A Study On Node Authentication and Identification In IOT Based Smart Homes

Naif Waheb Rajkhan *rajk4446@vandals.uidaho.edu*
Computer Science Department
University of Idaho
Moscow, ID, 83844, USA

Jia Song *jsong@uidaho.edu*
Computer Science Department
University of Idaho
Moscow, ID, 83844, USA

Abstract

Smart home is one of the most popular Internet of Things (IoT) implementations. It is widely used because of the autonomous functions that it provides to homeowners. Smart home is equipped with smart IoT devices that are designed to perform special and specific functions automatically. The IoT smart home network has different types of connections based on the application's requirements. Any attacks or unauthorized access to IoT smart home system or to the connected devices, could harm the system and may lead to unauthorized access to the homeowner's information. Therefore, such devices in the smart home system must adopt the best and recent security and privacy standards to better secure the sensitive information about the homeowners. Node/device authentication is a crucial challenge in the security of smart homes. Depend on the types of devices, different node authentication mechanisms are used in smart homes. This paper analyzes the widely used mechanisms for IoT device authentication and identification in smart homes, along with possible threats that are related to them. There are different node authentication challenges at smart home that should be resolved by researchers and smart home devices' manufacturers. The goal of this paper is to provide an analysis and comparison of the major IoT device authentication mechanisms so that the findings from this research can help other researchers and developers to choose the proper one that best suits the needs of a specific system environment.

Keywords: Internet of Things (IoT), Smart Homes, Node Authentication, Smart Home Devices.

1. INTRODUCTION

Recently, one of the most useful and interesting technologies that influenced researchers and technology manufacturers around the world is Internet of Things (IoT). IoT is a special network that connects heterogeneous smart and digital devices, such as sensors and actuators, to the internet and also allows the devices to communicate and share information among them through wired or wireless connections [2]. According to Gartner, the IoT industry "will include 26 billion units installed by 2020 IoT product and service suppliers will generate incremental revenue exceeding $300 billion, mostly in services in 2020" [1].

One of the most popular and globally used implementations of IoT is smart homes. It is a combination of heterogeneous automation systems or regulations that can be managed or customized through a remote user with the help of the internet to ease the communications [21]. The definition of a "smart home device" is any single purpose Internet-connected device that is designed for a home or a hub, like a device that is designed to connect and control more than one single purpose device such as smart security cameras [3]. The smart IoT devices are in almost half of the houses in each continent, at least one smart IoT device per home [4].

IoT smart homes present a spectacular improvement in the quality of living along with benefits from using its customized applications to save time, money and human interactions. Electricity cost is an issue nowadays, because the connected devices, such as smart TVs or smart security cameras, consume power to function and provide services. There are some benefits related to the automation environments that IoT smart home supports for extra comforts. For example, monitoring the performance of all the connected devices to ensure that all functions are accomplished, finding any system or device failure and provide solutions or suggestions, or providing malfunction alarms. The most fascinating thing about the IoT smart home is that it could learn the owner's habits and set a special environment automatically before they arrive. Using the IoT smart homes would maintain the best bandwidth consumption and save communication energy by implementing the energy-aware authentication scheme. In addition, data privacy and protection from leakage along with involuntary privacy breaching are two major benefits that IoT smart homes offer by involving Artificial Intelligence methods [20].

Cyber-attacks are recognized by individuals and organizations around the world. These attacks are happening every minute and without any notice from the hacked systems. These attacks could be recognized and counted using special software in powerful organizations. According to the United States FBI, on the 1st of January 2015, there were 42 committed random attacks in just an hour, 1000 in a day, 3000 in a month, and 0.36 million in a year. The surprising fact is that these numbers increased by 300% in January 2016. Additionally, annual Cyber-Crime reports that 1.1 million web attacks were committed in just one day! [7]. As IoT smart home is widely used, there are many cyberattacks that are targeting the smart home systems as well. Many researches have been conducted to make the smart home systems more secure, one of them is node authentication and identification.

Node authentication and identification are important in the smart home environment because it's considered the first stage of network protection and basic security requirement for IoT smart home network connection. Weak authentication techniques may lead to easy and harmful attacks. IoT smart homes should adopt the highest standards of security to prevent such attacks, because of the sensitive information that could be exposed such as people's names, addresses, and financial accounts. Any successful attack on a single smart home device might harm the whole smart home system and the connected devices. Moreover, IoT smart homes are connecting heterogeneous smart devices that usually support different automated functions such as smart lights, and smart security cameras. The authentication process during this heterogeneity is a dilemma in the IoT smart homes industry that requires attention from IoT security researchers and manufacturers [10].

2. BACKGROUND

There are different smart devices that are widely used in smart homes, each smart home device is responsible for a certain task that was manufactured to do. Such as Security-Smart Door Locks (e.g. August Smart Lock Pro 3rd), Entertainment-Smart TVs (e.g. Apple TV), Electricity-Smart Plugs (e.g. Amazon Smart blogs.). IoT smart home automation environments have a high potential for cyber threats because of the heterogeneous smart devices that are powering the smart home, which is automatically based on the available information from the communications in the surrounding environment [7]. It's a double-edged sword, because of the wireless remote access and control via smartphones and web applications, which raises the risk of unauthorized access to IoT devices in smart homes. The main risks in the IoT smart homes are summarized under Risk of Safety Certification, Risk of RFID Technology Security, and Risk of Information Leakage [6].

