Internet of Things (IoT) Security: A Survey of Challenges and Possible Solutions

Mehdi Himmiche
ARTIS College of Science and Technology, Radford University, Radford, VA 24141 USA

IoT networks have seen an increase in the last few years, from complex interconnected networks, to medical equipment, to simple devices found around the household. This increase in use, however, did not see a match in increase of security for such devices. By looking at multiple solutions offered to tackle the IoT security problem, and determining the challenges that researches face in their research, I hope to demonstrate that the next step in research should be focusing on ways to implement these solutions, as these devices and networks are already widely available and being used increasingly be people who are not seccurity savvy.

***Index Terms*—Internet of Things, IoT, Security**

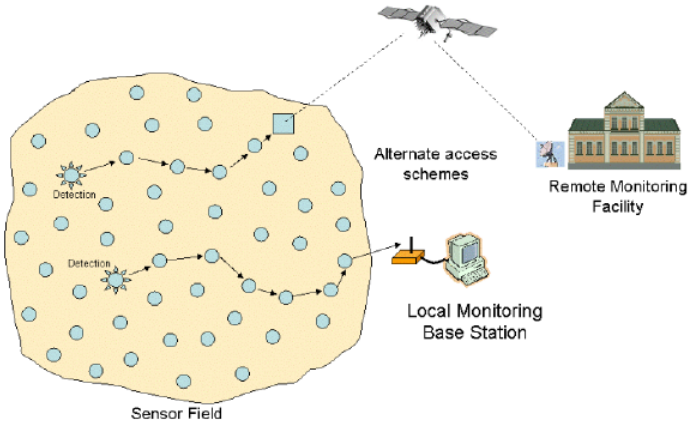

Fig. 1. Example of IoT network

I. Introduction

With the rise in usage of Internet of Things (IoT) devices, a focus on security becomes important. IoT is defined as "A network of internet-connected objects able to collect and exchange data using embedded sensors." [1]. Such definition allows for multiple devices to be considered, from complex drone networks as seen in Fig. 1, to medical sensors used to keep patients alive, to every day items such as fridges and "smart homes." All these devices allow for every day user to remain interconnected within the ever moving landscape surrounding them.

IoT networks provide many benefits, and have allowed scientists to make leaps and bounds in improving every day lives; from allowing the creation of "smarter labs" to allow for better food and beverage research and development [2], to helping scientists improve chemical reactions - "Based on the softwares assessment, it could suggest optimal reaction conditions, specific synthetic routes, or even compounds to evaluate" [3].

Although IoT provide numerous benefits, they also come with challenges, especially when it comes to ensuring that the date they collect is secure. In fact, IoT face a huge challenges in their being computationally weak - they do not have the same computational resources as traditional systems, therefore, "Traditional security mechanisms are no longer applicable because of the involvement of resource-constrained devices, which require more computation power and resources." [4].

In this survey paper, I will explore current research in the field of IoT security, discuss some of the challenges researchers are facing in this domain, as well as propose further research to possibly overcome some of these challenges.

II. Approach to Explain the Topic

The architecture of IoT devices is not unlike any other such systems, it relies on a layered approach to help ensure all communication amongs "things" works properly [5]:

- sensing layer: integrated with end components of IoT to sense and acquire the information of devices
- network layer: the infrastructure to support wireless or wired connections among things
- service layer: provide and manage services required by users or applications
- application-interfaces layer: consists of interaction methods with users or applications

By designing IoT devices in a 'layered' manner, much like the OSI or TCP/IP layer mode, IoT can allow for multiple a guideline for developers to follow, as well as compartmentalizing the work that each node in an IoT network must accomplish.

The layer architecture of IoT devices creates the challenge that each layer must now be secured, with each layer having its own set of requirements that may not allign with other layers, even being contradictory with other layers' security requirements; i.e. the sensing layer must allow all information to flow through it as to gather the most data, while the network layer must ensure that only 'correct' information is being transmitted. Not every organization agrees on the exact number of layers that exist within the IoT field, some use less layers, while others use more. Fig. 2 shows an example of how the layers model can be used.

