A Comparative Analysis of the Multi-factor Authentication Protocols presented in the Literature

J. BALS, University of Twente, The Netherlands

The Internet of Things continues to develop and impact or world and even our daily lives. it is vastly changing our world, whether this at university, at home, at supermarket or even in street. IoT is getting intention in ideas like smart homes and smart cities, raising a number of security concerns. Every node in IoT platforms should be identified by the whole components of the system and by other nodes also. So every node should be authenticated before being able to communicate. In this paper , we will investigate authentication schemes used in IoT and particularly multi-factor ones. As a result bench mark of all multi-factor schemes presented in the literature will be analysed regarding their strength, weaknesses and the factors used in each one.

Additional Key Words and Phrases: Multi-factor Authentication protocol, analysis, security, IoT, internet of things

1 INTRODUCTION

Over the past few years, Internet Of Things (IoT) has become one of the most relevant technologies in the existing century. Many physical objects are being embedded with sensors and are becoming a part of the IoT ecosystem for the purpose of connecting and exchanging data with other devices and systems over the internet [55]. Such devices are being deployed in large spectrum of domains ranging from smart grid, public health, to smart homes, smart cities and smart agriculture [48]. With the IoT having grown to such an extend and still growing at this moment, shows that the IoT has become an integral part of daily life and will remain for quite some time to come. The majority of devices connected to be part of IoT are resource constrained ones by design[8]. Such limitation displayed a number of challenges. One of the most important challenges is security [27]. As most of that information is being send over or is accessible via public channels, this means that possible attackers don't need access to the devices to try and get sensitive data from them[12]. However implementing security in these small IoT devices has many challenges on its own. These devices have limits on the amount of power they have, limits on computing power they have access to and sometimes limits on time as some devices have delay restrains due to real-time applications. [14]

In an article written in the Guardian [2] it was said that over half a million pacemakers needed to be recalled due to the possibility of hackers being able to gain access to and control the medical devices. They would be able to run down the battery or alter the heartbeat of a patient, both cases could lead to the death of the patient. This case shows the importance of authentication in IoT devices. Having anyone not a doctor or otherwise capable person being able to gain access to the device and be able to alter or shut down its functionality is a scary thought. This leads to IoT devices needing acceptable authentication protocols in place to prevent unauthorized access.[28] To ensure adequate authentication single-factor authentication is not enough. Single factor authentication can be broken by one attack, guessing or cracking for passwords and PIN codes or stealing for smart cards and phones[44]. A possible solution would be Multi-Factor Authentication (MFA) due to the fact that attackers would need multiple attacks to be able to breach into a system[15]. Just stealing a smart card is not enough when the system also requires a specific password that matches the smartcard, or when an attacker sees the PIN code from someones login but, then needs the one-time token send to their phones.

In this paper, we will benchmark existing MFA systems, to do this a handful of questions will need to be answered. Firstly, it needs to become clear what vulnerabilities IoT systems face in the sense of security and authentication. Secondly, the Multi-factor authentication protocols presented in the literature should be explored. And Lastly, what are the factors are used in the proposed systems and how do those affect the IoT and their devices. The above-mentioned problem statement leads to the following research question:

RQ1 : What are the Security challenges facing IoT platforms?
RQ2 : What are the multi-factor authentication factors presented in the literature?
RQ3 : What are the factors used during authentication in the schemes?

The rest of this paper will set out to answer these questions and analyse the results. In section 2 we will start with explaining security challenges that the IoT faces, and then explore what challenges can be stopped or lessened by an authentication protocol. After the attacks the chosen authentication protocols will be explained in section 3 these protocols will be further analysed in section 5, before that in section 4 this paper will present the different factors that could be used for different authentication protocols. Lastly, this paper will end in section 6 with a conclusion of the paper and ideas for further research.

2 SECURITY CHALLENGES

In this section we will have a look at different security risks in IoT, but before getting to the security risks in IoT it would be smart to understand the underlying architecture of the Internet of Things. In the literature [23], [10], [30] two different architectures are proposed as can be seen in figure one. A three layered and a five layered architecture, the three layered architecture, shown in figure 1[23], which consists of the following layers:

- **The Physical or Perception layer**: This is the layer where the real tangible components of the IoT, the hardware where the software components are build into[30]. This layer is in addition to ensuring functionality also responsible for sensing physical properties of its environment by the means of sensors (temperature, speed, location, etc.)[23].

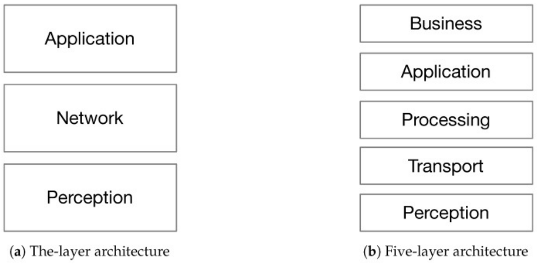
TScIT 37, July 8, 2022, Enschede, The Netherlands

- **The Network layer**: This layer is responsible for getting the data from the physical layer, storing and managing, and lastly passing the data to the application layer via different mediums (Wi-Fi, Bluetooth, 4G, etc.)[30]. This layer should handle the data in a secure and authentic manner[32].
- **The Application layer**: This is the layer where users will interact with. The application layer provides services to the customer using the data given to the layer via the physical and network layers[10][30]. This layer is in addition to providing services to the customers also responsible for guaranteeing the authentication, confidentiality and data integrity [32].

The five-layered architecture is said to go more in dept about the workings of the IoT, adding two more layers to the previously mentioned architecture as illustrated in figure 1[30][32]:

The Processing layer and the Business layer. The processing layer would specifically be responsible for analysing, storing and processing large amounts of data that has been send over the network (or transport) layer. The business layer is responsible for making graphs, analyses data and generating business models[30][23].

For the purpose of this paper the three layered architecture will be used as the business part of the IoT is not relevant to this benchmark and the processing layer can be combined with the transport layer for this paper.