2.1 Smart Home Architecture

Smart homes are one of the best examples of the specific and crucial application of the IoT. They implement the network communication, automation, and control technologies along with the artificial intelligence technologies in one integrated platform [8]. As shown in Figure 1, IoT smart homes system architecture can be divided into three layers [9]:

1. Perception layer: usually called the sensing layer, it consists of adaptors that collect information from the surrounding home environment.
2. Network layer: responsible for data communications and transmission within the environment using different medium types. It also works as a multi-protocol aggregator and convertor.
3. Management layer: all data is managed and processed by this layer using the home information service terminal. The results are presented to the end-user using the IoT devices' companion applications through mobile applications or web services.

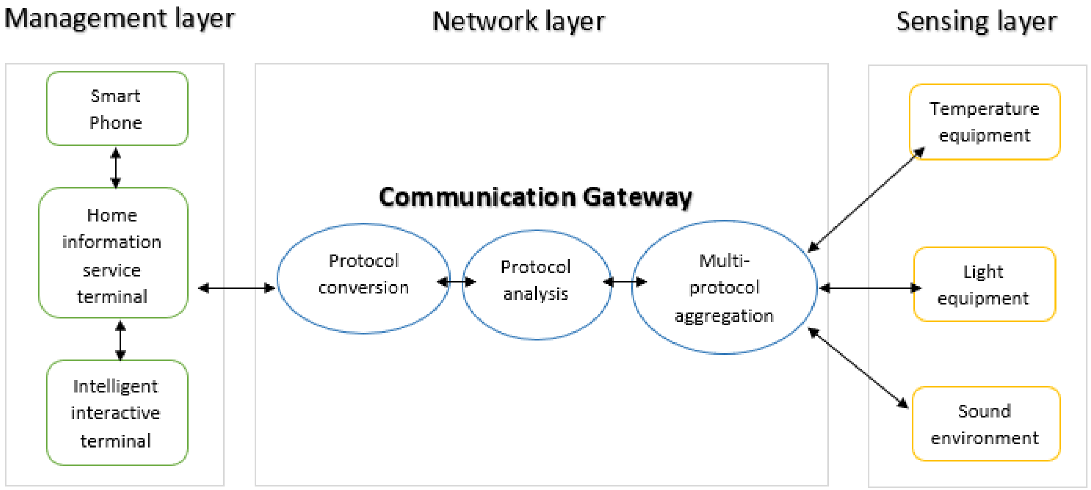


FIGURE 1: Smart Home Architecture Based On IoT [9].

IoT device authentication is the first security aspect that should be considered when designing an IoT device that uses communication methodology (e.g. user authentication) [12]. It is an important part of the perception layer of IoT smart home architecture because these devices must be authenticated to use and share accurate data. IoT network is connecting a large scale of heterogeneous devices that cooperate for different goals, any unauthorized device would harm the network at different levels. There are two authentication types: 1) Source authentication: guarantees that the source object is the one that it claims to be and is well known to everybody in the domain of the IoT network, and 2) Data authentication: guarantees that this message is original, and not a replay of the original one [11].

An intelligent interactive IoT device can control and affect the adaptors/sensors in smart homes for any changes in the environment parameters [9]. Any smart home has five components to achieve the best intelligent automation environment:

- IoT devices: sensors that collect information and actuators to execute actions.
- Coordinators: control all processes and report everything to the IoT service provider.
- IoT services: a cloud-based service accessed by users at any time.
- Controllers: control the IoT system.
- Sensor bridge: the connection between the local IoT network and the IoT cloud services.

Smart homes are using different wireless technologies to manage communications using different standards that vary based on the implemented applications [14]. The common technologies include Wi-Fi, ZigBee, Z-Wave, Bluetooth LE (Low Energy) and etc.

The communication between the IoT-based smart home devices is a very critical issue, because of the personal and sensitive information that these devices pass to each other to be able to make crucial decisions in the IoT environment. Four Communication Models are used by IoT-based smart home devices in general [13]:

- Device to Device Communications: The communication is established when two or more IoT devices are directly connected, without any intermediary object (e.g. server).
- Device to Cloud Communication: The communication is established when there is a connection between the device and the IP network using Wi-Fi or an ethernet cable such as the Samsung Smart Kit.
- Device to Gateway Communication: Application Layer Gateway service is used to establish a connection between the IoT device and the cloud service. It is an intermediary between them and acts as a local gateway for data translation and security such as a fitness tracker watch.
- Back-End Data Sharing Model: This model uses an architecture that helps users export data along with smart object data analyzing from different sources (service clouds). All data are collected from IoT sensors and utility systems, then uploaded to multiple application service providers.

2.2 Node Authentication Mechanisms In Smart Homes

The authentication of IoT smart devices is very important. The current IoT device authentication schemes that are used in smart homes could be categorized as the following [10]:

- One-time Password: create a new passcode that is used once for each time there is a communication or transaction. This scheme is wildly used in international banking systems and e-Commerce.
- Zero-Knowledge Proof: a technique that verifies information between the communicator parts, but without revealing any sensitive information.
- Mutual Authentication: two-way authentication, both entities authenticate each other.
- Public-Key Cryptography: It's asymmetric encryption by generating public and private key pairs used between the IoT devices.
- Digital Signature: use the source private key, which is widely used in authentication technology.