As previously stated, IoT devices suffer from having very little computational power [4], forcing researchers to look at developing less resource intensive ways to insure that data

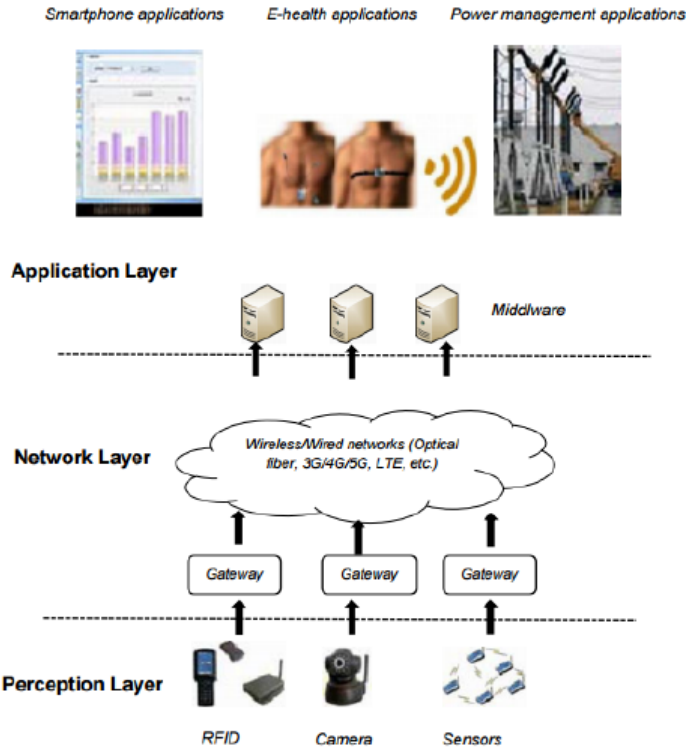

Fig. 2. Example of layers model used in IoT

being transfered is secure and safe.

IoT networks will cause a giant shift in how end users consume information, just as much as the invention of the INTERNET caused the leap, by allowing any default, 'dumb' device to communicate with other devices, end users can power and connect their entire lives, making everything in their surrounding interconnected. It falls on the IoT developers and designers to ensure that the consumer's data and information is secure at all stages, from collection to use and consumption. By focusing on security, designers can ensure that this revolutionary step in distributed computing can truly benefit everyone without causing any major breach.

III. Existing Research Issues on the Topics

There exists multiple schools of thought when it comes to IoT security, with some focusing on the specific layer models develkoped, others paying more attention to securing the base stations in the IoT networks topologies as seen in Figures 1 and 3. Some researchers focus on developing better encryption and methods to secure data at rest, or obfuscating the data during transfer. Other researchers suggested that the secret to ensuring data security is focusing on physical security on each node in the IoT network. By looking through each of the different approaches, we can get a better understanding at what could be the most optimal way to ensure data is protected from breaches.

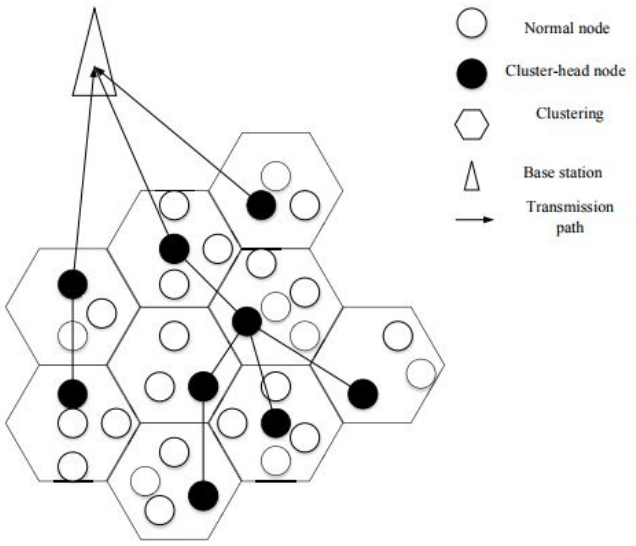

Fig. 3. Network topology for IoT networks

A. Layer Security Approach

In order to understand the methods to ensure data safety, we must first understand what kind of attacks IoT networks at each layer. By gaining a better understanding at the threats and vulnerabilities at each layer, better solutions can be developed to mitigate these vulnerabilities and prevent, or rather minimize possible exploitations of these vulnerabilities.