(**a**) The-layer architecture (**b**) Five-layer architecture

Fig. 1. IoT Layer Architecture

2.1 Physical layer

Of these Physical attacks shown in table 1, most could be solved in a sense by well developed authentication protocols in the following ways: The node injection attack can be solved by having the network authenticate each node on specific, hard or impossible to forge traits before it is accepted into the network. One of the ways to stop a replay attack is by using time as a factor in the authentication messages, the recorded messages cannot be used later since the system will know it has the wrong timestamp. The tag cloning attack can be prevented by using more than only an RF-ID tag as authentication, but additional hard to forge factors(for example bio metrics or Geo location). Lastly the timing attack, adding a random amount of delay between responses can help with preventing any meaningful knowledge to be presented to the attacker.

2.2 Network layer

Of the network attacks mentioned in table 2, no attacks can be prevented by using authentication schemes. all of these attacks either need some form of message encryption, routing schemes, both or in case of the sleep deprivation attack a specialized scheme to detect continuous power consumption to be able to stop the attack entirely.

2.3 Application layer

Lastly, of the application layer attacks shown in table 3, there is one attack that can be prevented the data access attack, with a proper authentication scheme IoT applications should be able to ensure no one gets access to data that is not relevant for that person. The other three attacks need encryption in the case of the privacy leak attack and the sniffers, or an application that checks all input to ensure malicious code cannot be injected in running software.

In this section we answered the first research question that was proposed in 1. This section showed many attacks that systems in IoT could face and what they entail, in addition this section also talked about what attacks could be stopped by implementing a sufficiently thought out auhtentication scheme.

3 RELATED WORK

This section surveys the literature of the multi-factor authentication schemes for IoT.

In [13] authors presented an authentication scheme that is proposed based on a combination of cryptographic-protocol and the fingerprints of IoT devices, these fingerprints consist of traits of the system such as: physical network parameters, energy consumption and traffic send from a device. It takes three messages to achieve a secure connection by using extracted features and 10 hash-functions, this

Table 1. Physical layer attacks

Physical risk	**Explanation**
Malicious node injection [38]	Adding a fake node into the network to try and get information about the system.
Node capture attack [62]	Controlling a node in the network, usually results in protocol data being stolen.
Replay attack [63]	An attack that sends messages previously recorded to try and get the system to re transmit the data.[63]
Tag cloning [36]	Making a physical copy of a registered tag to be able to log into certain applications.
Timing attack [57]	An attack with the goal to figuring out which encryption algorithms are used by repeatedly recording the time the node needs to respond to a request.

makes the scheme relatively fast when compared to other schemes.

The authentication scheme proposed by authors in [55] used bio metrics and a password in addition to a specific login protocol. Users and Nodes get registered separately at the gateway node. When the User logs in for a device, the device will check the credentials and bio-metrics at the gateway node, who will in turn verify or deny the user. This scheme will take an extra message compared to the previous scheme to secure a connection, but should in turn be very resistant to attacks due to the difficulty in copying or forging bio-metrics.

The scheme proposed by the authors of [5] is similar to the one presented by authors in [55] in the sense that both use registration and a central entity that helps in the login phase. But this scheme uses a key card in addition to credentials and bio-metrics, this makes the scheme even more resistant to attacks at the cost of requiring an extra component. The goal of this scheme was to achieve high scalability and being light in system resources, so the complexity of the cryptographic functions is lower.

In [61] authors proposed a scheme that consist of three algorithms, the first one used a password and Geo-location, the second one used a password and a token, and the last one used a time-based combination of the first two. All algorithms are increasingly more secure, but also take increasingly more resources. Making the scheme time and location sensitive makes more resilient to some attacks, this is because location and time are hard to forge and immune to "guess"[70].

Table 2. Network layer attack

Network risk	Explanation
Sleep deprivation attack [34]	An attack focused on keeping the nodes in a network from going asleep to ensure maximum battery consumption. Results in nodes shutting down earlier than expected.
Sinkhole attack [39]	An attack that makes it seem that all traffic should be forwarded via a certain node due to being cost efficient, then dropping all packets send through the node.
Man in the middle attack [35]	An attack where traffic between two nodes is intercepted and controlled.
Hello flood attack [3]	An attack with which the attacker floods the networks with Hello messages, this then forces the nodes to reply to the messages congesting the network.
Denial of Service [31]	Similar to an hello flood attack, except the attacker floods the network with a vast amount of random traffic the until it becomes unavailable to users.

Table 3. Application layer attack

Application risk	Explanation
Malicious Code injection [47]	An attack where the attacker might use one of the nodes to inject a fragment of code that gives complete control of the network, or shuts it down.
Sniffers [26]	Sniffers allow for an attacker to capture and view not encrypted data from the application.
Data Access [22]	With the amount users of IoT application comes the need of access control to ensure that people have access to the data they need or are allowed to access, but nothing more.
Privacy Leak [51]	A leak of sensitive data of users. Any data generated by users of the application should be kept save and the application should ensure privacy of the users.

Authors in [54] presented a scheme that uses a central gateway to authenticate users and nodes separately, for users it uses both a one-way hash and elliptic curve cryptography (ECC). The gateway chooses an elliptic curve and a one-way hash and sends that to the user and nodes. The user then generates a signature and sends the password and id to the gateway who verifies it and returns the id and password in a smartcard. A similar approach is used for the publishers with the exception that a password is absent. Thus achieving authentication in 5 messages if the gateway message is broadcast instead of sending it to both parties only.

Authors in [19] presented a three-factor scheme is proposed utilizing a password, biometrics and a smartcard. Similar to the previous scheme it uses a gateway, ecc and a one-way hash to authenticate users and nodes. But, due to the presence of biometrics also use perpetual hashing to help with the slight variations that can occur in different biometrics. Nodes are registered with a unique id when deployed, while users register by sending their id, password and biometrics to the central gateway. The gateway returns a smart card to the user that can be used to login.

In [60] authors presented a scheme based on a Password , Biometrics and a smartcard to authenticate users like the last scheme. To register the user sends his or her password, id and biometric data to the gateway node, after which the gateway node generates a smartcard that gets send back to the user in a secure manner. When a user wants to log into the system they input their id,password and biometrics into the reader which will check the data with the data saved in the smartcard, when the data is acceptable the reader sends a message to the gateway node.