The IoT device should be authenticated before any data transmission or communication. This authentication should be done from the IoT device source, and any cryptographic keys that have been generated in this transmission should not make any overhead for the IoT devices in the IoT system. IoT authorization and access control are two different things. The main difference between them is that authorization is only responsible for giving access rights to the resources, but access control is responsible for giving access to the authorized resources. [15].

2.3 Current Node Authentication and Identification Challenges At Smart Homes

The IoT device authentication procedure could be either user authentication or device authentication. Light-weighted, bulletproof, and distributed authentication schemes are big challenges in smart home implementations. Management security, physical security, and information security are the three dimensions that should be counted and well-considered when devices are suffering from is the openness of environments such as security lights and outdoor cameras. RFID tags could be easily noted and suffer from privacy leakage during the authentication process because they could be scanned or misplaced to be used by the hacker [12]. Lightweight and distributed authentication schemes are still a big challenge in IoT smart homes. TCP/IP Protocols such as HTTP, TCP, and IP are not efficient in handling M2M communications; more protocols should be designed to overcome this challenge in IoT environments.

Some researchers proved that they might get users' sensitive information by analyzing the IoT data from smart devices such as a sense sleep monitor, a Nest Cam Indoor security camera, and an Amazon Echo [3]. It sounds suspicious, but by applying security standards for authentication in IoT devices, everything would become safe to use at a smart home. Much research has been done on this subject but still, there is no common approach whose adoption is approved by IoT device manufacturers [16]. IoT device authentication is a software issue rather than a hardware issue; that's why there is no common solution for all the application yet! [17]. 40% of the IoT smart home devices are being targeted by botnets attacks; this number is rising to 75% by 2021 [18]. Several attacks are popular in IoT smart home applications and deal with device authentication such as insider attacks, impersonation attacks, a man in the middle attacks, unknown sharing attacks, replay attacks, and unknown sharing key attacks.

Home Appliance	Vulnerabilities	Attack Surface
Smart Thermostat	• Encryption • Weak password	• Local data storage • Device firmware • Ecosystem communication • Authentication or authorization
Smart Refrigerator	• Unencrypted Services • Denial Of Service (DoS) • Firmware version	• Mobile application • Local data storage • Authenticationor authorization
Smart TV	• Unencrypted Services • Weak password • Two-Factor Authentication • Firmware version	• Ecosystem Access Control • Device web interface • Device network service • Authentication or authorization • Local data storage

TABLE 2: Possible threats to popular IoT-based smart home devices along with the attacks' surface area [5].

2.4 Threats Against Node Authentication In Smart Home

Smart homes ought to be safest for owners who invested in new technologies that present a modern and convenient lifestyle. Some of the IoT smart home manufacturers do not consider using the high-security standards in their products in the initial states and leave the end-user with no clue about the vulnerabilities that this purchased device might have [24].

There are different threats against the authentication in smart devices such as DoS, eavesdropping, physical attacks, tracking, and cloning attacks. Smart devices have some crucial vulnerabilities which can happen by using weak user credentials, un-encrypted or un-scanned data transmissions, or downloading un-encrypted updates. Here is a classification of the IoT authentication threads and attacks at smart homes. These classifications are derived based on the IoT three-layer architecture described in this paper in section 2.1. Table 2 lists the common threats at the device level, network level, and application level.

Layer	Threats	Attacks	
		In Transit	At Rest
Device Level	Limited Resources Architecture Interfaces Software	Firmware Brute force Defraud DoS	Firmware Physical Credentials
Network Level	Architecture Openness Protocols	Eavesdropping Device scan Spoofing MITM Reply Unknown key Sharing	Device scan Brute force
Application Level	Interactions Constrains Environment Human	Impersonation Malware Insider	

TABLE 2: Classification of Authentication Threats and Attacks [12].

2.5 Current Ways To Mitigate Authentication Threats

There are different solutions that are widely used to mitigate authentication threats and attacks. Such as, using default user credentials (username & password) is not encouraged because they could be obtained by dictionary or brute force attacks. Also, all unused smart device's network ports should be disabled. In addition, ensure the last update of the smart device's firmware to avoid any un-patched problems. Moreover, authenticated access should be required for all smart device's access (from inside or outside the smart home). Also, all data communication should be encrypted. Finally, all smart home devices manufacturers should avoid the usage of USB port to prevent any source of attack [19].

3. LITERATURE REVIEW

This section summarizes the major node authentication and identification techniques at the smart homes.

A. Shivraj et al. proposed a one-time password (OTP) technique based on identity-based elliptic curve cryptography (IBE-ECC) and Lamport's algorithm [25]. There are four steps to perform this scheme which start with setup, extract, generate, and end with validation. To perform the setup phase, two prime numbers are generated from the Public Key Generator (PKG) which are P and Q. For the extract phase, all IoT devices must be registered in the PKG to be able to get their public and private keys to be used in the elliptic curve. In the Generate phase, when the IoT devices in smart homes communicate and exchange information using the IoT cloud, the PKG will create a private key of that communicated device and computes the new torsion point to extract the desired data. After that, this new torsion point is sent to the IoT device and application. Finally, after the IoT device receives the OTP from the application, it compares it with the one from the IoT cloud. If it matches, it is verified and that's the last phase. This scheme is using a lightweight system that makes it more efficient along with two authentication factors to enhance security and protection against MITM attacks or replay attacks. However, the main disadvantage of this scheme is the complex computation of the Keys [25].