1) Sensing Layer

Some of the vulnerabilities that the sensing layer in IoT devices face include:

- Unauthorized Access: An attacker can gain physical access to the node, or exploit a vulnerability in the software to gain access to the data being collected.
- Spoofing Attack: An attacker can masquarade a malicious node as a good one, causing the IoT network to receive and process false or malicious data.
- Denial of Service (DoS): An attacker can cause the node's resources to not be available for usage.
- Routing Attacks: Attacking the routing of the nodes.
- Transmission Attacks: Attacking the transmission of data; includes interuptions or disruptions, diversion of data. Encompasses multiple other exploitations and possible threats.

The threats present at this layer can then be classified as either physical threats, gaining direct access to the node and manipulating it, or threats to the data collected by each node on the IoT network.

2) Network Layer

The Network Layer in an IoT faces many of the same challenges as the Sensing Layer, bar the threats that deal with physical access. Some of the threats unique to this layer include:

- Malicious Code

- Public key and Private key: A compromise to the keys used to communicate can cause data to be leaked to unauthorized parties.
- Node Mapping: An attacker could map the location and number of nodes in an IoT network to get a better strategic understanding (perform reconnaissance on the network).

The threats present in this layer are not unique to IoT networks, these are threats that are inherintly present within each network, though they can be mitigated and minimized if the network is setup and onfigured properly.

3) Service Layer

While the Service Layer manages the services required, it does face threats that could cause disruption to the stream of data. Such threats include:

- Service Discovery: An attacker can discover the services running on the netowkr, leveraging each service's vulnerabilities for greater access.
- Attack on Trustworthiness: As this layer handles establishing trustworthiness between the users and the network, an attacker could cause a disruption by allowing or disallowing the wrong users access.

The threats facing this layer are much like ones facing Domain Controllers in traditional networks, or any service running on a traditional network for that matter (web servers, databases... etc), as this layer can serve as the 'nervous system' to the entire IoT network. Ensuring that this layer is protected is of the utmost importance.

4) Application Layer

This layer, being the most user facing one, faces similar threats that we are accustomed to in traditional networks. Threats such as misconfiguration, security management... etc, are all present within this layer. This one is the most easy to understand as it translates directly to the application layer in traditional networks.

5) Analysis of This Approach

Reading through this approach, it becomes clear that it is designed to be very thorough; it attempts to cover as many threats as possible between each layer, ensuring that each one is as secure as possible could mean that the entire network is fairly secure. There are limitations however. This approach assumes a sort of 'rigidity' in the network; it assumes that the IoT network will do the same thing, therefore it can be configured to ensure that every layer is the most secure. In an ideal world, every layer would be secured equally; to the most secure configuration possible. In a real situation however, some of the layers may end up not being secured properly, and if one of them causes a disruption to the network, or facilitates a denial of service in the resources of the network, the network itself becomes 'useless.'

This approach does not take into account human error when it comes to configuration, assuming that everything would be set up appropriately, ignoring human laziness or malice. It also assumes that administrators and network engineers can devote all the needed time to ensure that each layer is properly secure - in a perfect world, this would be ideal. It becomes quicly apparent that a better solution may be to devote as much time and resources to protect critical sections of each layer, weighing the pros and cons of leaving some aspect insecure. This decision could allow more flexibility for the designers, and the organizations, to be able to tailor theit IoT networks appropriately.

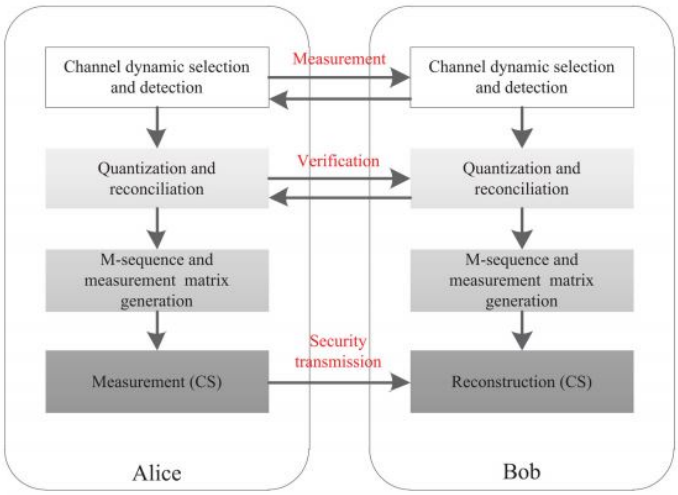

Fig. 4. Proposed physical layer security approach [6]