Authors in [33] proposed a two-factor authentication protocol using Password and phone verification. The user sent to a central server his id, password and phone number to register, when the user wants to login, he do that using his password and id as initial phase. Then the server sends a one time password (OTP) to the phone, the user copies this password to the login field and is then logged into the system.

In [9] authors proposed a two-factor authentication scheme is proposed, but instead of using phone verification as [33] uses this scheme uses a Physical Unclonable Function (PUF) in addition to an identity. In this scheme all devices are equipped with a PUF, which will render the device useless when tampered with. To register the device communicates with a server to receive an identity, to get this identity the server sends a challenge to the device and awaits a response. When the response is received the server sends an array of challenges to the device to also return the answers for which will function as the responses the server will expect. When a device wants to login into the system the device sends its identity to the server which will respond with a challenge, if the response is valid a new id will be generated for the next session and the challenge will be removed from the database of the server.

Authors in [16] proposed a scheme that uses an alphanumerical password, a graphical password and lastly a security question to provide a secure authentication. To login the user first gives his or her password, after that gets checked the user is asked for the graphical password and if that is also correct a security question will be asked. If the user passes all three factors entry to the system is permitted.

Authors proposed a scheme in [1] which lets the user register with a password and his/her biometrics, after that the gateway node has calculated all data, the user is provided with a smart card containing a shared key to help with the authentication process. The login process is as simple as plugging in the smart card and inserting the password and biometric data, when everything checks out the gateway node updates the shared key for future logins.

In [65] the authors propose a scheme that uses biometrics, a smart card and a password as factors. The register and login sequence is similar to the previous schemes that use these factors: input an id, password and biometric data, then the gateway node calculates values to put into the smart card which gets send to the user. To login the user inputs the password, biometric data and smart card into the reader and the gateway node checks if the data received is similar to the smart card data.

The authors in [41] propose a scheme that uses three factors for authentication: a password, a smart card and the user's biometrics. For registration, the user first enters an id for the system, if the id already exists, the gateway node sends a smartcard with the id to the user. The user inserts the card into the reader and enters a password and his/her biometrics. The system then updates the smartcard to include these factors as well. To login the user inserts the smartcard, the password and fingerprint, after which the system validates the attempt.

Similar to [41] the authors of [43] propose a scheme that uses a password, a smart card and the user's biometrics to authenticate its users. Differently than the previous scheme, when the user wants to register he or she first inputs an id, password and his or her biometrics into the system and sends it to the gateway node. The node will calculate some values with the data received and puts it in the smartcard that gets send to the user. The login sequence is similar to the previous three factor schemes by inputting all the factors and the system checking the values given by the smartcard to either refuse or allow the attempt.

In [18] the authors present a scheme which uses a password and the users biometric data like previously mentioned schemes but also uses a mobile device as the third factor. To register a user registers at the gateway node of the network the user registers a password, id and fill in the biometrics. The gateway node uses these values to calculate some parameters that gets stored in a mobile device in the form of some kind of app. To login the user opens the app, and inputs his or her id, password and biometrics, the mobile device then sends the info to a node in the network. The node will then use the info received to check with the gateway node if the user is a real user and if so if the user is allowed to access the node.

Authors in [53] and [56] both propose a scheme that uses two factors, namely: a smart card and a password. To login the user selects an id and password, which get send to the gateway node to calculate some parameters with. These parameters get send to the user inside a smart card which can be used to login by inserting the card into a reader and typing in the password. After the reader establishes the user it sends the accepted request to the gateway node.

In [25],[67],[24] and [6] authors present schemes who use two factors, but in addition to a password this schemes uses a Mobile device as second factor. The user registers him or herself at a gateway node, first the user fills in an id and password, which will generate a value that gets send to the users mobile device to store. To log in the user fills in their password and id on the mobile device which will generate a value and sends it to the gateway node. The gateway node will send data to both the sensor and the user that allows for mutual authentication between the sensor and the user.

In [42], [37] and [66] authors propose schemes that use biometrics, passwords and smart cards as factors. They have similar register and login procedures that have been seen earlier. The user picks an id and fills in their password and biometric data. The data gets send to gateway node, who computes a parameter that gets put into the smartcard and send to the user. The user logs into the system by scanning the card, filling in the data and the system verifies the input with a database.

The authors of [20] and [17] both propose schemes that use three factors, but instead use a smart device as the third factor, the first to also being a password and biometrics. To register for the system a user fills in their id, biometric data and password at a gateway node, who calculates a couple parameters that later get stored in the smart device of the user. Then, when the user wants to login to the system the users opens the application on the device, fills in the id, password and biometric data which the device then sends to the gateway node to request access. The gateway then checks the data and decides to accept or refuse it.

The authors in [45],[46] and [68] all propose schemes that use two factors namely: a password and a smart card. First the user chooses an id and password and sends it to the head admin of the system, the admin will then send back a smart card with parameters inside. If the user then wants to log into the system it is as simple as seen in earlier schemes: fill in the id and password, scan the smart card and the head admin rejects or accepts the login request.

Lastly, the authors in [7] present a protocol which uses a smart device and a password to authenticate its users. At registration a user give an id and password to the server, after the server receives these it calculates some values and sends them back to the user to be stored in the smart device. When the user wants to log in they fill their id and password into the mobile device, the device then sends the request with parameters from its memory to the server. The server checks the values and either rejects or accepts the login attempt.

4 FACTORS IN THE LITERATURE

In the literature[59], there are plenty of factors that can be used for authentication, in this section we will compile these factors and give some strengths and weaknesses for each one. These factors are differentiated into three main groups[50]:

(1) Something that the user **knows**.
(2) something that the user **has**.
(3) something that the user **is**.

In table 4, we have collected several factors that are used or could be used in MFA schemes and the type of the factor.

