# A Survey on Authentication Techniques for the Internet of Things

**Yahya Atwady**
School of Computing, Mathematics and Digital Technology
Manchester Metropolitan University
All Saint Building
Manchester M15 6BH
Yahya-mohammed.n.atwady@stu.mmu.ac.uk

Mohammad Hammoudeh
School of Computing, Mathematics and Digital Technology
Manchester Metropolitan University
All Saint Building
Manchester M15 6BH
M.Hammoudeh@stu.mmu.ac.uk

## ABSTRACT

Abstract The Internet of Things (IoT) is the technology, which forms the foundation of todayfis smart and connected world. The IoT is a network used to interconnect embedded devices, such as sensors, which are able to generate, communicate and share data with one another. In such an enormous network of interconnected fismart objectsfi, the identification of a specific object poses a fundamental task that influences all other functions of the system, such as its governance, privacy features, access control, overall architecture, etc. This paper presents a critical review of the prominent and recent authentication techniques for IoT objects. This is followed by a discussion of the limitations of current authentication techniques and future research avenues and opportunities.

**ACM Reference format:**
**Yahya Atwady** and Mohammad Hammoudeh. 2017. A Survey on Authentication Techniques for the Internet of Things. In *Proceedings of ICFNDS '17, Cambridge, United Kingdom, July 19-20, 2017,* 6 pages.
DOI: 10.1145/3102304.3102312

## KEY WORDS

Internet of Things (IoT); Authentication; Security; IoT; PUF; IDM

## 1 INTRODUCTION

Arguably, nothing affects our lives more than technology. Every day, it has something new to offer or it can provide us with new challenges to solve. However, technological advancements occur amidst a series of difficulties. Among the significant developments witnessed in technology, one such phenomenon is the Internet of Things (IoT). IoT is described as a network of interconnected things, objects or devices that are equipped with sensors, network connectivity and other essential electronics that enables them to collect and exchange data about their environment [3].

In large-scale networks of interconnected 'smart objects', the identification of a specific object rises a fundamental challenge that influences all other functions of the system, such as its governance, privacy features, access control, overall architecture, etc. Authentication is the process of identifying users and objects in networks to restrict access to authorized people and non-manipulated devices. Traditionally, authentication mechanisms rely on usernames and passwords, which can be easily compromised, need frequent changing, do not particularly suite unattended devices and broad range objects used do not support next-generation security functions. Their limitations become obvious as we try to connect devices of different vendors; most HTTP-based authentication protocols are bootstrapped through user interaction, which does not scale in IoT. Finally, smart objects often have constraints on resources including energy, memory, computational speed and communications bandwidth. Scarce resources necessitates only lightweight operations on the smart objects, particularly, if a distributed authentication is implemented to achieve scalability.

Cryptographic mechanisms present a robust way of securing the IoT against a variety of attacks, e.g., firmware tampering. However, cryptographic protocols incur high computation and communication load. Additionally, the specification IEEE 802.15.4 has key management problems and inadequate integrity protection. Consequently, the highly constrained IoT environment does not easily support cryptographic solutions. The gathering and use of data from smart devices that people interact with and control on a daily basis has several implications related to privacy. Not all privacy requirements can be satisfied only by the authentication schemes, but support for privacy at different levels is an essential property. The key challenge in a privacy preserving authentication scheme is to guarantee its ability to guard the possibility to link information from smart objects with a particular user or group of users. To illustrate, consider data about the location of a specific object. This, in itself does not raise a privacy concern, unless this object is associated to a specific user. This link makes the data valuable and deserving protection. Yet, the idea of ambient backed living and many of its applications are founded on the voluntary sacrifice of particular private information. Therefore, the challenge is how authentication schemes should provision the preservation of user's privacy, while also supporting the development of applications and scenarios, e.g., emergency call, where the user chooses to voluntary reduce his level of privacy?

This paper provides an in-depth survey of recent authentication methods specifically developed for IoT devices. After the introduction, Section 2 presents a survey of prominent and recent authentication methods developed specifically for IoT ecosystems. Section


*ICFNDS '17, Cambridge, United Kingdom*

DOI: 10.1145/3102304.3102312

3 identifies the current gaps in the literature and outlines future research avenues. Section 4 concludes the paper.