B. Shah et al. proposed an authentication scheme that is established between the IoT device and the IoT server [26]. It is based on a multi password and aims for more security and validity. This scheme is using a secret between the server and the IoT device that's called a "secure vault". This secret holds n keys and m bit size that is driven by security requirements. The initial value for the secure vault is already stored in the IoT device and shared with the IoT server. The value of the secret vault is changed after any successful communication by performing Hash Message Authentication Code (HMAC) on the available vault using the exchanged information from the IoT device and the server as an HMAC key. The authentication procedure contains encrypted messages and challenges that IoT servers and IoT devices must decrypt for a secure communication session. After a successful authentication scheme, the IoT device and the server could communicate using a session encryption key for a faster communication setup. This scheme prevents MITM and DoS attacks. It changes the passwords of every communication session to ensure the validity of the passwords. However, the key size will restrain the security enhancement, because of the high-power consumption for processing [26].

C. Alizia et al. proposed an authentication scheme based on a multi-factor scheme using device capability and digital signatures [27]. The IoT device can communicate with the network only if it is authenticated. The authentication procedure starts from the IoT device side by sending a connection request to the network server. The server responds with a nonce (which is signed with the server private key) and a timestamp. The IoT device will verify the response and perform a functional operation on the nonce that is sent from the server. After the IoT device performs the functional operation, it responds to the server with timestamp, nonce, and functional operation results, all signed with the device's private key. The server should check the result of the operational function and the device digital signature for the final validation announcement. The main advantage of this scheme is the low overhead. However, key storing is a big issue [27].

D. Lee et al. proposed a blockchain anonymity enhancement authentication scheme that uses a smart contract system with zero-knowledge proof function [28]. This system was implemented for a smart meter system (which measures power consumption) to enhance the security aspects such as privacy and authentication. This scheme has two steps for the authentication process: registration and authentication. Each step has three phases: client, server, and blockchain. In the registration step, the client enters data that is presented as a “secret key” to be used to generate two prime numbers (p, g) for public key generating. All secret keys, prime numbers (p, g) and public keys are transmitted to the server to be stored. Only the public key and the prime numbers (p, g) are transmitted and saved in the blockchain. The authentication step is completed when the client requests the data that has been stored on the server and will select the public key that is already stored on the server database. If the blockchain receives any query through calling the public key, it will transmit the prime numbers (p, g) to the server, which will generate two new values (R1, w) to be used for authentication by the blockchain. By using the smart contract system in the blockchain, it executes the proof knowledge function on the values that have been generated by the server (R1, w) to find the value of R2. The transaction is authentic: if R1=R2 and R2=R1, then it proves that the secret data saved on the server is correct and no secret data transmission is needed to the blockchain. This scheme enhances the privacy of communication and detects any data integrity issues. However, the dependency on the blockchain anonymity is not efficient [28].

E. Li et al. proposed an authentication scheme based on the blockchain rather than a third party (central authority) [29]. It has two steps: registration and authentication. This scheme depends on public-key cryptography and blockchain; each device must be registered in the blockchain before starting the authentication process. In the registration step, all the device's public key, a hash of some critical information and device ID are saved in the blockchain. This critical data needs to be identical between all the devices in the blockchain. Each device creates its private key randomly using the cryptographical secure pseudo-random number generator (CSPRNG) and generates a public key by implementing the elliptic curve multiplication. The generated device's private key is stored locally, but the public key is saved in the blockchain. In the authentication step, if a device receives a communication request from another device, it looks for the sender device's public key in the local blockchain database. If it’s not found, the device looks for it in the consensus node. If the public key is found, then it’s verified; if not, the communication request is rejected. This scheme is lightweight and avoids the problems that could happen by depending on a third party such as single-point failure. This system will not stop if any node suffers from a DDoS attack. However, the scheme's performance depends on the blockchain platform and how efficient it is [29].

F. Sahu et al. proposed a two-way authentication scheme based on smart home hub systems (ISH) that use WiFi or ZigBee technology that supports the IEEE 802.15.4 protocol for device communications. This smart home hub is connected to the cloud or internet services. The proposed scheme considers the outside threats in this proposal. The authentication scheme assumes that there is n number of smartphones associated with ISH that are using their ID's as their unique identifier. The authentication is achieved by completing three successful steps that start from smartphone (SPi) that sends its unique ID and generates personal random number (r) to the ISH using the internet. After that, the ISH identifies the received information and generates a random session key to be used for communication with the corresponding smartphone, then send it along with a "C" message to precise integrity to the corresponding smartphone (SPi). Finally, the smartphone (SPi) decrypt the received information and verifies the C massage and session key to check their values, if the values are correct then the ISH authenticates the corresponding smartphone (SPi) and they can communicate using a temporary key. This authentication scheme is designed to prevent external attacks and has a two-way authentication protocol to enhance security. The use of the temporary key after authentication between the two entities provides a smooth and lightweight system. However, the defense leak against internal attacks is considered the main drawback that needs development [21].