Table 4. Authentication factors

Type of factor	Factors
Know	Text passwords
	Graphical passwords
	Cognitive authentication
	Personal Identification Number (PIN)
	Questions
Have	ID-based (Smart Cards)
	One Time Password (OTP) tokens
	Mobile-based
	Physical unclonable functions (PUF's)
	Received signal strength indicator (RSSI)
	Geo location
Are	Face biometrics
	Keystroke biometrics
	Hand gestures
	Palmprint biometrics
	Touchstroke biometrics
	Fingerprints
	Iris biometrics
	Brainwaves
	Heartbeats
	Knuckleprint biometrics
	Gait biometrics
	Multi-modal biometrics

Firstly, the **know** category, Text passwords, Graphical passwords, PIN, Security questions generally work upon the same principles, to unlock the factor give the password,number sequence, pattern or answer to the question that the user has previously given to system. A simple mechanism for most user to understand and use, but most of these passwords are relatively simple so they are easier to remember, are used by multiple people on a shared account or are used for multiple systems[21]. All of these factors fall prone to similar attacks: they can be guessed if too easy, cracked if harder, can be replayed to the system if recorded or shouldered if the user is physically in close proximity to an attacker or when monitored remotely if not[21, 40]. A slightly more sophisticated "know factor"is cognitive authentication, this factor uses a predetermined secret scheme to be shared with the user, for example a couple pictures, then the login screen would show pictures with numbers at the bottom and right screen. In this case the formula could be: "if the picture is in the secret group go right, otherwise go down" [64]. This makes the password much harder to break as even seeing the answer one time will not be sufficient to find the next answer.

Secondly, for the **Have** category the first three factors: smart cards, mobile and tokens share most of their advantages and disadvantages with each other. They are all easy to use, low in costs and in case of loss new ones can be made. But at the same time are prone to forging and theft or being shared between people[29, 58]. Forging and theft being more impactful than being shared, but both compromise the idea that the one in possession of the token/card/phone is the person linked to it. Then the last three factors are a bit more different than the previous "have factors": first, PUF's are small circuits that output a certain sequence for a certain input where no two circuits produce the same output, so unless an attacker physically has the PUF it is difficult to guess the right response to an arbitrary challenge[11]. The only noticeable drawback is that PUFs sometimes suffer from noise that can change one or two bits making the response invalid for a certain challenge, certain precautions can be added to a systen to help with this drawback[13]. second, RSSI can be used to authenticate certain users for a given system, it uses the received signal strength at a node to determine the identity for a user. Since the RSSI is dependant on the power of the send signal, the terrain the signal has to travel over and the distance to the node/system. If set-up properly it can identify different users that are within close proximity due to the RSSI of different devices being unique per device[4]. and last we have geolocation, this factor uses hardware or software components to determine whether a user in the right area to use the system. This can be done via WiFi, Bluetooth, IP-address, or cellular network. This ensures that only people in a specific area can access the system, but does so in a broad way, so needs to be combined with other factors to authenticate individuals[71].

Lastly, in this project we will be combining all the different kinds of **biometric** factors into one factor, as the different kind of biometrics that can be used by different IoT devices is completely dependant on the resources it has available and the purpose of the scheme while fulfilling the same role in each scheme[69]. Also shared between these different kinds of biometrics are most of the drawbacks and the benefits. Biometrics are hard to forge, cannot be stolen or guessed, are in most cases very user friendly and is often faster than other authentication factors[49]. But the drawback of biometrics are that they are prone to false positives and positives when any noise is introduced to the system, systems could be costly and users might have a hard time accepting such data to be used[49, 69].

In this section we answered the second research question that was proposed in 1. This section showed factors that could be used in different multi factor authentication schemes and strengths and weakness of these factors.

5 ANALYSIS

In this section we will analyse thirty multi-factor authentication protocols that are proposed in the literature. To do this we have compiled table 5 that is shown in the appendix of this paper. The table consists of the name of the scheme, the number of factors used and which factors they are, strengths of the scheme and its weaknesses. The table itself answers the third research question posed in section 1: "What are the factors used during authentication in the schemes?".

Exactly half of the schemes in the table are two factor authentication protocols, and half of the schemes are three factor authentication. What we also see in the table is that the difference in strengths and weaknesses between two and three factor authentication barely depends on the number of factors used but rather depends on what kind of factors are used in the schemes.

For example: the scheme proposed in [16] uses three factors, but all of the factors are from the **know** category as described in section 4 while the scheme proposed in [33] uses only two factors but are from the **know** and **have** categories respectively and has less weaknesses and more strengths. So we can conclude that schemes that have more factors from different categories in general are better than schemes who uses only one category.

We also do not see in literature many four or more factors used in authentication schemes designed for the internet of things, while you do see them in the literature for other fields. From this we conclude that more factors is in the realm of IoT not a preferred method to increase security because of the restrictions on battery, computing power and in some cases acceptable delay that are in play with IoT devices[14].

We also see that schemes who use biometrics, physically unclone-able functions (PUFs), device fingerprints and geolocation in the form of RSSI generally have less weaknesses that those without. This could be derived from the explanation given in section 4 that all these factors are hard to forge or imitate and cannot be stolen or cracked as the other factors could. So, using these factors in future schemes may improve security compared to the schemes presented here with the same number of factors but using other factors.

So to conclude the recommendation that this paper does for future multi-factor schemes: First recommendation, the authentication schemes should seek a balance between security and system load given the situation it is made from. Adding another factor to a scheme might improve the security of a schemes more, but the load on the system resources could be more detrimental than having some vulnerabilities the system for some systems. The second recommendation is that the schemes use factors different groups rather than multiple from the same group, table 4 gives a good overview of possible factors that could be used in future schemes as that table is the result of a literary review of current factors used and proposed in the literature. As a password and a security question would be more secure that only one or the other, they could both be bypassed in a similar manner. And the last recommendation that the paper does is to preferably use factors mentioned earlier in this section. These factors are in general more resistant to attacks than other factors and could thus increase security while keeping the same number of factors, and thus steps that users have to take.

6 CONCLUSION

In this paper we have taken a critical look at different security challenges that the IoT faces, then we took a look at different factors that multi-factor authentication protocols could use in their schemes and their strengths and weaknesses. Lastly, we analysis thirty MFA schemes proposed in the literature and did some recommendations for MFA schemes in the future.

For future work, it could be beneficial to research new attacks on IoT networks and similarly research new factors that could be used in authentication schemes to further improve the security of the IoT or be more cost efficient while still providing the needed protection against attacks that are currently known.