## 2 AUTHENTICATION TECHNIQUES FOR IOT

Establishing an object identity in IoT is critical to the privacy and security of the system users and owners. Therefore, efficient authentication techniques is crucial in order to establish secure and trusted IoT ecosystem. In this section we present a review of recent authentication IoT object authentication methods.

A One Time Password (OTP) authentication scheme for IoT, which is based on elliptic curves is presented in [16]. This method of authentication has been developed from pairing facilitated by elliptic curves. Private Key Generator (PKG) generates the OTP, and at the same time, it assumes the role of validation at the IoT platform. OTP generation occurs in a scheme that runs in four phases namely setup, extraction, generation, and validation. In the first phase, PKG produces a pair of numbers $p$ and $q$, which are prime numbers. In this scheme $p = (2)^2 \pm c$, where $c$ must be less than $log2n$. At the time $p = 3(mod4)$. On the other hand, $q|p + 1$ as a super singular elliptic curve. These parameters, which are primarily cryptographic are used to optimize the computations so that the resulting scheme is lightweight. In the second phase, IoT applications and devices register with the KPG and obtain private and public keys. These keys act as the torsion point on the elliptic curve. The third phase is the generation phase. In this stage, the authors assert that the application requests or sends data to the IoT device with an identification and an instance of time via a cloud platform. The PKG at the IoT cloud auto generates the key of the requesting device, which acts as the torsions point in this case. A new torsion point is generated for the device on the curve at that point and time. The requested data focuses on the new device and application. The final phase is validation. In this phase, this application and the device exchange data through OTP. Once OTP gets to the device, the device verifies the OTP as sourced from the application and if so, it accomplishes the task required. This method relies on the Lamport algorithm for its security by generating the OTP.

A certificate based authentication technique was presented in [8] to redress the issues of password based authentication. This technique requires that certification authorities issue certificates to users. Arguably, promoters of this method advocate that those who verify users' passwords at some point know those passwords or at least, data that is equal to them. However, this is different to viable certificate based authentication. The certificates are issued and certified by a remote authority who seals the link between them and the public cryptographic key. Certificate based authentication works under a very strict principle, providing that those who issue the certificates and those who award access be differentiated. The interconnection scenario proposed by [8] consists of a smart object, gateways and service. The smart object is divided into two classes according to its RAM and ROM size. Each gateway connects groups of objects in the Web of Things (WoT) Domain, and also to the local network or Internet as shown in 1.

For security, Datagram Transport Layer Security (DTLS) handshake protocol is used to authenticate clients on the server. Full DTLS handshake protocol is suitable for objects with large RAM and ROM size, but in many cases, IoT object/devices are limited in hardware resources [1, 4, 5]. To address this, the authors propose to delegate the initial handshake to the owner of an object. This approach assumes that the object has a unique identifier ID and secret key, and suggests that it should be embedded in the device at the manufacturing time. This authentication technique can be described in four major steps: 1. Out-of-band shared-secret exchange 2; Certificate-based TLS or DTLS handshake; 3. Session-state transfer; 4. DTLS session resumption.

