Cybersecurity Threats and Countermeasures of the Smart Home Ecosystem

Abdulbasit Darem[1*], Asma A. Alhashmi[2*], Jemal H. A.[3#]

[*] Department of Computer Science, Northern Border University, Arar 91431, Saudi Arabia
[#] Cybersecurity Research and Innovation Centre, Deakin University, Burwood, VIC 3217, Australia

Abstract
The tremendous growth of the Internet of things is unbelievable. Many IoT devices have emerged on the market over the last decade. This has made our everyday life easier inside our homes. The technology used at home has changed significantly over the past several decades, leading to what is known today as the smart home. However, this growth has also brought new challenges to our home security and privacy. With the smart home becoming more mainstream, cybersecurity issues have become a fundamental concern. The smart home is an environment where heterogeneous devices and appliances are interconnected through the Internet of Things (IoT) to provide smart services to residents. These services include home climate control, energy management, video on demand, music on-demand, remote healthcare, remote control, and other similar services in a ubiquitous manner. Smart home devices can be controlled via the Internet using smartphones. However, connecting smart home appliances to wireless networks and the Internet makes individuals vulnerable to malicious attacks. Remote access within the same environment or over the Internet requires an effective access control mechanism. This paper intends to shed light on how smart home devices are working as well as the type of security and privacy threats of the smart home. It also illustrated the types of authentication methods that can be used with smart home devices. In addition, a comparison of Smart home IoT-based security protocols was presented along with a security countermeasure that can be used in a smart home environment. Finally, a few open problems were mentioned as future research directions for researchers.

Key words:
Smart home, Cybersecurity, Internet of Things (IoT), Security countermeasure, Authentication.

1. Introduction

Advances in IoT have made it possible to realize a smart home, where home appliances and smart gadgets that can be accessed and controlled over the Internet provide a wide range of services. The variety of services can be ranged from home e-commerce, remote control, energy management, climate control, remote healthcare, video on demand, music on-demand, and other similar services [1][2]. To access and control smart home appliance through the Internet, the user can use any compatible device, such as a smartphone. Smart home devices and appliances interact not only with humans but also with each other and other wirelessly connected devices, objects, environments, and infrastructure. Smart home devices differ from laptops, servers, and other IP-based devices in several ways, such as the types of data these devices process, which services they use, access requirements, and the data flow. The growing use of connected smart home gadgets increases the opportunity for hackers and other unscrupulous operators to find a lucrative target. This has made cybersecurity one of the main requirements for the successful deployment of IoT in a smart home ecosystem. With the smart home becoming more mainstream, cybersecurity issues have become a fundamental concern. According to the Kaspersky IoT cyberattack report [51], the breaches during the period of January to June 2021 are 1.51 billion breaches of internet of things-based devices which is 639 million more compared to the same period in 2020.

The way smart home devices work is through the implementation of smart home devices that involve a wide range of devices that connect to their networks, despite their size and scope. While traditional security software could focus on Windows PCs, iOS devices, or other widely used platforms, smart home security must deal with a variety of devices, both old and new, each with its own operating system and vulnerabilities. A smart home hub must be provided to act as a central command center for each connected device to be able to talk to each other and also interact with house residents. Wi-Fi enables house devices to connect with main system while house resident at home or away and at the same time, it must provide a secure way for the devices on the network to talk to each other. It is essential to access, control, monitor, and manage all smart products, whether using a cell phone, tablet, or voice. In a smart home ecosystem, devices communicate with each other to provide complicated services; therefore, communicating with a trusted and uncompromised module is crucial [28].

The State of the Connected World 2020 report from the World Economic Forum stated that greater usage of connected devices during the COVID-19 pandemic provided many benefits, but also raised threat. In the IoT ecosystem, cybersecurity threats are still a significant concern. At the regional, national, and state levels,

Manuscript received March 5, 2022
Manuscript revised March 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.3.39

governments are beginning to address the need for stronger IoT security governance, but efforts to date have been widely dispersed, making compliance difficult and expensive for businesses. As stated in [8], security comes first, followed by performance, dependability, and management. Smart home technology provides consumers with automated and interactive services to more efficiently manage their homes, appliances, and utilities [11]. It also allows homeowners to remotely control their smart devices and appliances over the Internet.