REFERENCES

[1] Abdi Nasib Far Hossein;Bayat Majid;Kumar Das Ashok;FotouhiMahdi;Pournaghi S. Morteza;Doostari M. A. 2021. LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. https://doi.org/10.1007/s11276-020-02523-9

[2] Hern A. 2017. Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

[3] T. Aditya Sai Srinivas and S.S. Manivannan. 2020. Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm. , 162-175 pages. https://doi.org/10.1016/j.comcom.2020.03.031

[4] Mohammed A. Alanezi, Houssem R.E.H. Bouchekara, and Mohammed. S. Javaid. 2021. Range-Based Localization of a Wireless Sensor Network for Internet of Things Using Received Signal Strength Indicator and the Most Valuable Player Algorithm. *Technologies* 9, 2 (2021). https://doi.org/10.3390/technologies9020042

[5] Ahmed Yaser Fahad Alsahlani and Alexandru Popa. 2021. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. https://www-sciencedirect-com.ezproxy2.utwente.nl/science/paper/pii/S1084804521001879

[6] Ruhul Amin, SK Hafizul Islam, G.P. Biswas, Muhammad Khurram Khan, and Neeraj Kumar. 2018. A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Generation Computer Systems* 80 (2018), 483–495. https://doi.org/10.1016/j.future.2016.05.032

[7] Chaudhry; Shehzad Ashraf, Albeshri;Aiiad, Xiong;Naixue, Lee;Changhoon, and Shon;Taeshik. 2017. A privacy preserving authentication scheme for roaming in ubiquitous networks. *Cluster Computing* 20, 2 (2017), 1223–1236. https://doi.org/10.1007/s10586-017-0783-x

[8] Haroon; Asma, Ali; Munam, Asim; Yousra, Naeem; Wajeeha, Kamran; Muhammad, and Javaid; Qaisar. 2016. Constraints in the IOT: The world in 2020 and beyond. *International Journal of Advanced Computer Science and Applications* 7, 11 (2016). https://doi.org/10.14569/ijacsa.2016.071133

[9] Gope P. Sikdar B. 2019. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. journal = IEEE internet of things journal. https://doi.org/10.1109/JIOT.2018.2846299

[10] Mohanty J.; Mishra S.; Patra S.; Pati B. and Panigrahi C.R. 2020. IoT Security, Challenges, and Solutions: A Review. https://doi.org/10.1007/978-981-15-6353-9_46

[11] Armin Babaei and Gregor Schiele. 2019. Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges. *Sensors* 19, 14 (2019). https://doi.org/10.3390/s19143208

[12] Bharat Bhushan, G. Sahoo, and Amit Kumar Rai. 2017. Man-in-the-middle attack in wireless and computer networking — A review. In *2017 3rd International Conference on Advances in Computing,Communication Automation (ICACCA) (Fall)*. 1–6. https://doi.org/10.1109/ICACCAF.2017.8344724

[13] Hassan N. Noura; Reem Melki; Ali Chehab. 2019. Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems. https://ieeexplore-ieee-org.ezproxy2.utwente.nl/document/8891082

[14] Zaher Dawy, Walid Saad, Arunabha Ghosh, Jeffrey G. Andrews, and Elias Yaacoub. 2017. Toward Massive Machine Type Cellular Communications. , 120-128 pages. https://doi.org/10.1109/MWC.2016.1500284WC

[15] C Lakshmi Devasena. 2018. Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security. , 7576–7579 pages.

[16] C. Lakshmi Devasena. 2018. Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security. https://www.ripublication.com/ijaer18/ijaerv13n10_46.pdf

[17] Parwinder Kaur Dhillon and Sheetal Kalra. 2017. A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications* 34 (2017), 255–270. https://doi.org/10.1016/j.jisa.2017.01.003

[18] Parwinder Kaur Dhillon and Sheetal Kalra. 2017. Secure multi-factor remote user authentication scheme for Internet of Things environments. *International Journal of Communication Systems* 30, 16 (2017), e3323. https://doi.org/10.1002/dac.3323 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.3323 e3323 IJCS-16-0515.R1.

[19] S. Dhillon P.K.; Kalra. 2018. Multi-factor user authentication scheme for IoT-based healthcare services. https://doi.org/10.1007/s40860-018-0062-5

[20] Sadhukhan; Dipanwita, Ray; Sangram, Biswas; G. P., M. K. Khan, and Dasgupta; Mou. 2020. A lightweight remote user authentication scheme for IOT communication using elliptic curve cryptography. *The Journal of Supercomputing* 77, 2 (2020), 1114–1151. https://doi.org/10.1007/s11227-020-03318-7

[21] Su Xin;Wang Ziyu;Liu Xiaofeng;Choi Chang;Choi Dongmin. 2018. Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures. https://doi.org/10.1155/2018/4296934

[22] Sophie Dramé-Maigné, Maryline Laurent, Laurent Castillo, and Hervé Ganem. 2021. Centralized, Distributed, and Everything in between: Reviewing Access Control Solutions for the IoT. https://doi.org/10.1145/3465170

[23] M. El-Hajj M.; Fadlallah A.; Chamoun and Serhrouchni A. 2019. A Survey of Internet of Things (IoT) Authentication Schemes. https://doi.org/10.3390/s19051141

[24] Mohammad Sabzinejad Farash, Shehzad Ashraf Chaudhry, Mohammad Heydari, S. Mohammad Sajad Sadough, Saru Kumari, and Muhammad Khurram Khan. 2017. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. *International Journal of Communication Systems* 30, 4 (2017), e3019. https://doi.org/10.1002/dac.3019 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.3019 e3019 dac.3019.