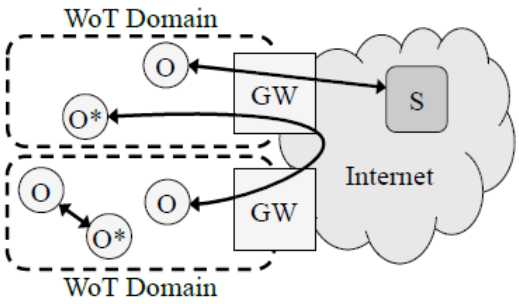


**Figure 1: Authentication network scenario as presented in [8]**

The authors of [15] propose an identity Management (IDM) system that focuses on providing access authorization as well as authentication for IoT users. The presented IDM and key-based authentication method provides single sing-on to IoT devices. This technique integrates four components, namely; the entity, in this case, the user, identity, in this case, their identifiers, identity providers, in this case, IdP and service providers. The work published in [18] suggest that an Identify provider (IdP) can manage the identity of users and their authentication characteristics; therefore, providing necessary credentials for their access to the system. In this process, credentials allow users to access the system while the service provider avails services to these users, according to the credentials they provide. A good example of this system is an open IdP [15]. There are works that have suggested the use of IDM in IoT, among other schemes that require user identification. Salman et al. [15] advocate that the IDM system for IoT would be easy to use and secure. Also, they believe that the method will enhance the operation of the system. The benefits of IdP are that it makes non-interactive login possible. This method provides better identity checks via a private keys. They are more secure than passwords, as malicious users must obtain the private key and their corresponding paraphrase to use the system.

Another IoT authentication technique that relies on patented hardware is presented in [13]. This technique is based on an intrinsic ID to provide IoT device authentication using its physical unclonable functions. A unique authentication process is used in the extraction of an IoT device security keys and its unique identifiers. These unique identifiers result from special traits of semi-conductors. Since these keys are only generated from the device unclonable features, they provide high level protection. The rationale behind this technique is especially true because the keys

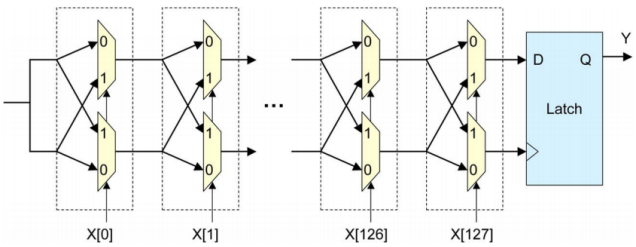


**Figure 2: Arbiter physical unclonable circuit. Adopted from [13]**

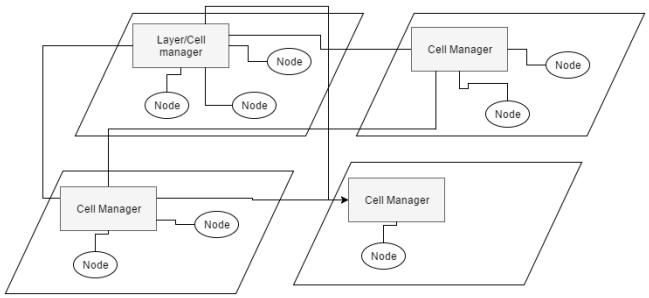


**Figure 3: Layer with cells and direct connection between nodes in different cells. Adopted from [11].**

are generated from the device on-board chips and their physical characteristics. Moreover, this method can be used to prevent identity theft through counterfeiting or cloning IoT devices. The proposed combines the use of the physical unclonable function and the elliptic curve cryptography. It is argued that the use of these technologies together will reduce the cost of tamper protection and lower the authentication computational and power requirements. The process of enrollment and authentication of the IoT device depends on gathering a public key from the device, continually generating the private key as needed, and without the need the to store that private key in the device. This technique is illustrated in 2.

Similar to [13], the work published in [9] focuses on authentication of devices in smart home environments using the physical properties of IoT devices and communications. The smart home environment use a variety of communication protocols. The proposed methods rely on using both the Physical Unclonable Function (PUF) and Physical Key Generation (PKG). The authors promote that the combination of the two methods results in an immediate enhancement of security. They also suggest reusing existing hardware to reduce overall system costs. The authentication process happens in four major steps. Firstly, the enrollment phase, which is done by the manufacturer who generates a random set of challenges that are presented to the PUF. The PUF responds to each challenge with a response $R$. Secondly, a function $W$ is used to generate the device secret key. This second step is referred to as the Key Generation Phase, which is carried on by the PKG to produce $K_i$ from the noisy channel of the PUF. This key is used as the symmetric encryption key. The third step is called the Authentication Phase, and in this stage, the hash of $K_i$ obtained from the last step is used to recover a challenge with a known response. The PUF knows all the valid challenges so, it generates the response $R_i$, using the helper Data function $W$. The hash of the response $h(R_i)$ is sent to the server encrypted by $K_i$. The final step is called the Re-enrollment Phase. This phase is done when a secure connection between the device and the server is established. In this step, a set of new valid challenges, responses and helper data, are all replenished.