Even though smart homes offer benefits such as safety, security, comfort, healthcare, energy-saving, and more, many consumers are concerned about cybersecurity, which is the primary reason for not adopting them. [8][9][10][11]. The smart home access control mechanism is very important for the reliable and secure functioning of smart home systems, and for the safety of the homeowner. If the IoT-enabled gadgets (e.g., smart fridge, smart TV, smart air conditions, and so on.) in a smart home are not sufficiently integrated, the occupant of the smart house will be exposed to a far broader range of security concerns, such as identity theft, device counterfeiting, and so on. Financial loss, Data leakage, health damage, physical damage to the smart home, mental trauma, and risk of death are all possible outcomes of a hacked smart home ecosystem. If successful, an attacker might gain access to sensitive data such as personal, geographical, medical, or financial information, as well as employ actuators to do serious damage to the device and even endanger the user's safety. [3]. For example, in January 2014, it was reported that over 750,000 products, including smart locks, thermostats, televisions, routers, televisions, refrigerators, and other devices, had been infiltrated and/or spied on the individual [7]. According to another study [8], there are 250 different security issues in smart devices, which equates to 25 vulnerabilities per smart device. This is due to the insecure security designs of private technologies and the lack of capable smart object security standards [9].

Suresh and Sruthi [10] identify multiple smart house advantages in different domains. However, the unauthorized use of smart home technology can be destructive to legitimate users [12]. Many security issues have been discovered by researchers. They devised several attacks based on these security weaknesses. Several studies [4][5][6] provide an examination of vulnerabilities and prospective attacks. Recent significant security breaches have demonstrated how Internet-enabled smart homes may be turned into very harmful environments for many illegal purposes, causing individual privacy issues. One possible way to address this problem is by using an efficient authentication mechanism. A user's identification is verified by a variety of methods, including passwords, smart cards, biometrics, and identity certificates. However, due to inherent flaws or user ignorance, these authentication techniques are vulnerable to compromise. Furthermore, several proposed traditional authentication methods require user intervention for identity clarification and authorization, as well as administrator setup. As a result, they are unsuitable for use in a smart home. A lightweight authorization method for IoT-based applications in a smart home ecosystem was presented by Chifor et al. [28], in which a cloud-connected device sends a message to a user's smartphone to grant access. It establishes a digital identity for smart gadgets as well as the people who interact with them.

Recently, authentication for the smart home is being considered to focus on devices. Min and Varadharajan [13] proposed the authentication through SMS. The SMS authentication mechanism, on the other hand, cannot be trusted because it does not ensure data confidentiality [50]. Furthermore, due to security flaws in standards like HTTP Strict Transport Security (HSTS), it is impossible to completely prevent session hijacking, etc. [14]. There are also several proposed techniques [11][12] based on public key encryption, however because of their restricted memory, network bandwidth, and power supply, this type of cryptography is difficult to employ on resource-constrained devices due to the long key size and necessary processing. Another issue is that, in order to be ubiquitous, they are constructed as low-power devices with limited resources, which makes security services difficult to provide. Traditional security systems are not viable on them due to limited computational and energy resources [7][8].

2. Security and privacy threats of the smart home ecosystem

The more people are connected to IoT, the more they give up their privacy and security, the more they become at risk without even realizing that. Before looking at the best methods of protecting smart home applications, it is important to understand the threats, challenges, and causes of data breaches and attacks on smart home devices. The threats can be summarized as follows. One of the most serious security concerns in the realm of IoT is the lack of unified IoT security standards. The majority of IoT developers and manufacturers do not prioritize device or user security. Additionally, it allows for hacking risk. The second concern is users' lack of IoT security awareness and functionality, which has an impact on their security and privacy, as well as anyone who may have linked to their device accidentally or wilfully. This emphasizes how critical it is for IoT makers to protect users from themselves by implementing solid security and privacy standards. The third is ineffective device update management. Smart home devices are sold with the latest software update. The new vulnerabilities will surface over time. If the device does not support the automatic update, it would be at the risk. The fourth threat is the rogue IoT devices. Because of the massive proliferation of IoT devices, rogue or malicious IoT devices can be placed on secured networks without authorization. To capture or change sensitive data between devices, a rogue device replaces or integrates with an IoT network protocol. The inherent vulnerability of data in centrally stored databases is the fifth threat. When data is kept centrally in the cloud, it is not secured end-to-end, exposing the data center to inherent vulnerabilities. In addition, it is not necessary to store the personal data of users in a central database. On the other hand, a decentralized P2P platform allows data to flow directly between the IoT device and the client. The IoT device securely stores all data. This allows the user total control over their network's data, almost eliminating the chance of data being intercepted by a third party. Sixth threat is the weak password policy. Inadequate passwords allow hackers to guess factory settings and take over the device, as well as excessive data collection and data encryption. As a result, attackers will have an easier time stealing Wi-Fi passwords and hijacking other devices on the home network. There have been multiple instances when hackers have taken control of linked toys, allowing them to communicate with children who are playing with the toy or even launch cyberattacks against the smart home. Several Bluetooth devices, such as the singing machine and the karaoke microphone, do not require session-based authentication. This might allow hackers to connect to the device anonymously and send potentially inappropriate or even manipulative audio messages encouraging the child to go outside