G. Santoso et al. proposed an authentication technique-based on public key mutual authentication protocol with pre-shared keys [22]. It uses a WiFi (IPv6) smart home system that uses a gateway to support security in communications between the IoT smart home devices, as well as accesses and controls the devices using the Graphical User Interface (GUI) on connected smartphone applications. The authentication is accomplished by successfully executing two rounds of authentication procedures. Firstly, authenticate the smartphone with the smart home device. It starts with the user entering the ID and the pre-shared secret key of the smart home device into the smartphone, then turns on the smart home device to be ready for the authentication process. Secondly, authenticate the smart home device with the home gateway: starts with the user entering the smart home device's ID and the pre-shared secret key into the gateway using the smartphone. When the smart home device communicates with the gateway for the first time, the gateway will start authenticating that smart home device using the entered information about the smart home device. Finally, after this successful authentication between the gateway and the smart home device, a shared key is generated and shared between them to be used for further communications.

All communications are performed based on the User Datagram Protocol (UDP). The use of the shared secret key reduces the need for establishing more public keys for the system. After the authentication is done, the gateway and the smart home device can use Elliptic Curve Diffie Hellman (ECDH) calculation to generate a shared key for any subsequent symmetric encryption. The smartphone could be used to do so if needed. All sent messages are encrypted by the Advanced Encryption Standard (AES) using the generated key by ECDH. The user can access the gateway through the smartphone and get all the information about the events and actions of the smart home system (the communication between the gateway and the devices) or customize automatic actions that could be crafted based on the collected information by the device.

This scheme uses a gateway that controls, monitors and maintains the high-security standards and translations between smart home devices. All communications are done through the gateway. This scheme uses AES and ECDH encryptions for more security along with a couple of shared keys. However, entering data about the smart home devices manually is considered a drawback that must be improved. Additionally, more versions should be created to support other operating systems such as iOS and Microsoft [22].

H. Huth et al. proposed a symmetric authentication scheme based on the physical properties of smart home devices and communications [30]. This scheme relies on a Physical Unclonable Function (PUF) and a Physical Generated Key (PGK) to enhance the security aspects along with reusing the available hardware to reduce the system's cost. The authentication is completed after four successful steps which start with the enrollment phase that relies on the IoT device manufacturers. The second step is the key generation phase for symmetric encryption purposes. The third step is the authentication phase which uses a hash function to solve any encryption challenges, then send the result to the server. Finally, the re-enrollment phase is responsible for regenerating all valid challenges, responses, and helper data after successful authentication steps are done. This scheme relies on the physical properties of the smart home devices to reduce the cost of the system and to enhance the communication protocols. The use of built-in factory keys enhances security and device confidentiality. However, hardware requirement is a weakness in this scheme [23].

I. Jan et al. proposed a lightweight asymmetric authentication scheme that verifies the identities of the participating clients and servers in a Constrained Application Protocol (CoAP) IoT environment [31]. The authentication is done by performing four-way handshake messages between the server and the smart home device with the help of a pre-shared secret key. The scheme starts when the smart home device sends its ID to the server. Secondly, the server searches for the smart home device's pre-shared key in its local lookup table. After that, it generates a nonce and a session key, then encrypts them and sends them back to the smart home device. Thirdly, the smart home device decrypts the message and finds the session key, then sends an encrypted nonce to the server. Finally, the server decrypts the message using the session key and verifies the nonce, if the nonce is verified, the authentication is completed [23]. This is a lightweight asymmetric authentication scheme that defines the communications between the server and smart home devices to achieve a novel proposal. However, that proposal should consider the smart home device power consumption and develop a solution for Sybil attacks.

A comparison of different techniques is summarized in Table 3.

There are some requirements that should be considered when designing and proposing an authentication scheme. It's always better to have a lightweight authentication scheme, because of the resource constraints of the IoT devices in low-power, limited computation and memory. Multi-factor utilization authentication is encouraged and will provide more security because it uses more than one factor for the authentication process. Dealing with a multi-factor authentication scheme puts an extra load on the IoT device, thus efficient authentication schemes are preferred. For extra security, encryption techniques should be combined with authentication schemes such as AES, RSA, or hash functions [10]. However, the manufacturers should implement high cybersecurity standards for non-technical users, along with minimum user intervention.

4. DISSCUSSION

Smart homes technologies provide the smart home devices with the best performance that could be achieved, using all the available resources from such constrained devices. In order to achieve the best performance and functionality, one major factor to achieve that performance is a powerful and stable internet connection to enable the data transmission between the smart home devices and the IoT service cloud. This internet connection is provided by ISPs. Most of the smart home devices are "always on" devices that use sensors to collect information from the surrounding environment and transmit all collected data using the internet. This raises an issue about the ISP companies which describe through passive network observation of the data traffic in smart homes. This is a smart home privacy risk.

There are different methods that smart home device manufacturers are using to connect their devices to the IoT smart home systems. Lack of device identification and authentication procedures in the configuration and connection phase is a critical issue. There is a need for strong identification and authentication procedures to ensure the best security and privacy standards at smart homes, because of the critical information that could be accessed by such devices. However, IoT smart home device vendors claim that they provide the consumer with the best security and privacy standards. This is not always true! especially when the smart device is not supporting any type of security login credentials such as username and password. Moreover, it is hard to address the identification and authentication process behind the scene of a smart home device, because some of the manufacturers lock their devices from any firmware access for security aspects. In such scenario, it is hard to know how accurate the identification and authentication procedures are, or if there is any truly available? Understanding the identification and authentication techniques that are adopted in IoT smart home devices would enrich the consumer knowledge to ask for high-security expectations from manufacturers, and help them for better purchase decisions.