B. Physical Layer Security Approach

Within this context, physical layer security refers to the ability of a wireless network to exchange confidential messages in the presence of eavesdroppers, without relying on higher-layer encryption [7]. Physical layer security can be split into two general categories, key-extraction based which rely on generating an extraction key in order to establish the communication, and keyless security in the physical layer security. In the case of the former, the generation rate for keys is still relatively slow, which is not ideal for the quick communication nature of IoT network communication [6]. While in the latter, the keyless physical layer security, comunication resources can be occupied as it takes resources to communicate (artificial noise being on the primary means) [6]. A combination of physical layer security and compressed sensing - where data is efficiently sampled then reconstructed by the receiving node - has been demonstrated to show promising results. In [6], the authors propose a new framework, shown in Fig. 4, to establish physical layer security combined with compressed sensing.

As noted in [6], compressed sensing relies heavily on static environments, which could cause a lot of issues for IoT networks. First off, static environments can lead to a stationary signal, causing lower randomness. The lower randomness can cause the information to be extracted easily and imitated. In [6], the authors reference a previous work that showed that an attacker does not need a precise measurement matrix to reconstruct the compressed signal.

To address the issues mentioned regarding compressed sensing, [6] proposed a new compressed sensing scheme based on resilient functions and circulant matrix. As shown in Fig. 5, the simulation of the proposed solution displayed an almost identical recovered electrocardiograph (ECG) when compared to the original ECG.

Although the proposed solution for the physical layer security approach is novel and very interesting, there stil exists a lot of research to be done in order to ensure proper security. According to cited work by [6], compressed sensing based encryption does not achieve perfect secrecy, but it does provide a computational guarantee of it. If that is the case, this solution only covers one aspect of security when it comes to IoT networks, which is data transfer. Although this is limited to current computational power, i.e. as computational power increases, settling for a computational guarantee might not be enought o guarantee security.

This approach focuses only on one security aspect for IoT networks, an attacker gaining access to a node can still send perfectly encrypted messages to other nodes. Although it could prevent such attacks as man-in-the-middle attacks, and increases the complexity to breaking the communication, it doesn't handle every possible scenrio when it comes to a full network communication and implementation.

C. Other Approaches and Challenges

One of the biggest challenges faced in IoT networks is the fact that data collected by each node isn't structured by nature. Developers can attempt to structure it but that may defeat the purpose of such networks.

Many security approaches exist that attempt to create some sort of structure to the collected data to make it easier to secure the network. Other created systems that attempt to create a model of the data collected as well as the IoT configuration, making it easier to detect and stop malicious nodes in the network [8]. The approach queries the configurations of the network in the context of IoT interactions and dependencies.

The solution provided in [8] provides a scalable approach to IoT security; configuration and node interaction queries can be run periodically allowing updates to happen as quickly as desired. It allows for a "hands off" approach; the system checks everything and detects malicious behaviour as it sees fit based on the configuration model it creates. Such an approach may be ideal in the fact that it removes human error from the equation. Although it does seem to rely on proper initial configuration of IoT network; the queries and model it creates assume that the network was created properly. The solution also ignores malfunctions in the network, as it could assume that a malfunctioning node is a malicious node.

Another possible solution to the IoT security problem involves relying on data fusion; integrating multiple data sources to produce a more consistent, accurate, and useful information [9]. This solution attempts to find a more optimal way for communication sharing without increasing resources,