[25] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, and M.A. Doostari. 2020. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks* 177 (2020), 107333. https://doi.org/10.1016/j.comnet.2020.107333

[26] Dragoş Glăvan, Ciprian Răcuciu, Radu Moinescu, and Sergiu Eftimie. 2020. Sniffing attacks on computer networks. https://www.proquest.com/scholarly-journals/sniffing-attacks-on-computer-networks/docview/2429826362/se-2

[27] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. , 1294-1312 pages. https://doi.org/10.1109/COMST.2015.2388550

[28] Meriem Guerar, Luca Verderame, Alessio Merlo, Francesco Palmieri, Mauro Migliardi, and Luca Vallerini. 2020. CirclePIN: A Novel Authentication Mechanism for Smartwatches to Prevent Unauthorized Access to IoT Devices. 4, 3, Article 34 (mar 2020), 19 pages. https://doi.org/10.1145/3365995

[29] B.B. Gupta and Megha Quamara. 2021. A taxonomy of various attacks on smart card–based applications and countermeasures. *Concurrency and Computation: Practice and Experience* 33, 7 (2021), e4993. https://doi.org/10.1002/cpe.4993 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/cpe.4993 e4993 CPE-18-0183.R1.

[30] Mohammad Ali Jabraeil Jamali, Bahareh Bahrami, Arash Heidari, Parisa Allahverdizadeh, and Farhad Norouzi. 2020. *IoT Architecture*. Springer International Publishing, Cham. 9–31 pages. https://doi.org/10.1007/978-3-030-18468-1_2

[31] Salim M.M.; Rathore S. Park J.H. 2020. Distributed denial of service attacks and its defenses in IoT: a survey. https://doi.org/10.1007/s11227-019-02945-z

[32] Latika Kakkar, Deepali Gupta, Sapna Saxena, and Sarvesh Tanwar. 2021. IoT Architectures and Its Security: A Review. In *Proceedings of the Second International Conference on Information Management and Machine Intelligence*, Dinesh Goyal, Amit Kumar Gupta, Vincenzo Piuri, Maria Ganzha, and Marcin Paprzycki (Eds.). Springer Singapore, Singapore, 87–94.

[33] Kumar Sekhar Roy; Hemanta Kumar Kalita. 2018. An Authentication Protocol for IoT Network based on Cloud Computing Environment using Two Factor Authentication. https://www.researchgate.net/profile/Kumar-Roy/publication/358978699_An_Authentication_Protocol_for_IoT_Network_based_on_Cloud_Computing_Environment_using_Two_Factor_Authentication/links/6220a21f801c922910553e53/An-Authentication-Protocol-for-IoT-Network-based-on-Cloud-Computing-Environment-using-Two-Factor-Authentication.pdf

[34] Ashvini Kamble and Sonali Bhutad. 2018. Survey on Internet of Things (IoT) security issues amp; solutions. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)*. 307–312. https://doi.org/10.1109/ICISC.2018.8399084

[35] James Jin Kang, Kiran Fahd, Sitalakshmi Venkatraman, Rolando Trujillo-Rasua, and Paul Haskell-Dowland. 2019. Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*. 1–6. https://doi.org/10.1109/ITNAC46935.2019.9077977

[36] Grishma Khadka, Biplob Ray, Nemai Chandra Karmakar, and Jinho Choi. 2022. Physical Layer Detection and Security of Printed Chipless RFID Tag for Internet of Things Applications. , 1 pages. https://doi.org/10.1109/JIOT.2022.3151364

[37] Das; Ashok Kumar, Wazid; Mohammad, Kumar; Neeraj, Vasilakos; Athanasios V., and Rodrigues; Joel J. P. C. 2018. Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment. *IEEE Internet of Things Journal* 5, 6 (2018), 4900–4913. https://doi.org/10.1109/JIOT.2018.2877690

[38] Bohan Li, Renjun Ye, Gao Gu, Ruochen Liang, Wei Liu, and Ken Cai. 2020. A detection mechanism on malicious nodes in IoT. , 51-59 pages. https://doi.org/10.1016/j.comcom.2019.12.037

[39] Yuxin Liu, Ming Ma, Xiao Liu, Neal N. Xiong, Anfeng Liu, and Ying Zhu. 2020. Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security. , 356-372 pages. https://doi.org/10.1109/TNSE.2018.2881152

[40] Ian Mackie and Merve Yıldırım. 2018. A Novel Hybrid Password Authentication Scheme Based on Text and Image. In *Data and Applications Security and Privacy XXXII*, Florian Kerschbaum and Stefano Paraboschi (Eds.). Springer International Publishing, Cham, 182–197.

[41] Karuppiah Marimuthu, Xie Qi, Ding Zixuan, and Hu Bin. 2021. A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things. (2021). https://doi.org/10.1155/2021/4799223

[42] Shuai; Mengxia, Yu; Nenghai, Wang; Hongxia, Xiong; Ling, and Li; Yue. 2021. A lightweight three-factor anonymous authentication scheme with privacy protection for Personalized Healthcare Applications. *Journal of Organizational and End User Computing* 33, 3 (2021), 1–18. https://doi.org/10.4018/joeuc.20210501.oa1

[43] Jiaqing Mo, Zhongwang Hu, and Wei Shen. 2022. A Provably Secure Three-Factor Authentication Protocol Based on Chebyshev Chaotic Mapping for Wireless Sensor Network. *IEEE Access* 10 (2022), 12137–12152. https://doi.org/10.1109/ACCESS.2022.3146393

[44] Tamara S Mohamed. 2014. Security of Multifactor Authentication Model to Improve Authentication Systems. *Information and Knowledge Management. ISSN* (2014), 2224–5758.