3. Types of authentication methods used in smart home devices

Smart home gadgets are typically designed to be resource-constrained, with limited storage and fit-for-computing capabilities. As a result, because most smart home gadgets lack proper defense, they are more vulnerable to security assaults. When compared to an existing user or personal identification approach that is not directly relevant to Smart home devices with limited resources, smart home device authentication must be unique and relatively lightweight. As a result, selecting the appropriate authentication technique is critical to ensure the security of smart home devices. In the smart home, there are three sorts of authentication mechanisms that can be employed. The first method is single-factor authentication [52][53][54], sometimes known as one-factor authentication. It is the most basic type of IoT device authentication, in which devices or users present something they already know to validate their identity. One-factor authentication is most commonly used with usernames and passwords. The second method is two-factor authentication methods [55][56]. It adds another layer to one-factor authentication of usernames and passwords, requiring users or devices to validate something they own. A one-time password or something unique, such as fingerprints, could be used. The third method is three-factor authentication [57][58]. It is also known as multifactor authentication which takes security to the next level by integrating numerous authentication mechanisms, namely, something you know (password), something you are (fingerprint or iris scan), and something you have (one-time password generator). The authentication mechanisms mentioned above are implemented in many authentication schemes relevant to the smart home ecosystem. The advancement of various authentication systems important to smart home sensor networks and IoT security countermeasures is compared in Table 1.

Table 1. Comparative analysis of the evolution authentication schemes relevant to the smart home

Authors	**Year**	**Authentication Schemes**	**Authentication factor**
Bethencourt et al. [15]	2007	CP-ABE (Ciphertext Policy, Attribute-Based Encryption)	NA
Frank Stajano [16]	2011	FIDO and PICO	Cryptographic keys for a password less
Yeh, H.L. et al. [17]	2011	Elliptical curve cryptography	NA
Z. Shelby, et al. [18]	2014	The Constrained Application Protocol (CoAP)	Web Transfer Protocol
M. Sethi et al. [19]	2014	Extensible Authentication Protocol - Nimble Out of Band (EAP-NOOB)	NA
Yoon Miyeon and Baek Jonghyun [20]	2015	FIDO protocol	The IoT gateway authenticates the IoT devices at the endpoint.
Barreto et al. [21]	2015	TPM (Trusted Platform Module)	NA
Hannes Tschofenig [22]	2016	FIDO (Fast IDentity Online) model	Instead of passwords, it used factor authentication and cryptographic keys.
Raham et al. [23]	2016	A cloud environment is used to interconnect IoT devices.	NA
Abera et al. [24]	2016	Intel SGX, software	hybrid
Amin, R., Biswas, G.P., [26]	2016	Smart cards for a distributed cloud framework	NA
Alpár et al. [25]	2016	U-Prove or Idemix attribute protocols	NA
Das et al. [27]	2016	Multi-gateway WSN's	Three-factor
Chifor, et al. [28]	2018	FIDO UAF (Universal Authentication Framework) protocol	NA