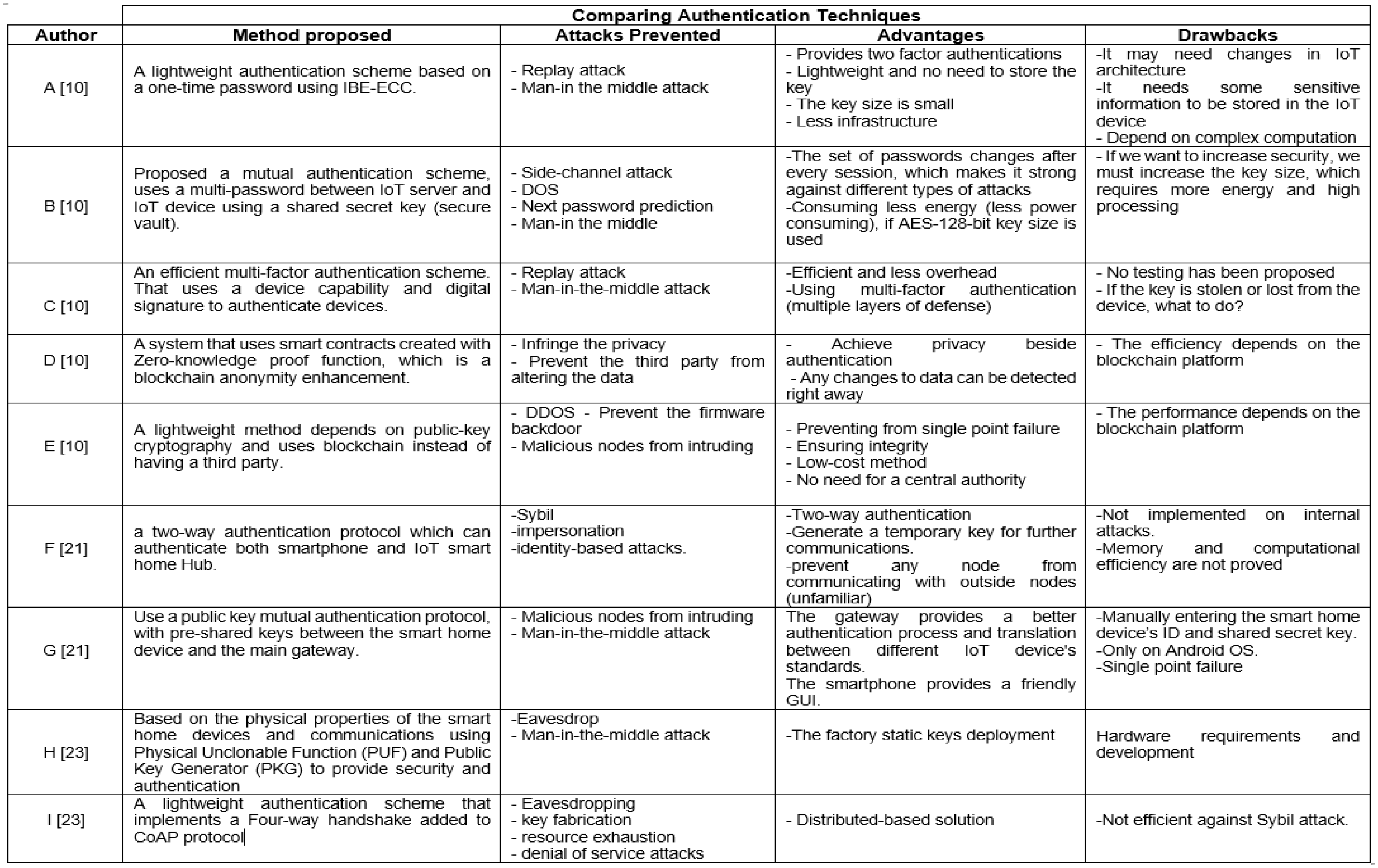
High security standards and network protocols consensus among smart home device manufacturers would prevent many vulnerabilities from happening. There should be agreements between manufacturers to ensure the best quality at all levels. Lack of such agreements between smart device manufactures would cause weak Interoperability, for instance.

5. FUTURE WORK

Explore more authentication schemes that support the IoT and implement them in smart homes to investigate the related weaknesses and vulnerabilities. This study would help in driving a new authentication scheme or improving an existing one, to overcome the weak points in the current schemes and apply a new authentication scheme on some of the IoT devices and homeowners to measure the fitness and the accuracy of the new solution. In addition, explore the security and privacy aspects of highly rated smart home devices by designing a testing module that presents a useful detail for consumers about the targeted smart home device of purchase.

6. CONCLUSION

In this paper, current efficient IoT node authentication and identification techniques at smart homes were reviewed. Throughout this paper, all presented techniques were analyzed to highlight the different solutions that they fix, and to understand the best possible implementations at smart home environments. The challenges that surround the node authentication and identification at smart home were elaborated. The possible threats to this issue were discussed, and some useful solutions were represented to mitigate them. This paper started with a general introduction to IoT smart home environments. The benefits of such homes were discussed, along with the importance of Node authentication and identification techniques at smart homes. Then, a background section detailed smart home automation system and architectures and provided a clear picture of the targeted environment. In addition, a clarification of smart home components was explained in detail with available communication technologies and models. Different Node authentication schemas were discussed too. Based on the analysis of the node authentication and identification techniques, some recommendations and best practices were provided for better designing of new techniques that could be used for better smart home environments.



