of things (IoT) has become an encouraging communication paradigm that has numerous applications including smart city, smart home and intelligent transportation system. The information sensed by several IoT smart devices can be security stored at the (cloud) servers. An external user, being a client, can access the services from a server for the sensing information, provided that a mutual authentication happens among them. Using the established session key among the user and the server, encrypted information with the help of session key can be delivered to the user by the server securely. Recently, Rana et al. proposed a smart-card based remote user authentication scheme using user password. In this comment paper, we carefully analyzed the scheme of Rana et al. and tracked down that their scheme is insecure against serious attacks, including stolen smart card attack, privileged-insider attack, user impersonation attack, password change attack and Ephemeral Secret Leakage (ESL) attack. Furthermore, their scheme does not preserve untraceability feature. To remedy these security pitfalls, we also provide some remedies that can help in building more secure and effective user authentication scheme to apply in securing next generation IoT infrastructure.	IEEE Access (Volume: 9)	Not found on conference portal. IEEE seems to have A*-B score mostly	2021	With the exponental increase of IoT devices deployed and of data, a new type of authentication scheme has been recently proposed by Rana et al.: a smart-card based remote authentication scheme based on user password. However, the proposed scheme has several security weaknesses which allow attacks such as useeer impersonation attack and Ephemeral Secret Leakage (ESL) attacks to be succssful.	Rana et al. smart-card authentication scheme, Lamport's password authentication, biometric-based authentication schemes, Kaul and Awasthi smart-card authentication scheme, Dolev and Yao threat model (DY model), Canetti and Krawczyk adversary model (CK-adversary model), Ephemeral Secret Leakage (ESL) attacks	The paper suggests several improvements to the Rana et al. authenticaiton scheme aimed to resolve its security weaknesses. The authors added a fuzzy extractor, a popular biometrics verification techniques, as third factor to improve security. The paper analyses each of the proposed attacks and add protection against them by modifying the original algorithms.	Each security fix describes the logical process and why it's secure based on a threat model: 1. Privileged-insider: To protect against privileeged-insider and smart-card attacks, the paper proposes to add an extra step to the registration phase. During this phase, the user needs to pick another random secret and a temporary identity (TID). In this way, an attacker can only know the TID, and not the user password or the user's personal biometrics imprint. 2. User impersonation and ESL attack: the solution for these types of attacks is to have the user input their credentials and imprint their biometrics after inserting the smart card. The server then generates a fresh timestamp, random seecret, and temporary identity, used to validate the session and generate a session key that depends on both permanent and temporary secrets. 3. Untraceability preservation: As an improvement of the previous fix (usr impersonation and ESL attack), the authors propose to a temporary identity (TID) instead of a static one in the authentication request, which is later updated with a new random TID. The attacker cannot link multiple sessions through the messages anymore, safeguarding untraceability and anonymity. 4. User password change attack: As a fix for user password change attacks, the paper proposes the implementation of an algorithm that allows the user to update their credentials locally without having to communicate with the server. Any remote attacker cannot have access to this process.	A. K. Das, B. Bera, M. Wazid, S. S. Jamal and Y. Park, "On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure," in IEEE Access, vol. 9, pp. 71856-71867, 2021, doi: 10.1109 /ACCESS.2021.3079312.	@ARTICLE{9427478, author={Das, Ashok Kumar and Bera, Basudeb and Wazid, Mohammad and Jamal, Sajjad Shaukat and Park, Youngho}, journal={IEEE Access}, title={On the Security of a Secure and Lightweight Authentication Scheme for Next Generation IoT Infrastructure}, year={2021}, volume={9}, number={}, pages={71856-71867}, doi={10.1109 /ACCESS.2021.3079312}}	https://ieeexplore.ieee.org/document/9427478	While not introducing a new authentication scheme, I found this comment paper to be really interesting because it analyses an already existing authentication algorithm (Rana et al. scheeme) and points out its security flaws through seveeral attacks. They also suggested ways to improve the scheme and improve its security. I wish there was more information on why each attack has been chosen for the threat assessment.
	Niklas Bernardo Correa	Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices - https://ieeexplore-ieee-org.ezproxy.rit.edu/stamp/stamp.jsp?tp=&arnumber=8421575		Fangmin Sun , Chenfei Mao, Xiaomao Fan, and Ye Li	Device security, gait recognition, sensor signal processing, user authentication, wearable Internet of Things (WIoT) devices.	With the rapid development of wearable Internet of Things (WIoT) devices, a significant amount of sensitive/private information collected by them poses a considerable challenge to the security of the WIoT devices. The accelerometer-based gait recognition is considered as an emerging and fast-evolving technology in security and access control fields and has achieved outstanding performance at certain fixed walking speeds. However, the gait recognition performance of the above technology deteriorates dramatically when the walking speed varies. To address this issue, both the speed-adaptive gait cycle segmentation method and individualized matching threshold generation method were proposed in this paper. Furthermore, the contrast experiments were conducted on the ZJU-GaitAcc public dataset sampled from five different body locations and the self-collected dataset sampled at various walking speeds. The experimental results indicated the average gait recognition and user authentication rates of 96.9% and 91.75%, respectively. As compared to the available state-ofthe-art methods based on the fixed walking speeds and constant thresholds, the proposed method improved the gait recognition by 25.8% and user authentication by 21.5%.	IEEE INTERNET OF THINGS JOURNAL, VOL. 6, NO. 1, FEBRUARY 2019	Not found on conference portal. IEEE seems to have A*-B score mostly	2019	The paper proposes an authentication method with 2 components 1) speed-adapative gait extraction able to authenticate a user walking at different speeds 2) Individualized threshold generation. To achieve this, there are the following goals: 1) Produce gait recognition method that is speed-adaptive and able to compute step frequency and estimate the gait cycle length. 2) Develop a Pearson correlation coefficient (PCC) based threshold generation method that adapts to the user's gait 3) Determine relationship between IoT device location on the user's body and recognition rate.	1) Nickel and Busch and Derawi et al: using sampled three-axial acceleration values for authentication, 5% and 9% EER via historgram similarity and cycle length method respectively. 2) Gait segmentation using fixed length, gait cycle, or basing endpoint of gat withn a fixed range not suitable when there is walking speed variation 3) Using public inertial sensor datasets for gait-based authentication like ZJU-GatAcc or OU-ISIR 4) Fast Fourier Trasnfer gait cycle estimation is better when walk speed varies	1) Registration * Collect walking acceleration data while the user walks for 1-min * Log data to computing module, subject it to Fast Fourier Transform and use it to estimate step cycle length. * Dervie gait cycle from step cycle and construct the gait template. 2) Authentication * Data collected during registration is segmented into 8 second windows with 4 second overlaps * Subject each segment to FFT to estimate cycle lengths, then gait cycles, which are then normalized using a special method * PCC-based template matching to determine whether to accept or reject the authentication attempt	Adaptive Gait Cycle Extraction Method: * Gait cycle = sampling rate of acceleration signal / step frequency * start-point + gait cycle < Endpoint of Gait < start-point + gait cycle + regulating factor User Authentication Algorithm: * PCC = covariance(x,y)/(standard deviation x * standard deviation y) * Individualized Threshold Generation = SUM(local_max (PCC(gait cycle, data_segment(k)), k=1, k=R)	Sun, F., Mao, C., Fan, X., &amp; Li, Y. (2019). Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices. IEEE Internet of Things Journal, 6(1), 820–830. https://doi.org/10.1109/jiot.2020.2968143	@article{sun_mao_fan_li_2019, title={Accelerometer-Based Speed-Adaptive Gait Authentication Method for Wearable IoT Devices}, volume={6}, DOI={10.1109/jiot.2020.2968143}, number={1}, journal={IEEE Internet of Things Journal}, author={Sun, Fangmin and Mao, Chenfei and Fan, Xiaomao and Li, Ye}, year={2019}, month={Feb}, pages={820–830}}	https://ieeexplore-ieee-org.ezproxy.rit.edu/stamp/stamp.jsp?tp=&arnumber=8421575	I found gait-based authentication interesting because it does not appear to have remote attack vectors, assuming authentication is strictly User-to-IoT and the device is not authenticating somewhere else. An attacker would need to have physical access to the device in order to try to mimic the user's gait. The paper claims that previous gait-based authentication schemes already were secure from such attacks it deemed "zero-effort" or "minimal-effort". I think that attacks against such devices would not target authentication but try to bypass it altogether to directly obtain data in the device. Gait-based authentication is also restrictied to small devices that can be worn in a particular location in the body so its readings are correct, so its applicability is somewhat restricted. Although many devices fall into this category,
	Sarah Dill	Secure and Safe In-Vehicle Device Pairing Using Accelerometer Sensor	Approved. closely related	Yu Seung Kim	Secure pairing, IoT, vehicle, Android, authentication, security	Secure pairing of Internet-of-Things (IoT) devices is a challenging problem because many of them lack the typical user interfaces to provide credentials in the authentication process different from conventional computing platforms. The identical problem is observed in a modern automotive environment. Users bring various smart devices besides smartphones to the cabin and want to connect to their vehicles. Moreover, as car/ride-sharing economy is expected to be continuously grown, such an in-vehicle device authentication will soon become a roadblock, without a proper mechanism, before enabling emerging services. In this study, we develop a novel authentication mechanism, which uses the shared context of two pairing ends. In a moving vehicle, for example, a vehicle and an IoT device located in cabin share the motion. The proposed mechanism compares the motion data from accelerometer sensors in both paring ends to determine their spatial co- existence. We implement a proof- of-concept Android app to prove its feasibility and evaluate in practical user scenarios. By minimizing the user interaction in device authentication, the proposed mechanism will improve safety and usability as well as security.	2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)	B	2019	There is an issue in the realm of device pairing to vehicles. The main issues here are in security of pairing and how to safely authenticate an in-vehicle device to that vehicle. This challenge becomes much harder when the ehicle is moving.	N/A	The authors created a solution that uses a 3-axis accelerameter sensor to determine whether the device in question is the device that should be paired to the vehicle. The solution also has the advantage that the authentication can still occur without a proper UI.	The authors ran the test to see if in a moving vehicle in various driving conditions if the device would pair to the vehicle. The experiment only provided a proof-of-concept, but the experiment showed that the proposed solution is feasible.	Y. S. Kim, "Extended Abstract: Secure and Safe In-Vehicle Device Pairing Using Accelerometer Sensor," 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1-2, doi: 10.1109/VTCFall.2019.8891603.	@INPROCEEDINGS{8891603, author={Kim, Yu Seung}, booktitle={2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)}, title={Extended Abstract: Secure and Safe In-Vehicle Device Pairing Using Accelerometer Sensor}, year={2019}, volume={}, number={}, pages={1-2}, doi={10.1109/VTCFall.2019.8891603}}	https://ieeexplore.ieee.org/abstract/document/8891603	This specific paper only focused on pairing a mobile phone to the vehicle, but can generalize to IoT devices without a proper UI.