[45] Nikooghadam; Morteza, Jahantigh; Reza, and Arshad; Hamed. 2016. A lightweight authentication and key agreement protocol preserving user anonymity. *Multimedia Tools and Applications* 76, 11 (2016), 13401–13423. https://doi.org/10.1007/s11042-016-3704-8

[46] Nikooghadam; Morteza, Jahantigh; Reza, and Arshad; Hamed. 2016. A lightweight authentication and key agreement protocol preserving user anonymity. *Multimedia Tools and Applications* 76, 11 (2016), 13401–13423. https://doi.org/10.1007/s11042-016-3704-8

[47] Gary Mullen and Liam Meany. 2019. Assessment of Buffer Overflow Based Attacks On an IoT Operating System. In *2019 Global IoT Summit (GIoTS)*. 1–6. https://doi.org/10.1109/GIOTS.2019.8766434

[48] Sandro Nizetic. 2020. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. https://www.ncbi.nlm.nih.gov/pmc/papers/PMC7368922/

[49] Mohammad S. Obaidat, Soumya Prakash Rana, Tanmoy Maitra, Debasis Giri, and Subrata Dutta. 2019. *Biometric Security and Internet of Things (IoT)*. Springer International Publishing, Cham, 477–509. https://doi.org/10.1007/978-3-319-98734-7_19

[50] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. 2018. Multi-Factor Authentication: A Survey. *Cryptography* 2, 1 (2018). https://doi.org/10.3390/cryptography2010001

[51] Ismini Psychoula, Liming Chen, and Oliver Amft. 2020. Privacy Risk Awareness in Wearables and the Internet of Things. , 60-66 pages. https://doi.org/10.1109/MPRV.2020.2997616

[52] Fu. AnMin ;Wang.Ding; Hong. Shuhong; Wang. Qingxuan. 2021. Revisiting a Multifactor Authentication Scheme in Industrial IoT. https://doi.org/10.1155/2021/9995832

[53] Minahil Rana, Akasha Shafiq, Izwa Altaf, Mamoun Alazab, Khalid Mahmood, Shehzad Ashraf Chaudhry, and Yousaf Bin Zikria. 2021. A secure and lightweight authentication scheme for next generation IoT infrastructure. *Computer Communications* 165 (2021), 85–96. https://doi.org/10.1016/j.comcom.2020.11.002

[54] Manasha Saqib, Bhat Jasra, and Ayaz Hassan Moon. 2021. A lightweight three factor authentication framework for IoT based critical applications. https://doi.org/10.1016/j.jksuci.2021.07.023

[55] J. Gowthami; N. Shanthi. 2020. Multi-factor Based User Authentication Scheme for Lightweight IoT Devices. https://ieeexplore-ieee-org.ezproxy2.utwente.nl/document/8997157

[56] Geeta Sharma and Sheetal Kalra. 2018. A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications. *Journal of Information Security and Applications* 42 (2018), 95–106. https://doi.org/10.

1016/j.jisa.2018.08.003

[57] Sofiane Takarabt, Alexander Schaub, Adrien Facon, Sylvain Guilley, Laurent Sauvage, Youssef Souissi, and Yves Mathieu. 2019. Cache-Timing Attacks Still Threaten IoT Devices. In *Codes, Cryptology and Information Security*. Springer International Publishing, Cham, 13–30.

[58] Fatemeh Tehranipoor, Nima Karimian, Paul A Wortman, Asad Haque, Jim Fahrny, and John A Chandy. 2017. Exploring methods of authentication for the internet of things. In *Internet of Things*. Chapman and Hall/CRC, 71–90.

[59] Ignacio Velásquez, Angélica Caro, and Alfonso Rodríguez. 2018. Authentication schemes and methods: A systematic literature review. *Information and Software Technology* 94 (2018), 30–37. https://doi.org/10.1016/j.infsof.2017.09.012

[60] R. Vinoth, Lazarus Jegatha Deborah, Pandi Vijayakumar, and Neeraj Kumar. 2021. Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT. , 3801-3811 pages. https://doi.org/10.1109/JIOT.2020.3024703

[61] Ahmed AA; Ahmed WA. 2019. An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things. https://www.ncbi.nlm.nih.gov/pmc/papers/PMC6749530/

[62] Chenyu Wang, Ding Wang, Yi Tu, Guoai Xu, and Huaxiong Wang. 2022. Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks. , 507-523 pages. https://doi.org/10.1109/TDSC.2020.2974220

[63] Mohammad Shafeul Wara and Qiaoyan Yu. 2020. New Replay Attacks on ZigBee Devices for Internet-of-Things (IoT) Applications. In *2020 IEEE International Conference on Embedded Software and Systems (ICESS)*. 1–6. https://doi.org/10.1109/ICESS49830.2020.9301593

[64] D. Weinshall. 2006. Cognitive authentication schemes safe against spyware. In *2006 IEEE Symposium on Security and Privacy (SP'06)*. 6 pp.–300. https://doi.org/10.1109/SP.2006.10

[65] Xiong Jinbo;Xue Lingyan;Huang Qinglong;Zhang Shuaiqing;Huang Haiping; Wang Wenming. 2021. A Lightweight Three-Factor Authentication and Key Agreement Scheme for Multigateway WSNs in IoT. https://doi.org/10.1155/2021/3300769

[66] Liu; Wenzheng, Wang; Xiaofeng, and Peng; Wei. 2020. Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access* 8 (2020), 8754–8767. https://doi.org/10.1109/ACCESS.2019.2962912

[67] Fan Wu, Xiong Li, Arun Kumar Sangaiah, Lili Xu, Saru Kumari, Liuxi Wu, and Jian Shen. 2018. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. *Future Generation Computer Systems* 82 (2018), 727–737. https://doi.org/10.1016/j.future.2017.08.042

[68] Qi Xie and Lingfeng Hwang. 2019. Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city. *Neurocomputing* 347 (2019), 131–138. https://doi.org/10.1016/j.neucom.2019.03.020

[69] Wencheng Yang, Song Wang, Nor Masri Sahri, Nickson M. Karie, Mohiuddin Ahmed, and Craig Valli. 2021. Biometrics for Internet-of-Things Security: A Review. *Sensors* 21, 18 (2021). https://doi.org/10.3390/s21186163

[70] Faheem Zafar, Abid Khan, Adeel Anjum, Carsten Maple, and Munam Ali Shah. 2020. Location Proof Systems for Smart Internet of Things: Requirements, Taxonomy, and Comparative Analysis. *Electronics* 9, 11 (2020). https://doi.org/10.3390/electronics9111776

[71] Yinyuan Zhao, Haoran Yuan, Tao Jiang, and Xiaofeng Chen. 2019. Secure distributed data geolocation scheme against location forgery attack. *Journal of Information Security and Applications* 47 (2019), 50–58. https://doi.org/10.1016/j.jisa.2019.04.003