	Comparing Authentication Techniques			
Author	**Method proposed**	**Attacks Prevented**	**Advantages**	**Drawbacks**
A [10]	A lightweight authentication scheme based on a one-time password using IBE-ECC.	- Replay attack - Man-in the middle attack	- Provides two factor authentications - Lightweight and no need to store the key - The key size is small - Less infrastructure	-It may need changes in IoT architecture -It needs some sensitive information to be stored in the IoT device - Depend on complex computation
B [10]	Proposed a mutual authentication scheme, uses a multi-password between IoT server and IoT device using a shared secret key (secure vault).	- Side-channel attack - DOS - Next password prediction - Man-in the middle	-The set of passwords changes after every session, which makes it strong against different types of attacks -Consuming less energy (less power consuming), if AES-128-bit key size is used	- If we want to increase security, we must increase the key size, which requires more energy and high processing
C [10]	An efficient multi-factor authentication scheme. That uses a device capability and digital signature to authenticate devices.	- Replay attack - Man-in-the-middle attack	-Efficient and less overhead -Using multi-factor authentication (multiple layers of defense)	- No testing has been proposed - If the key is stolen or lost from the device, what to do?
D [10]	A system that uses smart contracts created with Zero-knowledge proof function, which is a blockchain anonymity enhancement.	- Infringe the privacy - Prevent the third party from altering the data	- Achieve privacy beside authentication - Any changes to data can be detected right away	- The efficiency depends on the blockchain platform
E [10]	A lightweight method depends on public-key cryptography and uses blockchain instead of having a third party.	- DDOS - Prevent the firmware backdoor - Malicious nodes from intruding	- Preventing from single point failure - Ensuring integrity - Low-cost method - No need for a central authority	- The performance depends on the blockchain platform
F [21]	a two-way authentication protocol which can authenticate both smartphone and IoT smart home Hub.	-Sybil -impersonation -identity-based attacks.	-Two-way authentication -Generate a temporary key for further communications. -prevent any node from communicating with outside nodes (unfamiliar)	-Not implemented on internal attacks. -Memory and computational efficiency are not proved
G [21]	Use a public key mutual authentication protocol, with pre-shared keys between the smart home device and the main gateway.	- Malicious nodes from intruding - Man-in-the-middle attack	The gateway provides a better authentication process and translation between different IoT device's standards. The smartphone provides a friendly GUI.	-Manually entering the smart home device's ID and shared secret key. -Only on Android OS. -Single point failure
H [23]	Based on the physical properties of the smart home devices and communications using Physical Unclonable Function (PUF) and Public Key Generator (PKG) to provide security and authentication	-Eavesdrop - Man-in-the-middle attack	-The factory static keys deployment	Hardware requirements and development
I [23]	A lightweight authentication scheme that implements a Four-way handshake added to CoAP protocol	- Eavesdropping - key fabrication - resource exhaustion - denial of service attacks	- Distributed-based solution	-Not efficient against Sybil attack.

TABLE 3: Comparison of Different Device Authentication Techniques.

7. REFERENCES

[1] “Lack of security in Internet of Things devices”, ELSEVIER, vol. 2014, no. 8, p. 2, 2014. URL: https://doi.org/10.1016/S1353-4858(14)70075-3.

[2] Li, Q. Yan, and V. Chang,” Internet of Things: Security and privacy in a connected world”, ELSEVIER, vol. 78, 3, pp. 931-932, 2018. URL: https://doi.org/10.1016/j.future.2017.09.017.

[3] N. Apthorpe, D. Reisman, and N. Feamster, "A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic", Computer Science Dept. Princeton University, pp. 1-6, 2017.

[4] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, Z. Durumeric, “All Things Considered: An Analysis of IoT Devices on Home Networks”, 28th USENIX Security Symposium. URL: https://press.avast.com/hubfs/stanford_avast_state_of_iot.pdf.

[5] A. Gai, S. Azam, B. Shanmugam, M. Jonkman and F. De Boer, "Categorization of security threats for smart home appliances," 2018 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, 2018, pp. 1-5. doi: 10.1109/ICCCI.2018.8441213.

[6] I. Del Pozo and D. Cangrejo, "Creating Smart Environments: Analysis of Improving Security on Smart Homes," 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, 2018, pp. 303-310.DOI: 10.1109/FiCloud.2018.0005, URL: https://ieeexplore.ieee.org/document/8458028.

[7] W. Ali, G. Dustgeer, M. Awais and M. A. Shah, "IoT-based smart home: Security challenges, security requirements and solutions," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-6.DOI: 10.23919/IConAC.2017.8082057, URL https://ieeexplore.ieee.org/document/8082057.

[8] Y. Han and B. Liu, "Interactive smart home design based on Internet of Things," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 449-453. DOI: 10.1109/ICCSE.2017.8085534, URL: https://ieeexplore.ieee.org/document/8085534.

[9] R. Liu and Y. Ge, "Smart home system design based on Internet of Things," 2017 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, 2017, pp. 444-448. DOI: 10.1109/ICCSE.2017.8085533, URL: https://ieeexplore.ieee.org/document/8085533.