	Edwin Liu	Secure and anonymous authentication scheme for the Internet of Things with pairing https://www.sciencedirect.com/science/article/pii/S1574119220300572	Approved. Close related	Hsiao Ling Wu, Chin, Chen Chang, Long Sheng Chen	Authentication, Internet of Things, Bilinear pairing	The Internet of Things technology allows devices automatically connect with others or a server for the purposes of exchanging data. People can conveniently integrate data from those devices for a smart home, vehicular ad-hoc network, e-Health, etc. In 2017, Wang et al. proposed a simple authentication scheme for the Internet of Things. Although they formally proved that their scheme is secure, they did not consider the privacy of devices and stolen verifier attack. In this paper, we first demonstrate the weaknesses of Wang et al.'s scheme. Accordingly, we present a higher security level authentication scheme to resist the above weaknesses.	Pervasive and Mobile Computing 67 (2020) 101177	N/A	2020	Although the Internet of Things has brought convenience to people, according to the ENISA Threat Situation Report, the Internet of Things botnet was considered to be the second-largest threat in 2017. More and more hackers are trying to invade Internet of Things devices to gain unlawful profit. Therefore, mutual authentication in the Internet of Things is an important security issue.	Wang et al.'s scheme is based on Kalra and Sood's scheme and Chang et al.'s scheme.	The solution proposed is an ECC-based authentication scheme for an IoT system and cloud. There are two elements in our scheme, i.e., a server and devices. A device performs the registration phase to obtain the secret authentication token when this device joins this system for the first time. After the device obtains the secret authentication token, it can perform the authentication phase with the cloud server in order to construct a secure communication channel. We assume that the cloud server S chooses a random number x as it's private key to compute master secret key and public key . Then, the cloud server S keeps (x,) and publishes (, , h(.), H(.), e(,)), where h(.) and H(.) are one-way hash functions, and e(,) is a bilinear paring function. The notations and the flowchart of our proposed scheme are presented are two parts: the embedded device and the cloud server. The sender sends the message to the receiver by the direction of the arrow. After the authentication phase, the embedded device and the cloud server will share a common session key.	The registration phase - A device sends its unique identity to the cloud server S through the secure channel. When the cloud server S receives it, S first checks whether this identity is registered or not. If this identity is used, this process will be terminated; otherwise, the cloud server S will use its private key to compute X. Subsequently, the cloud server S will send the device's secret value and the expiry time EXP_Time to the device, and then store into its database. When the device receives and EXP_Time, it stores them in its memory. The authentication phase - When the device collects data from the environment and wants to upload those data to the cloud server S, the device needs to authenticate with the cloud server.	Hsiao-Ling Wu, Chin-Chen Chang, Long-Sheng Chen, Secure and anonymous authentication scheme for the Internet of Things with pairing, Pervasive and Mobile Computing, Volume 67, 2020, 101177, ISSN 1574-1192, https://doi.org/10.1016/j.pmcj.2020.101177. https://www.sciencedirect.com/science/article/pii/S1574119220300572)	@article{WU2020101177, title = {Secure and anonymous authentication scheme for the Internet of Things with pairing}, journal = {Pervasive and Mobile Computing}, volume = {67}, pages = {101177}, year = {2020}, issn = {1574-1192}, doi = {https://doi.org/10.1016/j.pmcj.2020.101177}, url = {https://www.sciencedirect.com/science/article/pii/S1574119220300572}, author = {Hsiao-Ling Wu and Chin-Chen Chang and Long-Sheng Chen}, keywords = {Authentication, Internet of Things, Bilinear pairing}, abstract = {The Internet of Things technology allows devices automatically connect with others or a server for the purposes of exchanging data. People can conveniently integrate data from those devices for a smart home, vehicular ad-hoc network, e-Health, etc. In 2017, Wang et al. proposed a simple authentication scheme for the Internet of Things. Although they formally proved that their scheme is secure, they did not consider the privacy of devices and stolen verifier attack. In this paper, we first demonstrate the weaknesses of Wang et al.'s scheme. Accordingly, we present a higher security level authentication scheme to resist the above weaknesses.}}	https://www.sciencedirect.com/science/article/pii/S1574119220300572#section-cited-by	
	Alison Nakai-Lackey	Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT	Approved	R. Vinoth; Lazarus Jegatha Deborah; Pandi Vijayakumar; Neeraj Kumar	Sensors, Authentication, Biometrics (access control), Cryptography, Internet of Things, Production	The application of Internet of Things (IoT) has generally penetrated into people's life and become popular in recent years. The IoT devices with different functions are integrated and applied to various domains, such as E-health, smart home, Industrial IoT (IIoT), and smart farming. IIoT obtains the general attention among these domains, which allows the authorized user remotely access and control the sensing devices. The user suffices to attain the real-time data collected by sensing devices during the process of production. However, these data is usually transmitted via an insecure channel, which brings the problem of the security and privacy arising from the hostile attacks in IIoT. To resist the hostile attacks by the adversary and protect the security of the transmitted data, we propose a secure multifactor authenticated key agreement scheme for IIoT to support the authorized user remotely accessing the sensing device. The scheme adopts password, biometrics, and smart card to identify the user in the IIoT environment. We employ the secret-sharing technology and Chinese remainder theorem to construct a group key among legitimate sensing devices, and then this group key is utilized to assist in negotiating a secure session key between the user and multiple sensing devices. The proposed scheme is suitable for the resource-constrained IIoT as it only uses hash function, bitwise XOR operation, and symmetric cryptography. The performance analysis indicates that our scheme has less communication and computational costs in contrast to other correlative schemes. Besides, the security analysis indicates that our scheme can withstand many known attacks.	IEEE Internet of Things Journal	N/A	2021	To resist the hostile attacks by the adversary and protect the security of the transmitted data, we propose a secure multifactor authenticated key agreement scheme for IIoT to support the authorized user remotely accessing the sensing device. The scheme adopts password, biometrics, and smart card to identify the user in the IIoT environment. We employ the secret-sharing technology and Chinese remainder theorem to construct a group key among legitimate sensing devices, and then this group key is utilized to assist in negotiating a secure session key between the user and multiple sensing devices. The proposed scheme is suitable for the resource-constrained IIoT as it only uses hash function, bitwise XOR operation, and symmetric cryptography.	Fuzzy Extractor, Access Structure,	To resist the hostile attacks by the adversary and protect the security of the transmitted data, we propose a secure multifactor authenticated key agreement scheme for IIoT to support the authorized user remotely accessing the sensing device	This is another theoretical authentication scheme, so the proposed solutions are mathematically based and do not have "real world" experiments associated.	R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar, "Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3801-3811, 1 March1, 2021, doi: 10.1109 /JIOT.2020.3024703.	@ARTICLE{9199812, author={Vinoth, R. and Deborah, Lazarus Jegatha and Vijayakumar, Pandi and Kumar, Neeraj}, journal={IEEE Internet of Things Journal}, title={Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT}, year={2021}, volume={8}, number={5}, pages={3801-3811}, doi={10.1109/JIOT.2020.3024703}}	https://ieeexplore.ieee.org/abstract/document/9199812	For research papers on MFA, it seems there's more a plethora on theoretical/novel autheticationt techniques, so this is yet another one of them. Good to check out, but because it's so math-heavy it'll be a little difficult to really evaluate clearly.
	Andrea Pallotta	Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes	Approved	Sungjin Yu, Namsu Jho, Youngho Park	Security, Smart homes, Authentication, Smart devices, Protocols, Elliptic curve cryptography, Password	Smart homes are an emerging paradigm of Internet of Things (IoT) in which users can remotely control various home devices via the internet anytime and anywhere. However, smart home environments are vulnerable to security attacks because an attacker can inject, insert, intercept, delete, and modify transmitted messages over an insecure channel. Thus, secure and lightweight authentication protocols are essential to ensure useful services in smart home environments. In 2021, Kaur and Kumar presented a two-factor based user authentication protocol for smart homes using elliptic curve cryptosystems (ECC). Unfortunately, we demonstrate that their scheme cannot resist security attacks such as impersonation and session key disclosure attacks, and also ensure secure user authentication. Moreover, their scheme is not suitable in smart home environments because it utilizes public-key cryptosystems such as ECC. Hence, we design a secure and lightweight three-factor based privacy-preserving authentication scheme for IoT-enabled smart home environments to overcome the security problems of Kaur and Kumar's protocol. We prove the security of the proposed scheme by using informal and formal security analyses such as the ROR model and AVISPA simulation. In addition, we compare the performance and security features between the proposed scheme and related schemes. The proposed scheme better provides security and efficiency compared with the previous schemes and is more suitable than previous schemes for IoT-enabled smart home environments.	IEEE Access (Volume: 9)	Not found on conference portal. IEEE seems to have A*-B scores	2021	As smart home devices are becoming more popular in the modern age, security and privacy must be taken into consideration as it can cause innumerable damages to the user. In 2019, Shuai et al. proposed a two-factor anonymous authentication scheme for smart home environment. Two years later, Kaur and Kumar, through a cryptanalysis of the aformentioned algorithm, pointed out security flaws with it and suggested improvements. However, even with the additional improvements, the authentication scheme is still vulnerable to impersonation, session key disclosure attacks, and also cannot provide mutual authentication. Additionally Kaur and Kumar's enhanced authentication scheme is not suitable for resource-limited IoT devices.	Shuai et al.'s two-factor based anonymous authentication protocol for smart homes, ECC, Kaur and Kumar's improved two-factor based anonymous authentication protocol for smart homes.	The authors propose a secure and lightweight three-factor authentication scheme that aims to protect the user's privacy. This scheme is based off Kaur and Kumar's scheme and it utilizes the fuzzy extractor mechanism to improve the existing two-factor authentication algorithm, so that even if only one of the three authentication factors are compromised, the scheme is still secure. Additionally, the authors' proposed scheme uses XOR and hash functions to reduce the computational overhead of Shuai et al.'s algorithm and to make it suitable for resource-limited devices, which are commonly used in the IoT industry.	The proposed authentication scheme is implemented in three phases: 1. Initialization Phase: the Registration Authority (RA) generates a master key and stores it in the tamper-resistant memory of the Gateway (GW). The smart device chooses an identity token and sends it to RA, which checks it and, if it is correct, stores it in the tamper-resistant memory of the Gateway. Finally, RA generates a master key for the smart device and stores it in the device's tamper-resistant memory. 2. Registration Phase: The user registers with RA to access the start device. Then the smart device interacts with RA to provide the home services. 3. Mutual Authentication Phase:The user and the smart device use the Gateway to establish a common session key, Once the session key is establishes, a secure channel between the user and the smart device is created and the user can access the home services. Additionally, there is an extra phase, during which the user is able to update their old password or biometrics.	S. Yu, N. Jho and Y. Park, "Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes," in IEEE Access, vol. 9, pp. 126186-126197, 2021, doi: 10.1109/ACCESS.2021.3111443.	@ARTICLE{9531969, author={Yu, Sungjin and Jho, Namsu and Park, Youngho}, journal={IEEE Access}, title={Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes}, year={2021}, volume={9}, number={}, pages={126186-126197}, doi={10.1109/ACCESS.2021.3111443}}	https://ieeexplore.ieee.org/document/9531969	As a smart-home device owner, I found this article really interesting as it goes throguh finding flaws in an existing security mechanism and propose an enhanced scheme that protects from the mentioned attacks. The comparisons between the proposed scheme and the existing one in terms of security and efficiency is very easy to understand

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