A TABLE OF MFA-SCHEMES

Table 5. Table with schemes and their factors

Scheme	**Number of Factors**	**Factors used**	**Strengths**	**Weaknesses**
Secure and Lightweight Mutual MFA for IoT Communication Systems [13]	2	Physical unclonable function(PUF), Received Signal Strength Indicator(RSSI)	protects against all the known authentication attacks, fuzzy extractor relieves the PUF noise	Location can influence RSSI
Multi-factor Based User Authentication Scheme for Lightweight IoT Devices [55]	2	Password, bio-metrics	Centralized authentication, Biometrics are hard to forge	PUF's can be modeled to crack pairs
An Effective Multifactor Authentication Mechanism Based on Combiners of Hash Function over Internet of Things [61]	3	ID, Password, device fingerprint	three schemes depending on speed and security	Brute force attack could break password when device gets stolen
LMAAS-IoT [5]	3	password, smart card, biometrics	0.022 seconds authentication time, Bio-metrics are hard to replicate, 3 message authentication	Card could be forged
A Lightweight Three Factor Authentication Framework for IOT Based Critical Applications [54]	3	smartcard, Password, Digital signature	0.190 second computational time, mutual authentication	Stolen device attack
Multi-factor user authentication scheme for IoT-based healthcare services [19]	3	password, biometrics and smartcard	mutual authentication, two message authentication, biometrics are hard to forge	smartcard could get stolen
Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT [60]	3	Password , Biometrics, smartcard	Hard to forge biometrics, 2.4 ms computation time	No forward secrecy, smart card loss attack, sensing device caputre attack [52]
An Authentication Protocol for IoT Network based on Cloud Computing Environment using Two Factor Authentication [33]	2	Password, phone verification	one time password and random nonce protects from replay attacks, mutual authentication	stolen smartphone attack
Lightweight and privacy-preserving two-factor authentication scheme for IoT devices [9]	2	ID, PUF	fuzzy extractor relieves the PUF noise, mutual authentication	stolen device attack
Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security [16]	3	Alphanumerical password, Graphical password, security question	graphical password difficult to crack	security questions usually have easy answers, guessing attack, social engineering
LAPTAS[1]	3	Password, biometrics, Smart card	Fuzzy extractor to ensure valid biometrics, mutual authentication	smartcard stolen plus Password cracking could gain entry
A Lightweight Three-Factor Authentication and Key Agreement Scheme for Multigateway WSNs in IoT[65]	3	Biometrics, Smart Card, password	fuzzy bio, mutual authentication, forward secrecy	higher computational cost than competitors

Continued on next page

Table 5 – continued from previous page

Scheme	Number of Factors	Factors used	Strengths	Weaknesses
A secure and lightweight authentication scheme for next generation IoT infrastructure[53]	2	smart card, password	Mutual authentication, 1536 bits storage, 0.0215 milisecond computation time	stolen smart card attacks, privileged insider attacks, user the impersonation attacks, password change attacks, and Ephemeral the Secret Leakage (ESL) attacks
A Secure and Privacy-Preserving Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things[41]	3	password, smart card, biometrics	mutual authentication, forward secrecy, hard to forge biometrics, 16.230 ms computation time	denial of sleep attack
A Provably Secure Three-Factor Authentication Protocol Based on Chebyshev Chaotic Mapping for Wireless Sensor Network[43]	3	password, smart card, biometrics	135.62ms computation time, hard to forge biometrics, forward secrecy	node capture attack
A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT[25]	2	Password, Mobile device	mutual authentication, forward secrecy, anonymity	mobile device attack, privileged-insider attack
Secure multi-factor remote user authentication scheme for Internet of Things environments[18]	3	password, biometric,mobile device	hard to forge biometrics,mutual authentication	mobile device attack, user impersonation attack; no session key agreement; no revocation
A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications[56]	2	password, smart card	mutual authentication, forward secrecy	stolen card attack
A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks[67]	2	Password, Mobile device	mutual authentication,	Suffer from Lack of forward secrecy and revocability
A robust and anonymous patient monitoring system using wireless medical sensor networks[6]	2	Password, mobile device	0.0136ms computation time, mutual authentication	offline guessing attacks and user tracking attacks, no forward secrecy
A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security[24]	2	mobile, password	Secure session key,0.0403ms computation time	user anonymity and mutual authentication. no local password verification, a faulty password change phase,replay attack, offline password guessing attack, and forgery attack.

Continued on next page

Table 5 – continued from previous page

Scheme	Number of Factors	Factors used	Strengths	Weaknesses
A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications[42]	3	password, smart card, biometrics	mutual authentication, hard to forge biometrics	stolen-verifier attack, modification of messages attack, and no perfect forward security
Security enhancement of an anonymous roaming authentication scheme with two-factor security in smart city[68]	2	password, smart card	anonymity, forward secrecy	Lack of input validation, Lack of identification, DoS attack, Lack of session key update
A privacy preserving authentication scheme for roaming in ubiquitous networks[7]	2	Mobile device, password	0.0414ms computation time, forward secrecy, mutual authentication	Stolen device, impersonation attack, no revocation, incorrect password change phase
A lightweight biometrics based remote user authentication scheme for IoT services[17]	3	password, biometrics, smart device	mutual authentication, anonymity, protection from most attacks	High verification time, memory consumption, scalability
Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things[66]	3	biometrics, password, smart card	forward secrecy, mutual authentication	7ms computation time
A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography[20]	3	Biometrics, password, smart device	mutual authentication, resist man-in-the-middel attack	no user anonymity ,user impersonation, privileged insider. In addition,no revocation, or user biometric and password change phases.
Biometrics-Based Privacy-Preserving User Authentication Scheme for Cloud-Based Industrial Internet of Things Deployment[37]	3	password, biometrics, smart card	mutual authentication, anonymity, hard to forge biometrics	stolen smart card,Privileged Insider, User Impersonation
A lightweight authentication and key agreement protocol preserving user anonymity[45]	2	password, smart card	0.0506ms computation time, anonymity	replay attack, insider attack, password guessing attack
A Lightweight User Authentication Scheme for Cloud-IoT Based Healthcare Services[46]	2	smart device, password	mutual authentication, forward secrecy	Impersonation Attack, capture attack, eavesdropping attack