A security approach that depends on grouping nodes into layers is proposed in [11]. Each layer has a layer manager and one or more cell. Every cell has a cell manager, which controls the communication with other cells. The authentication process is done either directly or indirectly. Direct authentication is performed between peer nodes in the same cell, which requires that any node knows the certificate of its peer in advance. In indirect authentication, a node must contact its cell manager in order to get its peer certificate. Where nodes belong to different cell managers, indirect authentication is done between these cell managers using the certificates issued by their layer manager. This distributed security management approach is illustrated in 3.

In Peng's [14] study, an ID-based authentication approach is proposed. In this technique, every node is authenticated by its neighbor's ID, which is distributed to each node once it connects to the network. The data is aggregated at each Node, along with its authenticated neighbor's ID, and sent to the sink node through its aggregator. The authentication process is performed at the sink that maintains a binding list of the nodes authentication neighbors' ID. Once authentication is successfully confirmed, the data is extracted.

Authentication and Access Control (ECC) in the Internet of Things was proposed by [12]. It uses two trusted authority models; the Registration Authority (RA) and the Home Registration Authority (HRA). When a user wants to access an object, the object issues an authentication request to the RA. Then, the RA asks for the user ID and contacts the HRA for user verification. The HRA verifies the user and sends the result back to the RA. Finally, when the verification process has been successfully achieved, the RA issues a session key, which is used in communication with the user, based on ECC.

Recently, Jan et al. proposed a robust authentication scheme for observing resources in IoT environments [10]. Their authentication scheme adds security features to the Constrained Application Protocol (CoAP) in order to perform secure client-server communication. The authentication process is performed in four-way handshake messages based on a pre-shared key between the client and the server. Firstly, the client sends its ID to the server. Then, the server retrieves a pre-shared key from its lockup table, generates a session key and a nonce, encrypts them in a message, and sends it back to the client. In the third step, the client decrypts the message, extracts the session key, and replies to the server with an encrypted message that contains the nonce. Finally, the server verifies the nonce after decrypting the message using the session key and acknowledges the authentication.

More recently, Salman et al. [15] published an identity-based authentication scheme for IoT. This network security solution is patented. The method includes a Software Defined Networking (SDN)

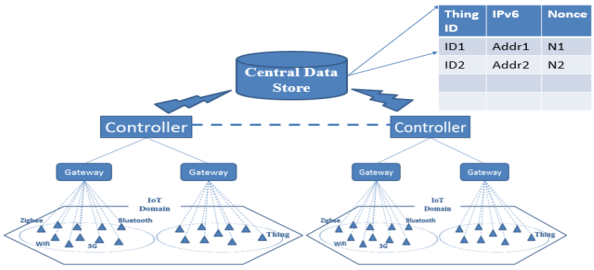


**Figure 4: Illustration of the identity controller gateway structure adopted from [15].**

**Table 1: Authentication Process Classification**

| | DSM | OTP | CBA | IDM | PUF |
|---|---|---|---|---|---|
| [16] | | ✓ | | | |
| [8] | | | ✓ | | |
| [18] | | | | ✓ | |
| [15] | | | | ✓ | |
| [17] | | | | | ✓ |
| [9] | | | | | ✓ |
| [14] | | | | ✓ | |
| [12] | | | | ✓ | |
| [10] | | | ✓ | | |
| [11] | ✓ | | | | |

controller, which is responsible for authenticating and managing all the gateways and nodes in the network, as shown in 4.

The authentication process consists of three major phases. During phase 1, the gateway acquire a public key certificate from the controller. In phase 2, the controller generates a hashed IPv6 using the object/thing ID, a randomly generated nonce sent by object, and the gateway certificate that connects the node to the controller. In phase 3, the node authenticates itself using the hashed IPv6 and nonce signed by the gateway public key.

The reviewed authentication techniques can be classified according to the following authentication process: Certificate Based Authentication (CBA), OTP, IDM, Distributed Security Management (DSM) and PUF. 1 presents this classification.