6	Niklas Bernardo Correa	FMS-AMS: Secure Proximity-based Authentication for Wireless Access in Internet of Things		Jeongyoon Heo, Yongjae Yoo, Jihwan Suh, Woojin Park, Jeongyeup Paek, and Saewoong Bahk	IEEE 802.11n, proximity-based authentication, security, wireless, authentication	Proximity-based authentication enables wireless access points (AP) to allow connection only to devices within a certain authentication range. This would be very convenient for allowing network access only to those within a physical boundary. However, an attacker not within the authentication range may deceive the AP into authenticating its proximity by eavesdropping with higher receiver gain and increasing its transmit power. This can be done easily using an amplifier or a directional antenna. To address this challenge, we propose 'Fixed MCS SNR (FMS)' filtering scheme based on the intuition that high MCS requires high SNR, and amplifying the received signal strength does not necessarily improve SNR. We experimentally show that this is true in reality, and our real-world evaluation in various environments (14 locations) shows that FMS scheme prevents 'amplifier attacks' in all cases. To further counter the false positives of FMS against 'directional antenna attacks' (avg. 35.7%), we also propose 'Authentication Motion with Signal strength gap (AMS)' filtering scheme which defends against both attacks in all cases at the cost of requiring the user to make a simple motion. FMS or AMS scheme can be selected according to the application requirement to enhance the security of proximity-based authentication in upcoming IoT.	JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 22, NO. 4	C	2020	quiring user's motion at a close distance. The contributions of this work are as follows. • We study two potential attacks in proximity-based authentication: 'amplifier attack' and 'directional antenna attack', and experimentally show that they both are feasible and plausible attacks. • We propose two schemes, 'FMS' and 'AMS', which use wireless signal characteristics to defeat the attacks. • We implement proof-of-concept prototypes of our proposals on COTS IEEE 802.11n devices, and evaluate them through extensive real-world experiments in various environments to show their effectiveness.	* Received Signal Strength (RSS) * RSSI Gap * WINNER-II Channel * Signal-to-Noise Ratio (SNR) * Bit-error-rate of modulation and coding scheme (BER of MCS)	* Fixed MCS with SNR based filtering scheme' (FMS scheme). FMS scheme is based on the intuition that typical amplifiers improve only the RSS but not SNR (signal-to-noise ratio) when receiving signals, and the BER (bit error rate) of MCS (modulation and coding scheme) is dependent on SNR not RSS. Said differently, an amplifier amplifies the noise component as well in addition to the intended received signal, which does not improve SNR. Since high MCS requires high SNR and SNR decreases with physical distance, an amplifier attacker not within proximity is unable to decode high MCS packets due to low SNR despite high RSS. Then, by fixing the MCS level high for authentication (temporarily disabling automatic MCS adaptation and keeping the MCS level high), the AP can infer whether the device is within proximity or not. * Authentication Motion with Signal strength gap (AMS) filtering scheme. AMS utilizes temporal change and spatial difference of RSS over time and over two antennas when a user makes a simple authentication motion that moves his/her device from one antenna to another. It is based on the idea that this motion (and resulting RSS change and difference) is difficult for an attacker to mimic from a distance.	* FMS: we performed a preliminary experiment using three devices with varying distances (Fig. 6); (1) one with a 5 dBi dipole antenna (legitimate device), (2) with a 5 dBi dipole antenna and an 11 dB receive gain amplifier (amplifier attacker), and (3) with a 24 dBi directional antenna (directional antenna attacker), respectively. In each case, we measured the maximum available MCS level with respect to RSSI measured by the device in line-of-sight with the AP with varying distances. We define the maximum available MCS as the maximum MCS level at which the device successfully decodes more than 90% of the received packets. To determine the proper transmit power, we follow the WINNER-II channel model [26] which provides a path loss model suitable for office environments. Based on this principle, we can choose an appropriate transmitpower of the AP depending on the environment. * AMS: When a device to be authenticated sends an authentication request message (e.g., as part of the connection establishment phase), the AP responds to initiate authentication. Then the device sends packets continuously to the AP (until authentication timeout period, 2 seconds in our prototype) during which the user can make a motion. The AP measures the RSSI of signals received from each antenna and calculates the RSSI gap (i.e., GAP1→2) between the two antennas. A simple moving average technique is utilized to suppress minor RSSI fluctuation. The authentication timeout period can be adjusted based on the application requirement; increasing it provides more convenience to the user, but also more chances to the attacker at the same time.	*Heo, J., Yoo, Y., Suh, J., Park, W., Paek, J., & Bahk, S. (2020). FMS-AMS: Secure Proximity-based Authentication for Wireless Access in Internet of Things. Journal of Communications and Networks, 22(4), 338–347. https://doi.org/10.23919/jcn.2020.100045*	@article{ heo_yoo_suh_park_paek_bahk_2020, title={FMS-AMS: Secure Proximity-based Authentication for Wireless Access in Internet of Things}, volume={22}, DOI={10.23919/jcn.2020.100045}, number={4}, journal={Journal of Communications and Networks}, author={ Heo, Jeongyoon and Yoo, Yongjae and Suh, Jihwan and Park, Woojin and Paek, Jeongyeup and Bahk, Saewoong}, year={2020}, month={Aug}, pages={338–347}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152596	Interesting that instead of developing one solution to all proposed problems, two were provided that tackle different situtions. Compared to Move2Auth, the combination of solutions does not require any of the devices to have additional specialized hardware and thus can be applied to Commercial-off-the-shelf (COTS) devices. The solution directly involves the AP in authentication and has it actively modify certain parameters that an attacker cannot control.
7	Sarah Dill	An Overview of Practical Attacks on BLE Based IOT Devices and Their Security	OK, but may not be such closely related work	Sode Pallavi, V Anantha Narayanan	BLE, IOT, Wireless, Security, MITM, pairing methods	BLE is used to transmit and receive data between sensors and devices. Most of the IOT devices employ BLE for wireless communication because it suits their requirements such as less energy constraints. The major security vulnerabilities in BLE protocol can be used by attacker to perform MITM attacks and hence violating confidentiality and integrity of data. Although BLE 4.2 prevents most of the attacks by employing elliptic-curve diffie-Hellman to generate LTK and encrypt the data, still there are many devices in the market that are using BLE 4.0, 4.1 which are vulnerable to attacks. This paper shows the simple demonstration of possible attacks on BLE devices that use various existing tools to perform spoofing, MITM and firmware attacks. We also discussed the security, privacy and its importance in BLE devices.	2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)	Not found on conference portal. IEEE seems to have A*-B score mostly	2019	The paper addresses BLE as an alternative to other protocols that use more energy. It addresses pairing methods, attacks, and precautions.	N/A	BLE is widely used, but it needs security enhancements and better implementation in order to have better security.	1) By manufacturers: Ensure that the device is connecting to the official intended application by using fingerprints. Prevent the devices from connecting to the malicious apps. Employ integrity checks before updating the firmware. The firmware should be updated only when there is an official update. Do not allow the user to downgrade or use the older firmware versions. Educate the user about security and privacy. 2) By Users: Use the devices that provide strong authentication. Do not install and use malicious applications for the devices that contains sensitive data. Wearables have less authentication. The attacker can send false connection request to the device to confuse. Hence ensure the connection and authenticate only if you are the one, sending the pairing request.	*S. Pallavi and V. A. Narayanan, "An Overview of Practical Attacks on BLE Based IOT Devices and Their Security," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), 2019, pp. 694-698, doi: 10.1109/ICACCS.2019.8728448.*	@INPROCEEDINGS{8728448, author={Pallavi, Sode and Narayanan, V Anantha}, booktitle={2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)}, title={An Overview of Practical Attacks on BLE Based IOT Devices and Their Security}, year={2019}, volume={}, number={}, pages={694-698}, doi={10.1109/ICACCS.2019.8728448}}	https://ieeexplore.ieee.org/abstract/document/8728448	Offers BLE as an alternative pairing mechanism to Bluetooth.
	Edwin Liu	https://link.springer.com/article/10.1007/s11277-019-06869-y	Approved	Mohammad Nikravan, Akram Reza	Internet of things, Security management, User authentication, Key agreement, Biometrics, Digital signatures	The Internet of Things (IoT) presents a new paradigm of the future internet that intends to provide interactive communication between various processing object via heterogeneous networks. By increasing the IoT usage, establishing the security of IoT becomes a big concern. One of the security related issues is user authentication; that means before a user can access to the IoT nodes, the user and IoT node must authenticate each other. In this paper, a multi-factor user authentication and key agreement protocol, with reasonable computational time, applicable for IoT environments is proposed. To gain access to the services provided by IoT nodes, first, the gateway must authenticate the user and then, with help of the gateway, the IoT node can authenticate the user. The proposed protocol uses elliptic curve cryptography (ECC) and provides: (1) mutual authentication between the user and IOT node; (2) fresh shared session key; (3) multi-factor authentication; (4) several security requirements (i.e., non-repudiation, anonymity and untraceability, etc.). Formal verification of the proposed protocol using Burrows–Abadi–Needham logic shows that the protocol achieves the desired goals. Protocol simulation using Internet Security Protocols and Applications tool proves the security and robustness of the proposed protocol against well-known attacks. Finally, comparing the proposed protocol with other protocols shows that it is efficient in terms of computational time.	Wireless Personal Communications (2020)	C	2019	By increasing the IoT usage, establishing the security of IoT becomes a big concern. One of the security related issues is user authentication; that means before a user can access to the IoT nodes, the user and IoT node must authenticate each other.	Elliptic curve cryptography (ECC), Burrows–Abadi–Needham logic, machine-to-machine communications (M2M), wireless sensor networks (WSN), radio-frequency identifcation (RFID), and low power wireless personal area networks (LoWPAN)	The proposed protocol provides mutual authentication, session key agreement, non-repudiation using digital signature properties, user anonymity, untraceability and other security requirements. The used digital signature scheme is cerifcateless and without key-escrow problem. To lighten the weight of authentication process in the IoT node and smart device of user, the gateway is used and a part of authentication process is delegated to it. In addition, none of the user important information such as identity ID, password, and biometric key is stored in the smart device, and the protocol is resistant against storage and smart device stolen vulnerabilities. Therefore, it is suitable for resource-limited environments such as IoT and WSNs.	1. System Initialization Phase 2. User registration 3. Node Registration 4. User login 5. User Authentication 6. Access to device	Nikravan, M., Reza, A. A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things. Wireless Pers Commun 111, 463–494 (2020). https://doi.org/10.1007/s11277-019-06869-y		https://link.springer.com/article/10.1007/s11277-019-06869-y#citeas	Cant seem to find the BibTex reference
	Alison Nakai-Lackey	Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT	Approved	Jason M. McGinthy; Lauren J. Wong; Alan J. Michaels	Artificial neural networks, Protocols, Authentication, Internet of Things, Performance evaluation, Radio frequency	Trust is a prominent concern with the continued expansion of the Internet of Things (IoT). As new devices enter the market, device security must be a design pillar. In order to trust these devices, they must be identifiable and authenticated before they begin transmitting possible sensitive information, and given the vast number of IoT devices in the future, it may prove difficult to properly trust and authenticate these authorized devices on networks with current methods. Machine learning neural networks (NNs) have the ability to uniquely identify transmitters based on their physical waveform characteristics which could be used to identify and authenticate IoT nodes in large networks with little impact to latency, providing an extra layer of security and trust. This paper presents the groundwork for performing NN-based specific emitter identification (SEI) on resource constrained IoT devices using only raw in-phase and quadrature (IQ) streams, with protocols to secure IoT networks. As proof of concept, an existing NN-based SEI algorithm is executed on both a resource-rich and a more resource-constrained device with low latency, demonstrating the feasibility of using such algorithms on IoT devices now and in the future.	IEEE Internet of Things Journal (Volume: 6, Issue: 1, February 2019)	N/A	2019	Using NN-based techniques to help identify and authenticate IoT using their RF fingerprints is particularly promising as such an approach reduces the need for human oversight. More specifically, an NN approach to device authentication can operate on the incoming raw in-phase and quadrature (IQ) data, eliminating the use of a priori-determined, expert-defined features often used. This makes the approach more flexible and robust because feature extraction techniques are often only accurate over a limited parameter range, can be heavily effected by channel conditions, and can be inconsistent.	IOT Security (Bluetooth, ZigBee, Long Range WAN, IEEE 802.11p), Multifactor Authentication (RF Fingerprinting, Physically Unclonable Features)	This paper presents the groundwork for performing NN-based specific emitter identification (SEI) on resource constrained IoT devices using only raw in-phase and quadrature (IQ) streams, with protocols to secure IoT networks. As proof of concept, an existing NN-based SEI algorithm is executed on both a resource-rich and a more resource-constrained device with low latency, demonstrating the feasibility of using such algorithms on IoT devices now and in the future.	Implemented in Python using the Keras and Tensorflow libraries, on both a resource-rich quad-core Intel CPU and a more resource constrained Raspberry Pi Zero, implementing the considered algorithm on the most resource-constrained devices, such as an MSP430FR5994, is not currently possible, nor is it likely to be possible in the near future	J. M. McGinthy, L. J. Wong and A. J. Michaels, "Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6429-6440, Aug. 2019, doi: 10.1109/JIOT.2019.2908759.	@ARTICLE{8681154, author={McGinthy, Jason M. and Wong, Lauren J. and Michaels, Alan J.}, journal={IEEE Internet of Things Journal}, title={Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT}, year={2019}, volume={6}, number={4}, pages={6429-6440}, doi={10.1109/JIOT.2019.2908759}}	https://ieeexplore.ieee.org/abstract/document/8681154/keywords#keywords	