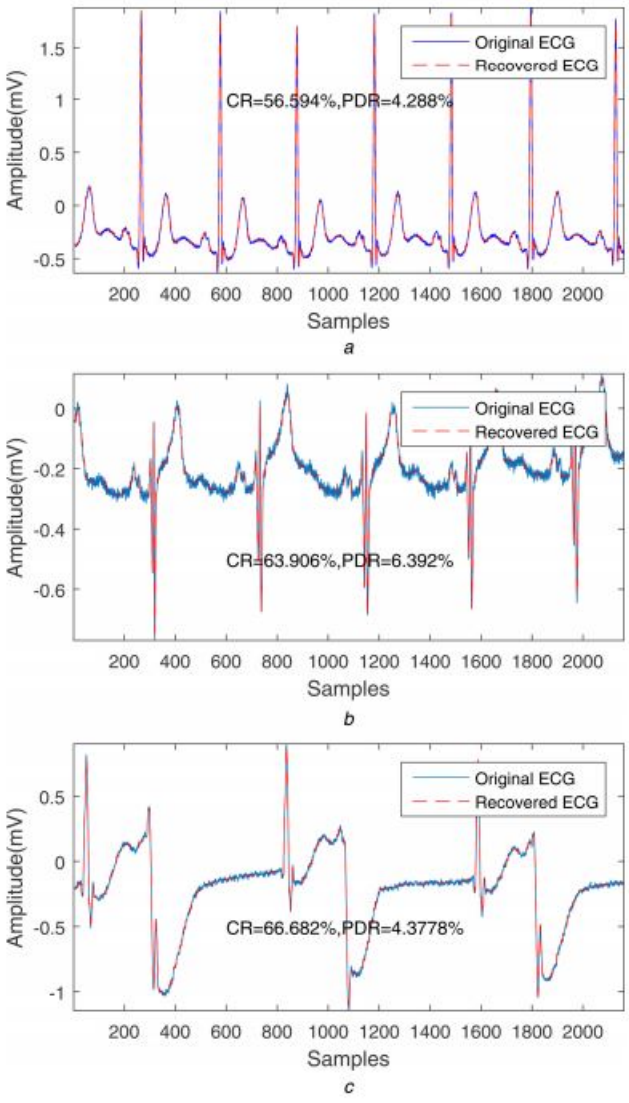

Fig. 5. Performance of the proposed security scheme in [6]

as "relevant research shows that the algorithm security is positively related to the consumption of resources" [10] - i.e. the more resources consumed, the more security needed to ensure the IoT network is up. This solution takes a different approach to security, instead of focusing directly on it and attempting to increase it, the oslution focuses on reducing the increased overhead - attempting to minimize security in this case.

Though it may not focus directly on security, such an approach should not be discredited. By limiting the resources required, and minimizing the security needed, more resources can go into the 'little' security required for communication. By taking such an approach, this solution attempts to reach a tradeoff that could be tipped towards focusing on security in the long term.

Through Fig. 6, [10] achieved a nearly identical performance between a data fusion algorithm (EDCSDA) and a simple ID encoding method. Such a result demonstrates that it is

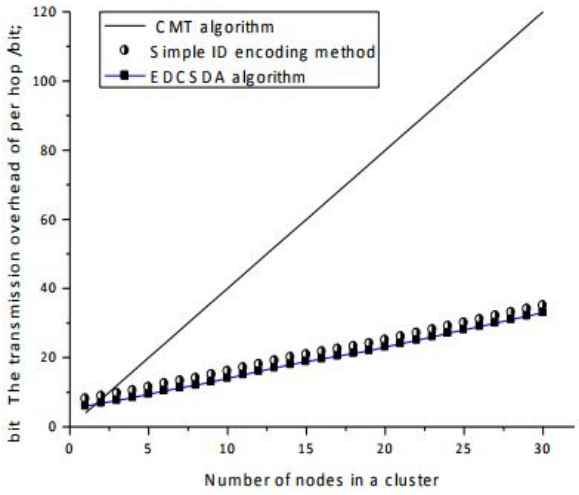

Fig. 6. Comparison between data fusion algorithm and simple encoding

possible to take full advantage of data fusion algorithms in IoT networks without having to give up on performance and/or security - in fact, by limiting the resources needed, each node has more resource available for other tasks, which in our case can be tasks to improve the security of the node itself.
Although this solution is promising, testing it with a bigger number of nodes would be something that would be more beneficial; it could give a better understanding of performance and resource usage. The solution, by itself, is also not a guarantee of security - it works on freeing resources to focus on security but it doesn't have a built-in measure for security.