IoT authentication techniques can also be classified based on the encryption methods used. Encryption plays a critical role in authentication authentication processes. The hardware limitations of IoT devices makes the utilization of complicated encryption techniques impractical or even impossible. In the literature, different authentication approaches used various types of encryption algorithms, as shown in 2. This table shows that majority of the reviewed methods use asymmetric encryption. To solve the problem of large key sizes, most of these methods used Elliptic Curve Cryptography (ECC) to handle the encryption.



**Table 2: Classification of authentication approaches by employed encryption methods.**

| | Symmetric | Asymmetric |
|---|---|---|
| [16] | | ✓ |
| [8] | | ✓ |
| [18] | ✓ | ✓ |
| [15] | | ✓ |
| [17] | | ✓ |
| [9] | ✓ | |
| [14] | | |
| [12] | | ✓ |
| [10] | | ✓ |
| [11] | | ✓ |

## 3 GAPS AND OPPORTUNITIES IN CURRENT IOT AUTHENTICATION TECHNIQUES

### 3.1 Poor Transport Encryption

One critical shortfall of current IoT ecosystems is the lack of reliable and secure communication channels. IoT devices transmit and receive sensitive data through networks regularly. Recently research was conducted on IoT devices to determine their effectiveness in securing the data they transmit [16]. The majority of tested devices failed to encrypt the network protocols to transmit data through the Internet and local networks. The authors also claim that the role of encryption within the system is difficult to support. This claim have strong merits, especially since data is transmitted through several times, from the device, the gateway, to the cloud platform and the application in use. Sensitive IoT data breaches occur almost every day at a large scale. Organizations that fail to encrypt their data and communication links can not escape the cost that comes with such security breaches, e.g., fines, forensic investigations, credit monitoring for clients, brand damage and litigation costs. These are expenses all IoT stakeholders want to avoid. Similarly, the reviewed papers studies did not explore the importance of end- to-end encryption in IoT and failed to stress its importance.

Another shortfall noted under this category is the poor symmetric encryption key management. The reviewed approaches discussed in this survey have overlooked this limitation. The challenge here is for the user to establish a method by which they can safely distribute the key to the intended parties to provide access authorization [17]. Due to the possibility of communications interception, the transmission of these keys poses new security challenges.

Another shortfall is the shared key access mechanism itself. The difficulties arising from this mechanism are magnified due to the ease with which the key can be misused. The prime issue here is that whoever has the key can decrypt everything within the network. This problem can lead to a compromise of information, as it is being shared between several parties who are able to view each others data.

Effective and reliable authorization and encryption are yet to be developed to protect IoT systems against cyber criminals and

**Table 3: Summary of the strengths and weaknesses of the reviewed approaches.**

| Author | Proposed Technique | Strengths | Weaknesses |
|---|---|---|---|
| [8] | Certificate-based DTLS handshake delegation method | Reduce overhead of certificate based authentication | Need change to be done on DTLS Protocol |
| [18] | A middle gateway devices pass content from the IoT device to Internet and vice versa | Node is isolated from security attacks | New layer of hardware must be implemented |
| [15] | Gateway, controller and central data store authentication architecture | Use IPv6 address as a node identifier | Single point failure in case of CDS failure |
| [14] | ID-based multiple authentication scheme | Strong ability to prevent different attacks | Requires changes to current IoT architecture |
| [12] | Session key issued after RA and HRA negotiation | Remove the overhead of authentication from the node | Single point of failure |
| [10] | Four-way handshake added to CoAP protocol | Distributed-base solution | Vulnerable to Sybil attack |
| [11] | Nodes are grouped into layers managed by layer manager | Provide simple efficient authentication using DH key exchange | Not tested against known attacks |
| [16] | One time password using IBE-ECC | Smaller key size and no need for storing passwords | Requires changes to current IoT architecture |
| [9] | Use PUF and PKG to provide security and authentication | Abandon factory-deployed static keys needs | Requires hardware change |
| [17] | PUF-based protocols over elliptic curves | Low computational and storage requirements and low-cost tamper | Requires hardware change |

messages interception. There is a clear need for enhanced ways of key distribution and maintenance, e.g., key encryption.