	Andrea Pallotta	You Walk, We Authenticate: Lightweight Seamless Authentication Based on Gait in Wearable IoT Systems	Approved!	Pratik Musale, Duin Baek, Nuwan Werellagama, Simon S. Woo, Bong Jun Choi	Authentication, Feature extraction, Smart phones, Password, Legged locomotion, Accelerometers	With a plethora of wearable IoT devices available today, we can easily monitor human activities, many of which are unconscious or subconscious. Interestingly, some of these activities exhibit distinct patterns for each individual, which can provide an opportunity to extract useful features for user authentication. Among those activities, walking is one of the most rudimentary and mundane activity. Considering each individual's unique walking pattern, gait, which is the pattern of limb movements during locomotion, can be utilized as a biometric feature for user authentication. In this paper, we propose a lightweight seamless authentication framework based on gait (LiSA-G) that can authenticate and identify users on the widely available commercial smartwatches. Unlike the existing works, our proposed framework extracts not only the statistical features but also the human-action-related features from the collected sensor data in order to more accurately and efficiently reveal distinct patterns. Our experimental results show that our framework achieves a higher authentication accuracy (i.e., an average equal error rate (EER) of 8.2%) in comparison with the existing works while requiring fewer features and less amount of sensor data. This makes our framework more practical and rapidly deployable in the wearable IoT systems with limited computing power and energy capacity.	IEEE Access (Volume: 7)	B*	2019	Walking is one of the most rudimentary and mundane activities and as such, we can easily extra information, unique to each individual, about their walking pattern: the gait, which can be then used as the fundamental principle for a new type of authentication scheme. However, due to lack of security measures in wearable IoT devices, their are more prone to cyber attacks and existing authentication mechanisms have not kept pace with the exponential growth and popularity of the devices. Therefore, as proven by different prior papers, existing authentication schemes are vulnerable to attacks that can put the user's privacy at risk.	Hanamsager et al's password habits study, Prigg et al's Google Glass security vulnerability, Muaaz and Mayrhofer's gait-based authentication, Cola et al's gait-based authentication, Zhao et al's touch-based authenticaton, Terada et al's gait-based authentication performance study.	To eliminate flaws in previous authentication mechanisms, such as high computing powers and time-consuming authentication process, the paper proposes LiSA-G, a gait-based seamless lightweight authentication scheme that securely authenticates users without extra computational overhead. Unlike previously proposed gait-based authentication schemes, LiSA-G: 1. uses both human-action-related features and statistical ones to increase the authentication accuracy; 2. reduces the number of features used for authentication in order to speed up the process without loss of accuracy; 3. eliminates the gait cycle detection to reduce the authentication time.	LiSA-G first extracts both statistical features and mechanical/physical ones: mean, standard deviation, skewness, kurtosis, correlation, Euler angles (pitch, roll, and yam), and force. Once ethe feature extraction process is complete, LiSA-G authenticates users by applying supervised machine learning algorithm to the feature dataset. The authentication system per se is a multi-class classification and requires the machine learning algorithm to be trained in order to minimize the classification error. The experiment uses a Motorola 360 Sport 2 smartwatch and a Motorola G4 plus smartphone to collect the sensor data for 51 volunteers. The experient consists of two phases: 1. Training Phase: LiSA-G trains the machine-learning classifier with the training feature matrix and the training label vector. 2. LiSA-G predicts the classes of the test feature matrix using the classifier from the training phase.	P. Musale, D. Baek, N. Werellagama, S. S. Woo and B. J. Choi, "You Walk, We Authenticate: Lightweight Seamless Authentication Based on Gait in Wearable IoT Systems," in IEEE Access, vol. 7, pp. 37883-37895, 2019, doi: 10.1109/ACCESS.2019.2906663.	@ARTICLE{8672772, author={Musale, Pratik and Baek, Duin and Werellagama, Nuwan and Woo, Simon S. and Choi, Bong Jun}, journal={IEEE Access}, title={You Walk, We Authenticate: Lightweight Seamless Authentication Based on Gait in Wearable IoT Systems}, year={2019}, volume={7}, number={}, pages={37883-37895}, doi={10.1109/ACCESS.2019.2906663}}	https://ieeexplore.ieee.org/document/8672772	As wearable devices are becoming more and more popular, new authentication schemes are being proposed. These authentication schemes differ from the more established ones (fingerprint, face, iris) as they are based human actions, like gait) instead of static features.
	Niklas Bernardo Correa	Iris Recognition Using Multi-Algorithmic Approaches for Cognitive Internet of things (CIoT) Framework		RamadanGad, Muhammad Talha, Ahmed A. AbdEl-Latif, M. Zorkany, Ayman EL-SAYED, NawalEL-Fishawy, Ghulam Muhammad	Biometrics Iris recognition Cognitive Internet of things Delta-mean Multi-algorithm-mean	The recent widespread development of connected sensors, cloud, big data analytics, and ubiquitous sensing technologies have facilitated cognitive Internet of things (CIoT) and its emerging applications. Although CIoT has a great potential to affect human life, scholars have not explored how biometric technologies (e.g., iris) can contribute toward the success of CIoT-oriented framework, where irisbased biometric recognition is used for verification or authentication. One of the trade-offs of biometric recognition designs is to choose a unimodal- or multimodal-based structure. In this study, an iris-based recognition technology was developed as a unimodal biometric with the aid of multi-biometric scenarios. In the segmentation phase, a new algorithm based on masking technique to localize iris was proposed. Two new algorithms, namely, delta-mean and multi-algorithm-mean, were developed to extract iris feature vectors. The proposed system was evaluated on CASIA v. 1, CASIA v. 4-Interval, UBIRIS v. 1, and SDUMLA-HMT. Results show the satisfactory performance of the proposed solution for authentication issues.	Future Generation Computer Systems	A	2018	Iris occlusion and localization considerations are some of the major factors that affect the quality of an iris image and iris template generation. In general, building an overall iris recognition system – as an authentication solution – is complex, computationally exhaustive and time consuming, and the system has moderate accuracy. This study presents and implements new algorithms to gain a robust and accurate system. Multi-biometric scenarios were suggested as a principal of the solution. The proposed method uses iris as unimodal biometrics with the aid of multi-biometric scenarios and not the multimodal scheme.	* MQTT protocol * Euclidean Distance Classifer * Delta Mean * Multi-Algorithm Mean	* Replace username/password in CONNECT packet of MQTT protocol with iris information. The proposed system consists of the following main parts: MQTT client, broker server, communication protocol, and cloud and big data servers (authorization server). The first three parts are the standard MQTT CIoT platform, whereas the fourth part is added to the CIoT platform to increase security of IoT applications based on iris recognition technique. The MQTT broker server can validate the access by communicating with cloud and big data servers. The iris recognition model is divided into the following phases: iris pre-processing (includes segmentation, localization, and normalization), feature extraction, and template matching. An iris database must be utilized for all clients to initiate CIoT platform. To implement the database, multiple iris images must be taken for each client to increase the accuracy of the system. Initially, the enrollment process forms the system database. It contains the features of all enrolled persons.Then, the recognition system may operate in a verification mode and/or identification mode. It depends on the particular application.	* Iris Image Pre-processing + Corneal and specular reflection removal: sequence of morphological operations, aiming at accurate and fast interpolation of corneal reflection + Pupil Detection: Adaptive local threshold (ALT) algorithm depending on mean filter is used to filter bright pixels in the output image. The pupil region mask is multiplied again in the original image to segment the iris region free of artifacts without deformation. + Proposed modified masking technique (MMT): 1) Mask generation, 2) Iris parts detection, 3) Eyelid detection, 4) Extract iris, 5) Normalize iris * Feature Extraction + Delta-Mean (DM) feature extractor: To decrease the number of pixels in the feature vector, the changes in pixel values should be held; the location of each homogeneous segment of pixels should be calculated. It should have the same meaning as the little change may be assumed as the average pixel value. A small segment size is more equivalent to the real pixel values. This method is called DM for future use. In this method, the normalized iris is divided into segments. Then, the statistical mean of each segment is calculated. Hence, the difference between the segments is fused for each row and for each column. A feature vector represents the iris signature code. + Multi -Algorithm-Mean (MAM) feature extractor: multiple different approaches to feature extraction algorithms are applied to a single biometric trait. These systems are more economical as no extra sensor devices are required to capture the data. + Matching and classification phase: To classify the iris templates, the enrolled sample is compared with the others stored in the database. Here, Euclidean distance (ED) [25] is used in feature vector matching of numeric values. As the rotation is not considered in the localization stage, the sample's feature vector shifts left and right to record the minimum value of the matching metric.	Gad, R., Talha, M., El-Latif, A. A., Zorkany, M., EL-SAYED, A., EL-Fishawy, N., &amp; Muhammad, G. (2018). Iris recognition using multi-algorithmic approaches for cognitive internet of things (ciot) framework. Future Generation Computer Systems, 89, 178–191. https://doi.org/10.1016/j.future.2018.06.020	@article{gad_talha_el-latif_zorkany_el-sayed_el-fishawy_muhammad_2018, title={Iris recognition using multi-algorithmic approaches for cognitive internet of things (ciot) framework}, volume={89}, DOI={10.1016/j.future.2018.06.020}, journal={Future Generation Computer Systems}, author={Gad, Ramadan and Talha, Muhammad and El-Latif, Ahmed A. and Zorkany, M. and EL-SAYED, Ayman and EL-Fishawy, Nawal and Muhammad, Ghulam}, year={2018}, pages={178–191}}	https://www.sciencedirect.com/science/article/pii/S0167739X18306915?casa_token=g-ammEW6CCMAAAAA:H6ggKinC9Q3BeNySoRMwS72OTwSvv3PUeAzMaI0oHS5kOzS1WqBUvivwoFUpF5t98H	I found it interesting how the authors managed to re-invent ways of performing expensive tasks such that they became feasible in resource constrained IoT

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
8	Sarah Dill	An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology	Approved, related	Longfei Wu; Xiaojiang Du; Wei Wang; Bin Lin	IoT, Authentication, two-factor authentication, Blockchain, IoT management, security	While the rapid development of IoT devices is changing our daily lives, some particular issues hinder the massive deployment of IoT devices. For example, current network ID management system cannot handle so many new terminals; there is no agreed security standards for IoT manufacturers to follow when designing their products. The whole IoT industry is expecting the breakthrough in network infrastructure and the development of novel security mechanisms that can enable the flexible, secure and reliable access and management of IoT devices. Bitcoin, first released in 2009, breeds the decentralized Blockchain technology. The decentralization, anonymity and proof of security characteristics of Blockchain can prevent collusion and single point failure of a centralized server. We believe that the application of Blockchain into the IoT system can clear the obstacles facing the development of IoT architecture and security. To this end, we propose an out-of-band two-factor authentication scheme for IoT devices based on Blockchain infrastructure. We implemented the IoT and Blockchain integrated system with Eris Blockchain and equivalent computing devices to emulate IoT devices. The overheads to run Blockchain and smart contract services on the emulator devices are measured. The BeagleBone Black and Raspberry Pi 3 nodes have an average memory usage of 29.5M, and the CPU usage of 29.55% and 13.35%, respectively.	2018 International Conference on Computing, Networking and Communications (ICNC)	Not found on conference portal. IEEE seems to have A*-B score mostly	2018	The authors use Blockchain to assist in the authentication of IoT devices due to the properties of Blockchain that prevent historical data from being manipulated and other properties that make it a viable solution.	Blockchain	The authors propose an out-of-band 2FA scheme that is supported by Blockchain technology in order to authenticate IoT devices using current networking and security technologies.	The authors used Beagle Bone Black and Raspberry Pi 3 boards in order to test the methodology. The device profiles are stored in a mapping data structure, which includes data such as the device name, device address, registration date, wireless I/F, and resources. The effectiveness of this was measured through memory and CPU usage.	L. Wu, X. Du, W. Wang and B. Lin, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 769-773, doi: 10.1109 /ICCNC.2018.8390280.	@INPROCEEDINGS{8390280, author={Wu, Longfei and Du, Xiaojiang and Wang, Wei and Lin, Bin}, booktitle={2018 International Conference on Computing, Networking and Communications (ICNC)}, title={An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology}, year={2018}, volume={}, number={}, pages={769-773}, doi={10.1109 /ICCNC.2018.8390280}}	https://ieeexplore.ieee.org/abstract/document/8390280	This article is interesting in that it uses Blockchain technology to assist with IoT device authentication, and it has been proven experimentally successful.