[10] A. Albalawi, A. Almrshed, A. Badhib, and S. Alshehri, "A Survey on Authentication Techniques for the Internet of Things," 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-5. DOI: 10.1109/ICCISci.2019.8716401, URL: https://ieeexplore.ieee.org/document/8716401.

[11] Hasan and K. Qureshi, "Internet of Things Device Authentication Scheme Using Hardware Serialization," 2018 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, 2018, pp. 109-114. DOI: 10.1109/ICAEM.2018.8536286, URL: https://ieeexplore.ieee.org/document/8536286.

[12] Gamundani, Attlee & Phillips, Amelia & Muyingi, Hippolyte. (2018). “An Overview of Potential Authentication Threats and Attacks on Internet of Things (IoT): A Focus on Smart Home Applications”, 10.1109/Cybermatics_2018.2018.00043. URL: https://www.researchgate.net/publication/329140617_An_Overview_of_Potential_Authentication_Threats_and_Attacks_on_Internet_of_ThingsIoT_A_Focus_on_Smart_Home_Applications.

[13] M. Husamuddin and M. Qayyum, "Internet of Things: A study on security and privacy threats," 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, 2017, pp. 93-97. DOI: 10.1109/Anti-Cybercrime.2017.7905270 URL: https://ieeexplore.ieee.org/document/7905270.

[14] S. S. I. Samuel, "A review of connectivity challenges in IoT-smart home," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-4. DOI: 10.1109/ICBDSC.2016.7460395, URL: https://ieeexplore.ieee.org/document/7460395.

[15] M. Conti, A. Dehghantanha, K. Franke and S. Watson," Internet of Things security and forensics: Challenges and opportunities", ELSEVIER, vol. 78, 2, pp. 544-546, 2018 URL: https://www.sciencedirect.com/science/article/pii/S0167739X17316667.

[16] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next-generation networks," 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Noida, 2016, pp. 315-318. DOI: 10.1109/ICICCS.2016.7542301, URL: https://ieeexplore.ieee.org/document/7542301.

[17] M. Azarmehr, A. Ahmadi and R. Rashidzadeh, "Secure authentication and access mechanism for IoT wireless sensors," 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, 2017, pp. 1-4. DOI: 10.1109/ISCAS.2017.805044, URL: https://ieeexplore.ieee.org/document/8050446.

[18] Robinson, S. (2019). "Internet of Things (IoT) - Smart home attacks are a reality, even as the smart home market soars". URL: https://www.cisco.com/c/en/us/solutions/internet-of-things/smart-home-attacks.html.

[19] M. Fagen, M. Yang, A. Tan, L. Randolph, K. Scarfone, "Security Review of Consumer Home Internet of Things (IoT) Products", Draft NISTIR 8267, URL: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8267-draft.pdf.

[20] Zaidan, A.A., Zaidan, B.B. "A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations", Artificial Intelligence Review 53, 141–165 (2020). URL: https://link.springer.com/article/10.1007%2Fs10462-018-9648-9.

[21] A. K. Sahu, S. Sharma, D. Puthal, A. Pandey and R. Shit, "Secure Authentication Protocol for IoT Architecture," 2017 International Conference on Information Technology (ICIT), Bhubaneswar, 2017, pp. 220-224. URL: https://ieeexplore.ieee.org/document/8423911.

[22] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," 2015 International Symposium on Consumer Electronics (ISCE), Madrid, 2015, pp. 1-2. URL: https://ieeexplore.ieee.org/document/7177843.

[23] Y. Atwady and M. Hammoudeh, "A Survey on Authentication Techniques for the Internet of Things," 2017. the International Conference, DOI: 10.1145/3102304.3102312 URL:https://www.researchgate.net/publication/320028921_A_Survey_on_Authentication_Techniques_for_the_Internet_of_Things.

[24] Y. Seokung, P. Haeryong, Y. Hyeong, "Security Issues on Smart home in IoT Environment", 2015. URL: 10.1007/978-3-662-45402-2_97.

[25] V. L. Shivraj, M. A. Rajan, M. Singh and P. Balamuralidhar, "One time password authentication scheme based on elliptic curves for internet of things (iot)", 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), pp. 1-6, Feb 2015.

[26] T. Shah and S. Venkatesan, "Authentication of iot device and iot server using secure vaults", 2018 17th IEEE International Conference On Trust Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 819-824, Aug 2018.

[27] Z. A. Alizai, N. F. Tareen and I. Jadoon, "Improved IoT device authentication scheme using device capability and digital signatures", 2018 International Conference on Applied and Engineering Mathematics (ICAEM), pp. 1-5, Sept 2018.

[28] C. H. Lee and K. Kim, "Implementation of IoT system using block chain with authentication and data protection", 2018 International Conference on Information Networking (ICOIN), pp. 936-940, Jan 2018.

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

[30] C. Huth, J. Zibuschka, P. Duplys and T. Güneysu, "Securing systems on the Internet of Things via physical properties of devices and communications," 2015 Annual IEEE Systems Conference (SysCon) Proceedings, Vancouver, BC, 2015, pp. 8-13, doi: 10.1109/SYSCON.2015.7116721.

[31] M. A. Jan, P. Nanda, X. He, Z. Tan and R. P. Liu, "A Robust Authentication Scheme for Observing Resources in the Internet of Things Environment," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014, pp. 205-211.