## 3.2 Password Limitations

The methods of authentication discussed in this survey have undermined the limitations of the one password scheme. They claim that OTP can withstand replay and modification attacks. Based on all of the information presented, this view is considered to be flawed. It was proven experimentally in [17] that experienced attackers may login to systems like properly authenticated users. If an attacker were able to intercept messages transmitted, at the login stage, they could replay it and access the system. Furthermore, with this type of authentication, once the attacker logs in to the system for the first time by impersonating a legitimate user, they can continue the attack other users without necessarily intercepting the messages again.

Unlike certificates, passwords are vulnerable to phishing attacks. The concept of asymmetry is the cause of this difference. In practice, certificate users do not reveal secret data to peers. As a result, attackers who impersonate servers do not learn anything of value from users.

Future work to address the limitations of the password system is that servers can be modified to protect their messages from first time attacks. New secure communication methods that rely on a key that is only shared between the two communicating users is needed. After users register with the system, authentication is then linked to and characterizes the user whose identity is verifiable via a series of steps. These steps would enable the system to determine when they would reject a login.

## 3.3 Faulty or Complex IoT Systems

Another limitation in the studies reviewed, is the inability to use IoT with a robust communication protocol stack. Various system layers introduce significant amount of computation and communication overhead. Furthermore, within the layers themselves, higher layers are unable to see what is in the lower layers. The effects of this problem becomes apparent when network connections are unreliable. As a result, IoT devices may be unable to adapt their transmissions and applications to the current network conditions, even if it is beneficial to do so [17]. Additionally, these layers are unable to specify alternatives when problems arise within the system. These problems are compounded by the system every time they occur, which makes the IoT system an open target for attackers.

This challenge provides exciting opportunities for IoT development. One such opportunity is the chance to address the problems that come with network connectivity. Resolving network problems and connectivity issues promotes efficient and safer IoT systems. This would be particularly helpful when robust connections are difficult to achieve. Another improvement opportunity is to encourage computer professionals to reduce the number of layers that exist within the communication protocol stack. This reduction would reduce the data communication complexity, hence minimize chances of interception.

Another limitation identified from the literature survey is overlooking the use of single sign-on in the system. This authentication and access control method is fast, efficient, user friendly and less costly. This authentication method makes it easier for cyber criminals who pretend to have forgotten their passwords, while in

reality, they are impersonating somebody else. Yet, this authentication scheme has very attractive features and should be further investigated and tested in IoT ecosystems.

### 3.4 Financial Implications

Another challenge that appears to have been overlooked by the reviewed studies reviewed is the limited resources, especially in the area of certificate-based authentication. Certificate based authentication is expensive. This scenario is even worse when it requires extensive use with millions of IoT devices. The primary reason for the expense is that it requires a support by a reliable public key infrastructure.

### 3.5 Insecure Interfaces

Another challenge hindering the implementation of reliable authentication methods in IoT systems is the access platforms and vulnerable user interfaces. According to [16], at least six out of ten devices tested indicated concerns with their web access interfaces. These concerns are issues around as poorly managed sessions, weak default credentials, and persistent cross site blocking. With features that allow password recoveries, the majority of devices, along with their mobile counterparts enabled attackers to identify and use valid accounts.

### 3.6 Faulty Authentication and Authorization

Experiment conducted by the authors of [16] on more than ten authentications techniques shown that at least four of techniques were faulty. Half this number were open for impersonalized access. The impersonation was made possible by poor passwords, risky password recovery mechanisms, and poorly defended login credentials. As discussed by the authors, the majority of devices, along with their cloud, failed to demand passwords that were sufficiently secure. Strong passwords require the incorporation of numeric values, alphabetic and special characters. Most devices failed to meet such requirement. Therefore, there is a need to test and evaluate authentication and authorization techniques by independent security experts or organizations before companies are allowed to sell their IoT products in the market.

### 3.7 Security flaws in Devices Software and Firmware

Most of the current IoT devices do not encrypt their communication over the local network or even the Internet. This leaves the IoT system open to interception attacks that may have considerable consequences on users privacy. Therefore, reliable mechanisms to ensure data integrity and secrecy are needed.