	Edwin Liu	https://link.springer.com/article/10.1007/s10586-021-03444-8 A secure authentication technique for connecting different IoT devices in the smart city infrastructure		Rohit Sharma, Rajeev Arya	Internet of things Secure authentication Security and privacy Smart city	Recently the IoT technology is widely used in the field of smart cities, smart banking, and smart transportation system, etc. Various sensors can be installed in an open environment which allows users to collect the information in an easy way using the internet of things. However, due to the open environment, it’s really difficult to provide security to the communicated information. In this paper, a secure authentication technique is presented for connecting different IoT devices in the smart city infrastructure. This technique shows the legitimacy of IoT sensors (IOi) to the reader (Ri) and Authentication Entity. In this paper, a set of primitives and the cubic equation are used to propose a secure authentication technique. In the proposed technique, an authentication entity is introduced between the IoT sensor and the receiver. The authentication entity will be responsible for performing the authentication process. The proposed authentication technique includes a strong mathematical procedure, which is very complex. The computational cost and Energy cost have also been analyzed and compared with previous techniques. It is providing a secure authentication process for the different IoT sensors, which is useful to start a secure communication with the receiver. The proposed technique offers the best computation and energy cost in comparison with the previous techniques.	Cluster Computing	Either A or C	2021	The major issue in smart cities and IoT is to be secure and safe but every product does not give this guarantee.	RSA method, ECC, Discrete Logarithm Problem (DLP), ID system, cloud-based techniques	The authors have been presented a signature generating technique that is based on SHA-3. A unique hash code has been generated by the sender for the data, which will serve as an authentication token. In the proposed authentication technique, an authentication entity has been assumed between the IoT sensor and the receiver. The introduced authentication entity will be responsible for performing the authentication process before the data transmission. Each and every IoT sensor have to prove their identity with the introduced authentication entity before to the start the data transmission.	Registration at sensor node, Proof of registration process, Authentication process at sensor node, Proof of the authentication process, Authentication process at authentication entity, and proof of correction at authentication entity.	Sharma, R., Arya, R. A secure authentication technique for connecting different IoT devices in the smart city infrastructure. Cluster Comput 25, 2333–2349 (2022). https://doi.org/10.1007/s10586-021-03444-8	N/A	https://link.springer.com/article/10.1007/s10586-021-03444-8	Needs to be approved, there was no bibtext reference
	Alison Nakai-Lackey	Building Low-Interactivity Multifactor Authenticated Key Exchange for Industrial Internet of Things	Approved	Zengpeng Li; Zheng Yang; Pawel Szalachowski; Jianying Zhou	Authentication, Password, Protocols, Servers, Standards	Industrial Internet of Things (IIoT) brings together computers, devices, advanced analytics, and people in industries, such as transportation, oil plant, and power grid that leads to major efficiency and productivity gains for almost any industrial procedures. Due to the interconnection of devices in IIoT, communication security has become a critical issue to address in many emerging industry standards that require the authentication and key exchange procedure to be done to guarantee the authorized machine access (e.g., from users) and secure the data transmission between machines. To overcome the shortcoming (i.e., low entropy) of the memorable password in user authentication, it is rightfully recommended by industry standards (such as IEC-62443 family) to use multifactor authentication (MFA) for higher security levels. Notably, latency is one of the main sources of inefficiency when a device is communicating with other machines on IIoT. To mitigate latency, a smooth projective hash function (SPHF) built from well-studied standard assumptions is used to achieve a lowinteractivity multifactor authenticated key exchange protocol (MFAKE) because SPHF allows each party to prove to the others that he knows the right authentication factor(s). In this article, we are, therefore, motivated to build a new MFAKE named “secure remote multifactor (SRMF)” to achieve the humaninvolved “machine-to-machine” secure communication in IIoT. That is, SRMF leverages multiple user-centric authentication factors (such as password, biometric fingerprints, and PIN), and it can synergistically support multifactor registration (MFR), MFA, and multifactor key exchange (MFKE). Furthermore, to prevent authentication factors stored at the server exposing to attackers, the password-harden service (i.e., Pythia-PRF and USENIX'15) inspires us to develop a multifactor hardening service (MFHS) utilizing an oblivious pseudorandom function (OPRF). The balanced security of the proposed protocol is proved...	IEEE Internet of Things Journal	N/A	2020	To systemize the MFAKE and make it easy to describe, the proposed SRMF protocol integrates with the multifactor registration (MFR) phase while it guarantees the security of multifactor stored at databases. Particularly, the SRMF , as illustrated in Fig. 2, is a secure composable protocol which covers three procedures: 1) human-factor (s) registration; 2) MFA protocol; and 3) MFAKE .	We introduce a new notation of secure remote multifactor (SRMF) protocol for practical use cases and we then improve the process of password authentication and authenticated key exchange for SRMF in the following sections	Various approaches are proposed in succession to mitigate the affection of the compromised password database and the password-cracking, such as [10] and [11]. However, the nature of password-based authentication is without a strong identity check, thus, it is not difficult for attackers to acquire the targeted user’s account because anyone can unlock using passwords.	Once again, this is a proposed theoretical solution, so there's not much practical in the experimental portion. A proof of concept was writtin in C using the GMP library, with a client-side Raspberry Pi used as the IoT device to authenticate.	Z. Li, Z. Yang, P. Szalachowski and J. Zhou, "Building Low-Interactivity Multifactor Authenticated Key Exchange for Industrial Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 844-859, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3008773.	@ARTICLE{9139491, author={Li, Zengpeng and Yang, Zheng and Szalachowski, Pawel and Zhou, Jianying}, journal={IEEE Internet of Things Journal}, title={Building Low-Interactivity Multifactor Authenticated Key Exchange for Industrial Internet of Things}, year={2021}, volume={8}, number={2}, pages={844-859}, doi={10.1109/JIOT.2020.3008773}}	https://ieeexplore.ieee.org/abstract/document/9139491	
	Andrea Pallotta	A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices	Approved	Tarek A. Idriss, Haytham A. Idriss, Magdy A. Bayoumi	Protocols, Authentication, Security, Integrated circuit modeling, Physical unclonable function, Delays, Servers	PUFs, or physical unclonable functions, are hardware security primitives that can offer lightweight security solutions for constrained devices through challenge-response authentication protocols. However, the lightweight PUF-based security solutions that have been presented often lack security features such as mutual authentication or message encryption, which could be vital for many applications. Other protocols suffer from vulnerabilities to denial of service attacks that make them impractical to use. This work introduces a lightweight PUF-based protocol that uses secret pattern recognition to offer mutual authentication and authenticated secret message exchange for constrained devices on the Internet of Things. The protocol utilizes several techniques to introduce nonlinearity, and it can employ any strong PUF circuit for which a soft model can be generated. The authentication process requires simple bitwise operations along with a PUF circuit and a true random number generator (TRNG). By avoiding the use of any cryptographic or hash functions, the protocol's lightweight nature is preserved. The security of the proposed protocol against modeling attacks is tested to showcase its resilience. Similar PUF-based protocols are investigated and found to lack some essential security features.	IEEE Access (Volume: 9)	B*	2021	Existing PUF-based authentication schemes often lack security features, including mutual authentication or messagee encryption, which could offer extra protection for certain devices and applications.	Dilay Arbiter PUF, PUF circuit, true random number generator (TRNG), pseudocryptographic algorithms, machine learning-based attacks	The paper proposes a lightweight PUF-based authentication protocol (LPA) that aimes to improve the system's security by introducing new security measures not found in previous PUF-based authentications schemes. These security measures are: - Mutual authentication based on secret pattern recognition. - Authentication message exchange that offers message encryption and garantees secrecy and origin of the message from and to the device. - Challenge tranformation functions that require a small implementation overhead while protecting the protocol from MITM attacks. According to the security analysis presented by the authors, the protocol is secure against MITM attacks and machine learning-based attacks, such as evolution strategies (ES), artificial neural networks (ANNs), and support vector machines (SVMs).	On the server side, the protocol is software-based. If a device cannot be permanently trusted, the protocol and model can be stored remotely, giving system administrators the ability to modify the devices' access right by revoking access to the remote server. The authentication is divided into three steps: 1. An initialization message and the PUF ID number are exchanged between the "prover" and the "verifier". 2. The transformed challenge exhcange process is performed m times. 3. The verifier checks whether the pattern of the challenge tranformations (step 2) match any of the patterns assigned to the prover device. If the match fails, the authentication fails	T. A. Idriss, H. A. Idriss and M. A. Bayoumi, "A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices," in IEEE Access, vol. 9, pp. 80546-80558, 2021, doi: 10.1109/ACCESS. 2021.3084903.	@ARTICLE{9444356, author={Idriss, Tarek A. and Idriss, Haytham A. and Bayoumi, Magdy A.}, journal={IEEE Access}, title={A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices}, year={2021}, volume={9}, number={}, pages={80546-80558}, doi={10.1109 /ACCESS.2021.3084903}}	https://ieeexplore.ieee.org/document/9444356	This paper is relevant because it introduces a new protocol that, while based on the same concepts as other PUF-based authentication schemes, also takes into consideration novel attacks, such as machine learning-based attacks, which may become more relevant and frequent in the near future