IV. Possible Future Research Issues on the Topic

Through the presented work, it is clear that the field of IoT security is still relatively young, with many solutions being offered to solve the challenges faced, and even more challenges rising every day.
Some solutions offered go into too much security detail, ignoring the usability and scability that is offered by IoT networks. While other solutions focus only on one single aspect of secure communication, rendering it difficult to implement in real life. This is not to say that research shouldn't focus on specific aspects, in fact such research is valuable when it is paired with other research that focused on different aspect, creating a full usable model to ensure security for such networks.
There are, however, multiple limitations when conducting security research on IoT security, mainly the fact that they do not offer a lot of computational power to 'defend' themselves, whilst adversaries are using high end, extremely powerful machines and botnets to carry out their attacks - this puts security professionals at a disadvantage against the adversaries. IoT networks, in a sense, still rely on classic network structure as well (the nodes must communicate to a central server), adding even more vulnerabilities to the system.
I do believe that the next step in research should be to combine multiple focused research to create usable application to protect the millions of current IoT devices currently connected to the internet. Focusing on using data fusion algorithms to minimize resource usage, combined with compressed sensing for secure communication, as well as a scalable solution such as offered by [8], one could reach applicable solution to increase the security posture of IoT networks.
Another important step to take would be researching ways to make the layers model approach more scalable and less rigid, although security is extremely important, it shouldn't come at the cost of usability - a very secure product that doesn't get used is not a product that the end user will care about adopting.
Researching better communication algorithms between nodes is something that is also incredibly important, if redundancy and availability become the norm of IoT networks, a node going down or sending wrong data would not affect the whole system as much. An approach to solve this problem would be having multip[le nodes close to each other, each sending their data back to the base station. The base station would then compare all the data it receives at any given instant, detecting any anomalies - each data point would have its location with it, allowing the base station to distinguish between different readings from different regions and readings from close nodes. If a node is found to be eroneous compared to neighbor nodes (after sending a certain number of 'wrong' data), the base station could disconnect it or put it in 'quarantine' where an administrator could make the final decision on whether the node should remain in the network or be removed.

V. Concluding Remarks

IoT security has made great strides in the past couple of years, allowing for the rolling out of millions of devices. Although there is still lots of research to be done, steps in the right direction are being taken to ensure that all the users' data remains secure.
Although some research in the security of these networks is focused on very specific aspect, such as the communication between nodes, other research focuses on a broad picture of security policy or implementation. Both serve an important role when it comes to creating secure IoT networks that affect millions of people's daily lives. I believe the next step in research should be ocmbining more that one previously established research to see how such a combination would affect the overall security posture of IoT networks without affecting the inherent scalability and not affecting the end user's experience with the product.

REFERENCES

[1] Meola, A. (2017). What is the Internet of Things (IoT)?. Business Insider. http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8

[2] Internet of Things for Food and Beverage R&D. (2017). Tetra-Science Blog. http://tetrascience.com/blog/internet-of-things-for-food-and-beverage-r-d/

[3] Transforming chemistry with machine learning. (2017). Tetra-Science Blog. http://tetrascience.com/blog/transforming-chemistry-with-machine-learning/

[4] Yaqoob, Ibrar, et al. "The Rise of Ransomware and Emerging Security Challenges in the Internet of Things." Computer Networks, vol. 129, Dec2017 Part 2, pp. 444-458. EBSCOhost, doi:10.1016/j.comnet.2017.09.003.

[5] Li, Shancang, et al. "The Internet of Things: A Security Point of View." Internet Research, vol. 26, no. 2, Mar. 2016, pp. 337-359. EBSCOhost, doi:10.1108/IntR-07-2014-0173.

[6] Ning, Wang, et al. "Physical-Layer Security in Internet of Things Based on Compressed Sensing and Frequency Selection." IET Communications, vol. 11, no. 9, June 2017, pp. 1431-1437. EBSCOhost, doi:10.1049/iet-com.2016.1088.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, Third Quarter 2014. doi: 10.1109/SURV.2014.012314.00178

[8] Mohsin, Mujahid, et al. "Iotchecker: A Data-Driven Framework for Security Analytics of Internet of Things Configurations." Computers & Security, vol. 70, Sept. 2017, pp. 199-223. EBSCOhost, doi:10.1016/j.cose.2017.05.012.

[9] M. Haghighat, M. Abdel-Mottaleb, & W. Alhalabi (2016). Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition. IEEE Transactions on Information Forensics and Security, 11(9), 1984-1996.

[10] Jie, Zhang. "Security Technology of Wireless Sensor Internet of Things Based on Data Fusion." International Journal of Online Engineering, vol. 13, no. 11, Nov. 2017, pp. 25-36. EBSCOhost, doi:10.3991/ijoe.v13i11.7748.