## 4 CONCLUSION

In summary, the time when all things will act together in synchronization is here [2, 6, 7]. There is no doubt that the IoT technological trend, along with its inherent security changes is gaining more popularity. It is predicted that, within the next five years more billion of devices will be connected to the IoTs. With the adoption of IoT in critical applications, such as healthcare, the consequences of insecure IoT devices would be potentially catastrophic. Fortunately, there is a solid security infrastructure provided by our knowledge of classical networks and the skills and resources required to secure the IoT are available. First, manufacturers need to thoroughly test their web interfaces for possible weaknesses. Second, they should set security standards to manufactured IoT devices to ensure that they offer reasonable security. Lastly, and perhaps most importantly, they should ensure that IoT devices undergo continuous tests for security

## REFERENCES


[1] Abuarqoub, A., Hammoudeh, M., Adebisi, B., Jabbar, S., Bounceur, A., and Al-Bashar, H. (2017). Dynamic clustering and management of mobile wireless sensor networks. *Computer Networks*, pages –.

[2] Abuarqoub, A., Hammoudeh, M., and Alsboui, T. (2012). *An Overview of Information Extraction from Mobile Wireless Sensor Networks*, pages 95–106. Springer Berlin Heidelberg, Berlin, Heidelberg.

[3] Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805.

[4] Bounceur, . O. A. A. A. M. H. U. R. A. (2016). Unmanned ground vehicle for data collection in wireless sensor networks: Mobility-aware sink selection. *The Open Automation and Control Systems Journal 8*.

[5] Hammoudeh, M., Al-Fayez, F., Lloyd, H., Newman, R., Adebisi, B., Bounceur, A., and Abuarqoub, A. (2017). A wireless sensor network border monitoring system: Deployment issues and routing protocols. *IEEE Sensors Journal*, PP(99):1–1.

[6] Hammoudeh, M., Aldabbas, O., Mount, S., Abuzour, S., Alfawair, M., and Alratrout, S. (2010). Algorithmic construction of optimal and load balanced clusters in wireless sensor networks. In *2010 7th International Multi- Conference on Systems, Signals and Devices*, pages 1–5.

[7] Hammoudeh, M., Newman, R., Dennett, C., and Mount, S. (2013). Interpolation techniques for building a continuous map from discrete wireless sensor network data. *Wireless Communications and Mobile Computing*, 13(9):809–827.

[8] Hummen, R., Ziegeldorf, J. H., Shafagh, H., Raza, S., and Wehrle, K. (2013). Towards viable certificate-based authentication for the internet of things. *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy - HotWiSec '13*, page 37.

[9] Huth, C., Zibuschka, J., Duplys, P., and Güneysu, T. (2015). Securing systems on the Internet of Things via physical properties of devices and communications. *9th Annual IEEE International Systems Conference, SysCon 2015 - Proceedings*, pages 8–13.

[10] Jan, M. A., Nanda, P., He, X., Tan, Z., and Liu, R. P. (2014). A robust authentication scheme for observing resources in the internet of things environment. pages 205–211.

[11] Lincke, N., Kuntze, N., and Rudolph, C. (2015). Distributed security management for the iot. pages 1373–1376.

[12] Liu, J., Xiao, Y., and Chen, C. L. P. (2012). Authentication and access control in the internet of things. pages 588–592.

[13] Mukhopadhyay, D. (2016). PUFs as Promising Tools for Security in Internet of Things. *IEEE Design and Test*, 33(3):103–115.

[14] Peng, S. (2012). An id-based multiple authentication scheme against attacks in wireless sensor networks. 03:1042–1045.

[15] Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A., and Kayssi, A. (2016). Identity-based authentication scheme for the internet of things. pages 1109–1111.

[16] Shivraj, V. L., Rajan, M. A., Singh, M., and Balamuralidhar, P. (2015). One time password authentication scheme based on elliptic curves for internet of things (iot). pages 1–6.

[17] Wallrabenstein, J. R. (2016). Practical and secure iot device authentication using physical unclonable functions. pages 99–106.

[18] Witkovski, A., Santin, A., Abreu, V., and Marynowski, J. (2015). An idm and key-based authentication method for providing single sign-on in iot. pages 1–6.