	Niklas Bernardo Correa	A Lightweight Anonymous Authentication Protocol for Resource-Constrained Devices in Internet of Things		Xuyang Ding , Xiaoxiang Wang, Ying Xie , and Fagen Li	Anonymous authentication, Internet of Things (IoT) security, privacy protection, resource-constrained devices	With the rapid development of Internet of Things (IoT) in recent years, the security of IoT becomes more and more prominent. To protect data privacy and device availability, dentity authentication technology has been applied to the IoT environment. However, although scholars have designed a variety of authentication protocols for the IoT environment, the resource costs of these protocols are still expensive for resourceconstrained devices. In particular, when the frequent upgrade of computer hardware has led to a gradual increase in the key length of the cryptosystem, IoT devices are hard to keep up with the upgrade speed because of the balance between cost and tasks. Although the storage space has increased in recent years, the computational and communication capabilities are still limited by some physical factors, such as energy, power, and communication link bandwidth. To improve the situation, this article proposes an anonymous authentication protocol suitable for IoT devices with current hardware performance, which is based on elliptic curve and signcryption techniques. Compared to other protocols, our protocol further reduces the communication and computing cost of the client devices while ensuring security requirements. Thus, we formally prove its theoretical security under the random oracle model and use simulation experiments to verify that the protocol can effectively reduce the resource requirements.	IEEE INTERNET OF THINGS JOURNAL, VOL. 9, NO. 3, FEBRUARY 1, 2022	Not found on conference portal. IEEE seems to have A*-B score mostly	2021	improve the problem that current anonymous authentication protocols are most limited by hardware resource, which leads to the incomplete coverage of security functions. So, we design a lightweight authentication protocol, which can support most of IoT devices for better data security and privacy protection.	* Elliptic-Curve Cryptosystem * Discrete Logarithmic Problem	1) We design a certificateless anonymous authentication protocol scheme after analyzing the existing authentication protocols, which has been proven to prevent attacks disguised as legitimate users. 2) We use few point multiplications on the elliptic curve that consumes a lot of resources, and it has been proved by programming experiments that the computational costs of restricted equipment are effectively reduced. 3) In the authentication stage, the communicating parties completed mutual authentication and session keys generation, even the network management center cannot get the anonymous party’s identity at this moment. In addition, the communication cost of IoT devices is also low.	* Initialization Phase: Network Manager Center (NMC) initializes system parameters pertaning to elliptic curve cryptography * Registration Phase: Device loads public system parameters from NMC, computes an identifier for itself based on its randomly chosen secret value. The device then sends a hash of its identity to the NMC which compares it against its database. Device is legal if there is a match and is rejected otherwise. NMC then randomly selects a prime and computes user's partial private key. Information Center (IC) then authenticates to NMC like the device did. IC stores {user's index, user's identifier, User's partial private key} * Authentication Phase: Mutal authentication of Device and IC. Device sends {ciphertext, temporary data, intermediate message, signauture, timestamp} to IC. IC checks timestamp, then calculates intermediate message, then confusing message, and finally decrypts ciphertext to obtain device index. IC looks for index in database, and if there is a match, obtains the corresponding public key. IC verifies it can reconstruct temporary data and the signature to ensure device is legal. Then a session key is generated along with a MAC and sends it to the device. Device computes session key and verfies MAC.	Ding, X., Wang, X., Xie, Y., &amp; Li, F. (2022). A lightweight anonymous authentication protocol for resource-constrained devices in internet of things. IEEE Internet of Things Journal, 9(3), 1818–1829. https://doi.org/10.1109/jiot.2021.3088641	@article{ding_wang_xie_li_2022, title={A lightweight anonymous authentication protocol for resource-constrained devices in internet of things}, volume={9}, DOI={10.1109/jiot.2021.3088641}, number={3}, journal={IEEE Internet of Things Journal}, author={Ding, Xuyang and Wang, Xiaoxiang and Xie, Ying and Li, Fagen}, year={2022}, pages={1818–1829}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9452132	Authors considered limited device and implemented solution able to provide security assurances under these conditions
	Sarah Dill	An Efficient Leakage-Resilient Authenticated Key Exchange Protocol Suitable for IoT Devices	Approved	An-Li Peng, Yuh-Min Tseng, Sen-Shan Huang	IoT, authentication, Authenticated Key Exchange (AKE), client-server	Authenticated key exchange (AKE) protocol for client–server environments is a significant cryptographic primitive that provides communication confidentiality and mutual authentication between clients and servers. In an Internet of Things (IoT) environment, clients typically employ IoT devices with limited computing capability to interact with servers through the Internet. Numerous AKE protocols suitable for IoT devices, called AKE-IoT protocols, have been proposed. Recently, side-channel attacks have been conducted to defeat traditional cryptographic protocols because a side-channel adversary can retrieve partial content of long-term or short-term secret keys. Several leakage-resilient AKE (LRAKE) protocols were presented to counteract such attacks. Unfortunately, the existing LRAKE protocols are not suitable for IoT devices because expensive pairing operations are required for client sides. In this article, we propose the first efficient LRAKE protocol suitable for IoT devices, named LRAKE-IoT. By the unbalanced computation method, no pairing operation is required for client sides in our protocol. In the generic bilinear pairing group model, security analysis is conducted to demonstrate the security of the proposed protocol in the continuous-leakage-resilient extended-Canetti–Krawczyk model. Finally, computational experiences on two IoT devices are given to show that the proposed protocol is well-suited for IoT devices.	IEEE Systems Journal (Volume: 15, Issue: 4, December 2021)	Not found on conference portal. IEEE seems to have A*-B score mostly	2021	IoT devices are susceptible to side-channel attacks, which is not addressed with current protocols in use (AKE). The authors propose an efficient protocol (leakage-reselient AKE) that addresses this issue that is lightweight enough to be used with IoT devices.	Authenticated key exchange (AKE), cryptography	The proposed LRAKE protocol protects against side-channel attacks. The solution has properties including computation leakage, limited leakage of single computational round, leakage independent, and totally unbounded leakage.	This protocol can be implemented on existing IoT devices. To assist with the computational burden, some of this is moved to a server to help with performance.	A. -L. Peng, Y. -M. Tseng and S. -S. Huang, "An Efficient Leakage-Resilient Authenticated Key Exchange Protocol Suitable for IoT Devices," in IEEE Systems Journal, vol. 15, no. 4, pp. 5343-5354, Dec. 2021, doi: 10.1109/JSYST.2020.3038216.	@ARTICLE{9273255, author={Peng, An-Li and Tseng, Yuh-Min and Huang, Sen-Shan}, journal={IEEE Systems Journal}, title={An Efficient Leakage-Resilient Authenticated Key Exchange Protocol Suitable for IoT Devices}, year={2021}, volume={15}, number={4}, pages={5343-5354}, doi={10.1109/JSYST.2020.3038216}}	https://ieeexplore.ieee.org/abstract/document/9273255	The protocol proposed builds upon an existing protocol and makes improvements on it.
	Edwin Liu	https://ieeexplore.ieee.org/abstract/document/8758847 Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments		Krishnashree Achuthan; Robin Doss; Lei Pan	Authentication, Logic gates, Local area networks, Microprogramming, Random access memory, Cryptography, cryptography, distributed processing, Internet of Things, local area networks, telecommunication network routing, wireless sensor networks, IoT deployments, IoT devices, edge computing device, protean authentication scheme, time-bound dynamic KeyGen authentication technique, IoT edge nodes, lightweight authentication scheme, IoT sensor nodes, wireless sensor network, IoT local area network, IoT LAN, Edge node authentication, IoT authentication, IoT security, time-bound IoT authentication, resource constrained devices	The IoT edge/sensor nodes are exposed to large attack surface and could easily succumb to several well-known attacks in the wireless sensor network (WSN) domain. Authenticating edge nodes before they join a network, especially after a sleep state, is a critical step to maintain the overall trust of any given IoT local area network (IoT LAN). The low resources and computational constraints of such IoT nodes make this a challenging and non-trivial problem. As many IoT deployments are in uncontrolled environments, the IoT devices are often placed in the open so that physical access to them is inevitable. Due to easy physical access of the devices, common attacks, including cloning of devices or stealing secret keys stored in an edge node, are some of the most common attacks on the IoT deployments. This paper focuses on developing an extremely lightweight authentication scheme for constrained end-devices that are part of a given IoT LAN. Authentication occurs between the end-device and the gateway that acts as an edge computing device. The proposed authentication scheme is put through both formal and informal security verification. Voltage drop, current, and power are measured to gauge the overall impact of the security scheme. All the three parameters were measured while configuring the edge node as an end-device or as a router. Our testing results show that the impact on the resources was minimal.	IEEE Access (Volume: 7)	B	2019	Securing IoT deployments in outdoor environments is a genuine challenge especially due to easy physical access to sensor nodes. Devices that can sense environmental parameters and/or can respond to them through wireless communication are qualified to be part of any given IoT LAN. The majority of these devices are sensors that sense and stream data wirelessly to a gateway or directly to a cloud-based application through middleware.	LWC - Lightweight cryptography.	An efficient key generation mechanism, where the authentication credentials are generated on the fly and exchanged securely between the gateway and edge nodes with minimal computational overheads on resource constrained IoT devices. Like many existing authentication schemes, our proposed mechanism does not require storing any static key value on the device. Instead, the keys are dynamically changing and shared securely to prevent message replay and device clone attacks.	1 - Initial Authentication Cycle From the Gateway Sid 2 - Initial Edge Node Auth Acknowledge Cycle 3 - Initial Auth Cycle from Gateway Side 4 - Subsequent Auth Cycles From Gateway to Edge 5 - Subsequent Auth Cycles From Gateway to Edge 6 - Subsequent Auth Confirmation at the Gateway 7 - Subsequent Auth Confirmation at the Gateway	S. Sathyadevan, K. Achuthan, R. Doss and L. Pan, "Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments," in IEEE Access, vol. 7, pp. 92419-92435, 2019, doi: 10.1109 /ACCESS.2019.2927818.	@ARTICLE{8758847, author={Sathyadevan, Shiju and Achuthan, Krishnashree and Doss, Robin and Pan, Lei}, journal={IEEE Access}, title={Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments}, year={2019}, volume={7}, number={}, pages={92419-92435}, doi={10.1109 /ACCESS.2019.2927818}}	https://ieeexplore.ieee.org/abstract/document/8758847/keywords#keywords	Needs to be approved
	Alison Nakai-Lackey	Authentication of IoT Device and IoT Server Using Security Key	Approved	Wael Alnahari; Mohammad Tabrez Quasim	Authentication, Companies, Servers, Internet of Things, Cryptography, Password	IoT is an emerging topic in the field of IT that has attracted the interest of researchers from different parts of the world. Authentication of IoT includes the establishment of a model for controlling access to IoT devices through the internet and other unsecured network platforms. Strong authentication of IoT is necessary for ensuring that machines and devices could be trusted when it comes to data sharing. The whole idea of authentication further prevents cybercriminals from using loopholes in IoT devices to access data that they are not allowed to access. Various authentication techniques could be used to secure IoT servers and devices. Establishing mutual authentication between IoT servers and IoT devices has attracted a lot of research interests because it helps enhance the effectiveness and overall security of data sharing. Therefore, this research provides the basis for analyzing the whole idea of using security keys to encrypt both IoT servers and IoT devices.	2021 International Congress of Advanced Technology and Engineering (ICOTEN)	N/A	2021	The unique ID of IoT servers and IoT devices enables system administrators to track them throughout their lifecycles, establish secure communication with them, and prevent them from executing processes that could be harmful. Should an IoT server or device start to exhibit a behavior that is not expected, the system administrators could revoke their privileges with ease.	Security Keys, Cloud Computing, Authentications, MFA, Weak Passwords,	This study proposes the use of security keys to secure IoT devices against cyberattacks. Therefore, some of the attacks and attackers that have been considered in this work include:	Proof of concept of how MFA can assist in preventing bypassing the use of passwords.General experiments against IoT devices.	W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-9, doi: 10.1109/ICOTEN52080. 2021.9493492.	@INPROCEEDINGS{9493492, author={Alnahari, Wael and Quasim, Mohammad Tabrez}, booktitle={2021 International Congress of Advanced Technology and Engineering (ICOTEN)}, title={Authentication of IoT Device and IoT Server Using Security Key}, year={2021}, volume={}, number={}, pages={1-9}, doi={10.1109/ICOTEN52080. 2021.9493492}}	https://ieeexplore-ieee-org.ezproxy.rit.edu/document/9493492	More discussion based about MFA rather than novel techniques, which I liked.

Alison

Week #	Student name	Paper title	Approved?	Author(s)	Keywords	Abstract	Conference/journals	Ranking/journals ranking http://portal.core.edu.au/conf-ranks/ http://portal.core.edu.au/jnl-ranks/	Year (within 5 years is encouraged)	Research problems/ design goals (You can summarize it from the last few paragraphs in the Introduction or from the section problem formulation)	Preliminary Techniques (Research papers: background knowledge or techniques would be used in the proposed solution. If none, N/A) (Survey papers: list the proposed solutions)	Solution (Research papers: key idea(s) of the proposed solutions. Generally, you can extract from "this paper proposes xxxxx") (Survey papers: how to organize the proposed solutions.)	Experiments (How to implement the proposed solution)	Citation	BibTex Reference	Link (pdf in G-drive)	Notes (why is this article interesting/relevant? anything specifically compelling/worth noting about the writing or display of information? any best practices you want to use/call out?) Any potential important information should be included in the final writing project
9	Andrea Pallotta	Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices	Approved	Sarmadullah Khan, Ahmed Ibrahim Alzahrani, Osama Alfarraj, Nasser Alalwan, Ali H. Al-Bayatti	Authentication, Sensors, Servers, Internet of Things, Elliptic curves, Monitoring	The Internet of Things (IoT) can includes many resource-constrained devices, with most usually needing to securely communicate with their network managers, which are more resource-rich devices in the IoT network. We propose a resource-efficient security scheme that includes authentication of devices with their network managers, authentication between devices on different networks, and an attack-resilient key establishment procedure. Using automated validation with internet security protocols and applications tool-set, we analyse several attack scenarios to determine the security soundness of the proposed solution, and then we evaluate its performance analytically and experimentally. The performance analysis shows that the proposed solution occupies little memory and consumes low energy during the authentication and key generation processes respectively. Moreover, it protects the network from well-known attacks (man-in-the-middle attacks, replay attacks, impersonation attacks, key compromission attacks and denial of service attacks).	IEEE Access (Volume: 7)	B*	2019	The Internet of Things consists of an exponentially increasing amount of devices which can be very different from each others and are often very resource-constrained. The security and privacy of these devices can be very challenging, depending on their deployment environment and how they need to communicate with resource-rich devices, such as computers. Lightweight authentication and key establishment meechanisms based on ECC have been proposed in the past. However, these schemes are based on PKI approches and require central certificate authorities to manage the keys. As a consequence, they do not have a way to protect the system from popular attacks, including man-in-the-middle attacks, impersonation attacks, and Sybil attacks.	Elliptic Curve Cryptography (ECC), intrusion detecion system for v2x networks, NIST Elliptic Curve Digital Signature Algorithm (ECDSA), TinyECC library, Sankar et al.'s Elliptic Curve Diffie Hellman (ECDH) key exchange mechanism, Gura et al's hybrid multiplication technique	The authors propose a new resource efficient authentication scheme that: - Is based on the ECC approach and protects the system from MITM attacks, impersonation attacks, and Sybil attacks. - Reduces the need of a central certification autheority to manage the devices' secret keys. - Introduces a secure communicate procedure that scales well for both resource-constrained devices and large heterogeneous networks. - Introuces a symmetric key establishment procedure to secure session communications. This procedure is suitable for resource-constrained IoT devices as it does not introduce additional computational overhead.	The architecture used to implement the proposed scheme consists of one of more instances of a device that uses a network manager's services. The network manager also provides services to reource-constrained and/or resourceful devices. Finally the architecture contains a truster server that provides trust certificates to the network manager. When two devices want to mutually authenticate each others using their generated set of materials, the authentication process consists of the following steps: 1. The first device sends to its network manager (NM1) a session establishement request with the second device. 2. If possible, NM1 uses the set of material of the second device's network manager (NM1). If the material is unavailable, NM1 and NM2 go through a registration phase. 3. NM1 and NM2 exchange the devices' authentication material. 4. The two network managers then forward the authentication materials to their respective devices. The first device will have the second device's authentication material and vice versa. 5. Both devices generate parts of cipher text C1 and C2 using the other device's authentication material. 6. The two devices exhange the newly generated C1 and C2. 7. Each device extract the nonce from the exchanged C1 and C2. 8. Each device sends back the extracteed nonce after encryption so they can verify each others authenticity.	S. Khan, A. I. Alzahrani, O. Alfarraj, N. Alalwan and A. H. Al-Bayatti, "Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices," in IEEE Access, vol. 7, pp. 170615-170628, 2019, doi: 10.1109/ACCESS. 2019.2955604.	@ARTICLE{8911344, author={Khan, Sarmadullah and Alzahrani, Ahmed Ibrahim and Alfarraj, Osama and Alalwan, Nasser and Al-Bayatti, Ali H.}, journal={IEEE Access}, title= {Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices}, year={2019}, volume={7}, number={}, pages={170615-170628}, doi= {10.1109/ACCESS.2019.2955604}}	https://ieeexplore.ieee.org/document/8911344	What I found interesting about the authentication scheme proposed in this paper is its scalability. As stated by the authors, it does not only target resource-constrained devices, but it can scale to support large networks with many different components. The authors also put emphasis on how the scheme is secure against different types of network attacks.
	Niklas Bernardo Correa	Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing using Different Sensor Types		Jun Han, Albert Jin Chung, Manal Kumar Sinha, Madhumitha Harishankar, Shijia Pan, Hae Young Noh, Pei Zhang, and Patrick Tague		Context-based pairing solutions increase the usability of IoT device pairing by eliminating any human involvement in the pairing process. This is possible by utilizing on-board sensors (with same sensing modalities) to capture a common physical context (e.g., ambient sound via each device's microphone). However, in a smart home scenario, it is impractical to assume that all devices will share a common sensing modality. For example, a motion detector is only equipped with an infrared sensor while Amazon Echo only has microphones. In this paper, we develop a new context-based pairing mechanism called Perceptio that uses time as the common factor across differing sensor types. By focusing on the event timing, rather than the specific event sensor data, Perceptio creates event fingerprints that can be matched across a variety of IoT devices. We propose Perceptio based on the idea that devices co-located within a physically secure boundary (e.g., single family house) can observe more events in common over time, as opposed to devices outside. Devices make use of the observed contextual information to provide entropy for Perceptio's pairing protocol. We design and implement Perceptio, and evaluate its effectiveness as an autonomous secure pairing solution. Our implementation demonstrates the ability to sufficiently distinguish between legitimate devices (placed within the boundary) and attacker devices (placed outside) by imposing a threshold on fingerprint similarity. Perceptio demonstrates an average fingerprint similarity of 94.9% between legitimate devices while even a hypothetical impossibly well-performing attacker yields only 68.9% between itself and a valid device.	2018 IEEE Symposium on Security and Privacy	Not found on conference portal. IEEE seems to have A*-B score mostly	2018	an autonomous context-based pairing protocol, named Perceptio, for IoT devices with heterogeneous sensing types, using a fingerprint mechanism that is robust to signal variation across devices, requires no time synchronization across devices, and needs no prior training phase.	Commercial Smart Home Sensors: Smart Home IoT with on-board sensors with specific capability (microphone, motion detector, ...) Human-in-the-Loop-based Pairing: Pairing schemes that require human intervention Context-based Pairing: Pairing schemes that leverage commonly observed context using on-board sensors.	Perceptio: Use time as a common factor across different sensor types capturing the same events within a security boundary (room in a home) to create a fingerprint that can be matched across many IoT devices. The fingerprint is then used to derive a numerically equivalent shared key that devices can use to encrypt communications.	1) Initialization: Devices discover each other and determine they must pair. 2) Key Agreement: Devices compute, exchange, and verify context fingerprints to establish a symmetric key 3) Key Confirmation: devices verify the correctness of the symmetric key and increment the confidence score if the key is validated 4) Confidence Score Check: devices either declare pairing success if the confidence score is above a certain threshold or repeat from the key agreement phase.	Han, J., Chung, A. J., Sinha, M. K., Harishankar, M., Pan, S., Noh, H. Y., Zhang, P., &amp; Tague, P. (2018). Do you feel what I hear? enabling autonomous IOT device pairing using different sensor types. 2018 IEEE Symposium on Security and Privacy (SP). https://doi.org/10.1109/sp. 2018.00041	@article {han_chung_sinha_harishankar_pan_noh_zhang_tague_2018, title={Do you feel what I hear? enabling autonomous IOT device pairing using different sensor types}, DOI={10.1109/sp. 2018.00041}, journal={2018 IEEE Symposium on Security and Privacy (SP)}, author={Han, Jun and Chung, Albert Jin and Sinha, Manal Kumar and Harishankar, Madhumitha and Pan, Shijia and Noh, Hae Young and Zhang, Pei and Tague, Patrick}, year= {2018}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418641	I liked the idea of using the shared environment as a source of entropy. But it does assume heavily that an attacker's ability to capture signals across the 'security boundary' is limited. I wonder with advances in technology, if attackers would be able to compensate for walls and distance and be able to generate a valid fingerprint. The solution is also not suitable for the cases where the attacker can place his device in the environment, like an office or another public space, which are most scenarios. The authors claim their solution can be adjusted to acomplish this, however.
10	Sarah Dill	Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT	Approved	Meng Shen, Huisen Liu, Liehuang Zhu, Ke Xu, Hongbo Yu, Xiaojiang Du, Mohsen Guizani	IoT, Industrial IoT, Blockchain, Authentication	Industrial Internet of Things (IIoT) is considered as one of the most promising revolutionary technologies to prompt smart manufacturing and increase productivity. With manufacturing being more complicated and sophisticated, an entire manufacturing process usually involves several different administrative IoT domains (e.g., factories). Devices from different domains collaborate on the same task, which raises great security and privacy concerns about device-to-device communications. Existing authentication approaches may result in heavy key management overhead or rely on a trusted third party. Thus, security and privacy issues during communication remain unsolved but imperative. In this paper, we present an efficient block-chain-assisted secure device authentication mechanism BASA for cross-domain IIoT. Specifically, consortium blockchain is introduced to construct trust among different domains. Identity-based signature (IBS) is exploited during the authentication process. To preserve the privacy of devices, we design an identity management mechanism, which can realize that devices being authenticated remain anonymous. Besides, session keys between two parties are negotiated, which can secure the subsequent communications. Extensive experiments have been conducted to show the effectiveness and efficiency of the proposed mechanism.	IEEE Journal on Selected Areas in Communications (Volume: 38, Issue: 5, May 2020)	Not found on conference portal. IEEE seems to have A*-B score mostly	2020	Industrial Internet of Things (IIot) can use blockchain and identity-based cryptography for authentication; however, the combination of both of these has a few issues: revocation of identity, identity privacy-preserving, and storage limitation.	Authentication techniques (Identity-Based Signature, ECDHE, Blockchain	The authors propose a blockchain-assisted authentication mechanism, an identity management method, and a key agreement mechanism.	The authors tested their solution using two admin domains with operations occuring on VMs on the host machines.	M. Shen et al., "Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT," in IEEE Journal on Selected Areas in Communications, vol. 38, no. 5, pp. 942-954, May 2020, doi: 10.1109/JSAC.2020.2980916.	@ARTICLE{9036971, author={Shen, Meng and Liu, Huisen and Zhu, Liehuang and Xu, Ke and Yu, Hongbo and Du, Xiaojiang and Guizani, Mohsen}, journal={IEEE Journal on Selected Areas in Communications}, title={Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT}, year={2020}, volume={38}, number={5}, pages= {942-954}, doi={10.1109/JSAC. 2020.2980916}}	https://ieeexplore.ieee.org/abstract/document/9036971/authors	This paper focuses on Industrial IoT and improves upon existing authentication solutions.
	Edwin Liu	https://ieeexplore.ieee.org/abstract/document/9493492 Authentication of IoT Device and IoT Server Using Security Key		Wael Alnahari, Mohammad Tabrez Quasim	Authentication, Companies, Servers, Internet of Things, Cryptography, Password	IoT is an emerging topic in the field of IT that has attracted the interest of researchers from different parts of the world. Authentication of IoT includes the establishment of a model for controlling access to IoT devices through the internet and other unsecured network platforms. Strong authentication of IoT is necessary for ensuring that machines and devices could be trusted when it comes to data sharing. The whole idea of authentication further prevents cybercriminals from using loopholes in IoT devices to access data that they are not allowed to access. Various authentication techniques could be used to secure IoT servers and devices. Establishing mutual authentication between IoT servers and IoT devices has attracted a lot of research interests because it helps enhance the effectiveness and overall security of data sharing. Therefore, this research provides the basis for analyzing the whole idea of using security keys to encrypt both IoT servers and IoT devices.	2021 International Congress of Advanced Technology and Engineering (ICOTEN)	N/A	2021	Authentication in the context of IoT servers and IoT devices is simply a model for the establishment of trust in the identity of IoT devices and servers to control access and protect data when information is conveyed through the internet or other unsecured network. It is important to have strong IoT authentication because it helps ensure that connected servers and devices could earn the trust of protecting data against possible control commands from malicious actors and unauthorized machines. Additionally, authentication plays an integral role in preventing potential attackers from pretending to be authorized IoT servers and IoT devices hoping that they will access sensitive data.	N/A	MFA is one of the proven approaches that could be used to increase cybersecurity. Even though passwords play an integral part in promoting security, they are not entirely infallible. Cyber-attackers can use different methods to compromise, steal, or guess your passwords. However, MFA can assist significantly because it makes it more challenging for malicious actors to access accounts or devices. That is why many companies have been providing MFA features in most of their product offerings.	The authors discussed a bunch of different authentication schemes, such as security keys, cloud computing, and MFA and believe MFA is the best authentication schema for IoT authenticatiion. Some examples of MFA could include the user of email and push notifications.	W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," 2021 International Congress of Advanced Technology and Engineering (ICOTEN), 2021, pp. 1-9, doi: 10.1109/ICOTEN52080. 2021.9493492.	@INPROCEEDINGS{9493492, author={Alnahari, Wael and Quasim, Mohammad Tabrez}, booktitle={2021 International Congress of Advanced Technology and Engineering (ICOTEN)}, title={Authentication of IoT Device and IoT Server Using Security Key}, year={2021}, volume= {}, number={}, pages={1-9}, doi= {10.1109/ICOTEN52080. 2021.9493492}}	https://ieeexplore.ieee.org/abstract/document/9493492	Needs to be approved
	Alison Nakai-Lackey	How to Dance your Passwords: A Biometric MFA-scheme for Identification and Authentication of Individuals in IIoT Environments		Christoph Lipps, Jan Herbst, and Hans Dieter Schotten	Biometric Authentication; Human-PUF; Physically Unclonable Functions; Physical Layer Security; Industrial Internet of Things; Plug & Trust	Current environments especially in the industrial sector including smart factories, the Industrial Internet of Things (IIoT) and Cyber-Physical Production Systems (CPPSs) consists of a multitude of different communicating "entities". To secure these environments and to protect them against unauthorized entry, malicious access and leakage of confidential information, it is necessary to authenticate and thus identify the various participants. For technical components such as sensors, actuators and other machines, there are a lot of solutions such as certificates, Trusted Platform Modules (TPMs) and Physically Unclonable Functions (PUFs). In this work, a Multi-Factor-Authentication (MFA) scheme is presented which is based on Human-PUFs (H-PUFs), uninfluenceable and characteristic features of humans. A combination of factors, Inherent given (gait, weight), Knowledge-based (secret step pattern/toe movement) and Possession factors (shoes/insoles), is used to identify and authenticate an individual person. For this purpose, an 18x6 sensor matrix of conductive lines is proposed, which is controlled and evaluated by a Microcontroller Unit (MCU) and a specially designed circuit board. By controlling of the MCU, a pressure profile of the foot during gait can be derived via corresponding voltages and resistances. Through evaluation and appropriate training, a Machine Learning (ML) algorithm is used to find features that separate humans. The recognition and authentication of workers with the MFA scheme enables a higher level of security than entering PIN codes or using Token cards. In order to increase security, the system can be expanded with additional factors, further biometric and technical features as well as context information. The idea is to integrate the H-PUF MFA into a general security framework that maps various aspects of device authentication and access control. Besides those industrial and security related scope, the system is also capable for further applications in the medical sector or in sports. Wherever the individual gait can indicate a disease, it can be used for therapeutic purposes or to measure and improve performance	16th International Conference on Cyber Warfare and Security	N/A	2021	Biometric multifactor authentication using ML to differ between humans	Authentication, Industrial Internet of Things, Biometric Authentication, Fingerprint Authentication, Multifactor Authentication, Insole Sensor Matrix,	This work proposes a gait based authentication scheme. Therefore an 18x6 sensor matrix of conductive lines controlled and evaluated by a Microcontroller Unit and a specially designed circuit board is applied. With the given data of the first prototype the system is able to recognise specific gait with an accuracy of up to 59 % after one step. Through applying Machine Learning Algorithms for regression problems the system predicts the specific pressure of the matrix points for a given time value.	No experiments performed, this is more of a theoretical paper using gait as a way to authenticate and differentiate between different persons	Lipps, Christoph & Herbst, Jan & Schotten, Hans. (2021). How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments. 10.34190/IWS. 21.016.	@inproceedings{inproceedings, author = {Lipps, Christoph and Herbst, Jan and Schotten, Hans}, year = {2021}, month = {03}, pages = {}, title = {How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of Individuals in IIoT Environments}, doi = {10.34190/IWS.21.016} }	https://www.researchgate.net/profile/Christoph-Lipps-3/publication/351348971_How_to_Dance_Your_Passwords_A_Biometric_MFA-Scheme_for_Identification_and_Authentication_of_Individuals_in_IIoT_Environments/links/60c24c30a6fdcc2e61315ff7/How-to-Dance-Your-Passwords-A-Biometric-MFA-Scheme-for-Identification-and-Authentication-of-Individuals-in-IIoT-Environments.pdf	This more deals with industrial IOT, but is a neat intersection between MFA and biometric authentication
	Andrea Pallotta	A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks	Approved	Jian Li, Zhenjiang Zhang, Lin Hui, Zhangbing Zhou	Privacy, Message authentication, Internet of Things, Authentication, Public key	With the rapid development and massive deployment of the Internet of things (IoT) networks, security related issues in the IoT networks have been paid more and more attention to. Among all the security concerns, message authentication is critical in preventing the unauthorized messages from being transmitted in the IoT networks. Many message authentication schemes have been proposed based on the public-key cryptosystem, where the key management is simple and scalable. Identity based cryptosystem is a special type of public-key cryptosystem and can further ease the process of the key management since the public keys can be obtained easily. In this paper, we devise an efficient message authentication with enhanced privacy (IMAEP) scheme using the identity based signature. Our proposed scheme can provide both unconditional privacy as well as the enhanced privacy under full key exposure attack. Our proposed scheme can also provide existential unforgeability under the adaptive chosen-message-and-identity attack. Compared with the scheme that has the same level of anonymity and security, our proposed scheme has much lower computational overhead, and can provide extra unconditional privacy. Next we propose an extended IMAEP (EIMAEP) scheme for the general access structures where the message is signed by a group of users instead of one user. We also conduct comprehensive analysis and demonstrate that the EIMAEP scheme can achieve the same level of privacy and unforgeability as the IMAEP scheme.	IEEE Access (Volume: 8)	Not found on conference portal. IEEE seems to have A*-B score mostly	2020	As IoT networks are becoming more and more "intelligent" and can sense physical data and respond to the physical world without human interaction, correct message exhange within the networks is becoming a critical functionality. Since there is no human interaction, the system must be able to successfully filter unauthorized messages without using too much of the sensors' resources. Different authentication algorithms that aim to protect the privacy and authenticity of the messages have been proposed. However, many introduce additional overhead and can be furhter simplified.	Ye et al.'s wireless meessage authentication study, PKI-based authentication, Guo's et al's group signature-based privacy-preserving framework, anoynmous authentication, ECC, Rajput et al's hybrid privacy-preserving authentication scheme, Chen et al's authentication protocol for Internet of vehicles, Sureshkumar et al's smart vehicles authentication and key stablishment protocol,	The authors propose an authentication (IMAEP) scheme that aims to: - Improve message authentication by detecting whether the message is being sent by a particular user group - Improve message integrity by detecting whether the message has been modified in the relay nodes. - Improve hop-by-hop authentication. Each relay node on the routing path should be able to check a message's authenticity and integrity. - Improve efficiency by removing additional computational and communicational overhead.	The proposed IMAEP scheme consists of four algorithms: 1. Setup algorithm: the key generation center (KGC) generates a set of parameters made publicly available and a master key, stores privately in the KGC 2. KeyGen algorithm: using the master key and a signer's identity, the KGC computes the signer's secret signing key. 3. Sign algorithm: the signer uses its secret signing key (generated using the KeyGen algorithm) and the group identities to compute the corresponding ring signature, used to sign a message. 4. Verify algorithm: a verifier can check the validity of a ring signature using the message, the identities of the signer's group, and aiding information computed by the KGC. If the signature is valid, the verifier will accept it. Otherwise, the verifier will decline it.	J. Li, Z. Zhang, L. Hui and Z. Zhou, "A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks," in IEEE Access, vol. 8, pp. 39689-39699, 2020, doi: 10.1109 /ACCESS.2020.2976161.	@ARTICLE{9007751, author={Li, Jian and Zhang, Zhenjiang and Hui, Lin and Zhou, Zhangbing}, journal={IEEE Access}, title={A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks}, year={2020}, volume={8}, number={}, pages={39689-39699}, doi={10.1109/ACCESS. 2020.2976161}}	https://ieeexplore.ieee.org/document/9007751	The IMAEP scheme proposed in this paper is based on well-established work and aims to introduce absolute privacy. I found it interesting because, while the implementation is really complex, the fundamental idea is fairly simple
	Niklas Bernardo Correa	Robust and Lightweight Mutual Authentication Scheme in Distributed Smart Environments		GURJOT SINGH GABA, GULSHAN KUMAR, HIMANSHU MONGA, TAI-HOON KIM AND PARDEEP KUMAR	Authentication, elliptic curve Qu-Vanstone (ECQV), Internet of Things (IoT), implicit certificate, security.	In the smart environments several smart devices are continuously working together to make individuals' lives more comfortable. Few of the examples are smart homes, smart buildings, smart airports, etc. These environments consist of many resource constrained heterogeneous entities which are interconnected, controlled, monitored and analyzed through the Internet. One of the most challenging tasks in a distributed smart environment is how to provide robust security to the resource constraint Internet-enabled devices. However, an authentication can play a major role ensuring that only authorized devices are being connected to the distributed smart environment applications. In this paper, we present a robust and lightweight mutual-authentication scheme (RLMA) for protecting distributed smart environments from unauthorized abuses. The proposed scheme uses implicit certificates and enables mutual authentication and key agreement between the smart devices in a smart environment. The RLMA not only resists to various attacks but it also achieves efficiency by reducing the computation and communication complexities. Moreover, both security analysis and performance evaluation prove the effectiveness of RLMA as compared to the state of the art schemes.	IEEE Access (Volume: 8)	Not found on conference portal. IEEE seems to have A*-B score mostly	2020	lack of sufficient authentication and/or design flaws in authentication mechanisms in IoT devices leads to sensitive information or data breach which may be misused. Resultant, security has been one of the main challenges in the success of distributed smart environments and applications.	Asymmetric key based schemes (ECDH, ECQV, ECC-based implicit certificates, ECC-based mutual authentication, Elliptic Curve Discrete Log Problem, Capability Access Control)	In this paper, we propose a robust and lightweight mutual-authentication scheme (RLMA) for the distributed smart environments. To achieve the efficiency and lightweightness at resource constrained nodes, elliptic curve cryptography (ECC), implicit certificates, and symmetric encryption are used. The proposed scheme exhibits several security properties, such as mutual authentication, session key agreement, message freshness and anonymity and/or untraceability	A. System Set-up Certificate Authority (CA) off-line initializes the cryptographic mechanisms (such as, EC, n, point generator, hash function, symmetric encryption algorithm). The CA generates own public key (QCA) and private key (dCA). In addition, it generates a key pool of secret keys (e.g., KS1,KS2, . . .KSn) for the Home Area Networks (HANs) (HAN1, HAN2, . . . HANn) B. IoT-Node Registration In each HAN, an IoT node needs to be registered to the CA and obtains security credentials including a certificate and a key. Node requests a certificate to the CA, which provides one. Node dervices key and verifies integrity. C. Mutual Authentication and Key Exchange Node U initiates the communication and sends key-request to node V. Upon receiving key-request message, the node V decrypts Z1 using KS1, obtains CertU , LT , nU , U, IDCA. It first verifies the lifetime LT of the certificate and IDCA of the CA. If these conditions are true then it goes to the next step. In order to verify the authenticity of node U, now the node V derives Key1 and verifiesToken1. If this condition fails then it aborts the session. Otherwise, the node V computes node U's public key. Now, the node V generates key2 and token2 which are sent in key-response. Finally, it computes pair-wise key using private key and the public key. Node U decrypts and obtains certificate, lifetime, and ID. It verifies the lifetime of the certificate and the ID. If true, it then computes token two and verifies it against the token sent by V. If successful, computes node v's public key and pair-wise key.	Gaba, G. S., Kumar, G., Monga, H., Kim, T.-H., &amp; Kumar, P. (2020). Robust and lightweight mutual authentication scheme in Distributed Smart Environments. IEEE Access, 8, 69722–69733. https://doi.org/10.1109/access.2020.2986480	@article {gaba_kumar_monga_kim_kumar_2020, title={Robust and lightweight mutual authentication scheme in Distributed Smart Environments}, volume={8}, DOI={10.1109/access.2020.2986480}, journal={IEEE Access}, author={Gaba, Gurjot Singh and Kumar, Gulshan and Monga, Himanshu and Kim, Tai-Hoon and Kumar, Pardeep}, year={2020}, pages={69722–69733}}	https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9060967	The proposed scheme seems to provide adequate assurances and is deployable in resource constrained devices. The scheme is device-to-device only, but can be extended to include user-to-device authentication as stated by the authors.