Mishra et al. [29]	2018	Multimedia communication authentication scheme based on a wireless sensor network	NA
Wu et al. [30]	2018	Wireless medical sensor networks	two-factor
Kazmi et al. [31]	2019	Harmony Search Differential Evolution (HSDE)	Implement two heuristic methods
Shin and Kwon [32]	2019	key-exchange protocol	Three-factor
Shidik et al. [33]	2019	Heuristic vs. metaheuristic strategy	NA
Alshahrani and Traore [34]	2019	Cumulative keyed hash chain	Mutual Key
Khan et al. [35]	2019	Biometric-based elliptical curve cryptography	NA
Bae and Kwak [36]	2020	Smart card in a multi-gateway	NA
Naresh et al.[37]	2020	Hyperelliptic Diffie-Hellman curve for WSN	Mutual-key agreement
Santos-Gonzálezet et al. [38]	2020	PAKE scheme for heterogeneous WSN's	key exchange
Masud et al. [40]	2021	Anonymous User-Authority-Preserving User-Authentication Scheme	NA
Shahidinejad et al. [39]	2021	Light edge: A lightweight authentication protocol	NA

4. The smart home security authentication model

There are many Authentication Models that can be used to secure smart home devices. One of these models is shared secret authentication (symmetric) [59]. In cryptography, a shared secret is a piece of data exchanged via secure communication. It refers to the symmetric cryptosystem's authentication key. A challenge-response technique of authentication using a shared secret is the most frequent. During the authentication process, one party asks a question (challenge), and the other side responds with the correct answer (response). The problem with symmetric encryption is to prevent a man-in-the-middle adversary from reading or spoofing the sender message. However, protection can be increased using various IoT encryption techniques, and in addition, a decentralized IoT solution can help avoid these risks. Another model is called public key / digital certificate authentication (asymmetric) [60]. Public-key encryption, often known as public-key cryptography, is a type of encryption that uses public keys. It encrypts the data using two separate keys and makes one of them (the public key) accessible to anyone. The public key infrastructure (PKI) can be used to authenticate operations where simple passwords are insufficient. The associated private key is used to verify identity in cryptography. A public key can, in some cases, be signed by a third-party authority using a digital key certificate (otherwise known as a public key certificate or identity certificate). One more model is a model called the Hardware Security Module (HSM) [61], where different hardware is used to protect keys and can be used to provide authentication and authorization to smart home devices. HSM is a separate hardware module that manages the device's trusted computing requirements, including cryptographic processors and key storage. As a result, HSMs may store and verify digital certificates such as X.509 certificates and SAS tokens. Compared to storing device secrets in a dedicated hardware security module, standard memory is less safe. Furthermore, a TPM [62] is a specialized IoT device chip that maintains device-specific keys for authentication, or the input/output (I/O) interface that connects to modules that perform standard authentication. TPMs come in various shapes and sizes, including firmware-based modules, discrete hardware devices, software-based modules, and integrated hardware equipment. TPM can store public key certificates and is more secure than SAS token-based authentication when compared to symmetric key authentication. Additionally, the TPM in the DPS employs the endorsement key (EK), which is a type of public or asymmetric key. Moreover, the biometric authentication model [63] is a popular user authentication method based on the unique biological characteristics of a user. Devices capable of measuring and recognizing the user's unique physical and/or behavioral characteristics, such as fingerprints, facial features, and others, are used to implement it. However, applying these strategies to IoT device authentication is difficult. Biometric authentication has become a viable solution due to recent advances in Physically Unclonable Functions (PUFs). PUF authentication systems can generate encryption keys that are digital fingerprints, which are analogous to biometrics in that they are unique and unclonable. Table 2 compares IoT-based smart home security protocols, while Table 3 compares the features of the protocols.

Table 2. Comparison of smart home IoT-based security protocols

Protocols	**Definition**	**Operation**	**Pros**	**Cons**
COAP (Constrained Application Protocol) [41]	A protocol to address the needs of HTTP-based IoT systems at the application layer.	Encryption layer rather than SSL.	- Low overheads Encryption provides simple data flows and greater data privacy and protection	- Message unreliability Issues with NAT and firewalls

AMQP (Advanced Message Queuing Protocol) [42]	An open standard application layer IoT protocol	Transactional messages between servers	- Using QOS to ensure message delivery. Adaptable to other IoT standards.	- Heaviness - Not user-friendly
DDS (Data Distribution Service) [43]	The first open international middleware IoT standard	- Data, events, and commands are sent and received between nodes using the publish–subscribe pattern.	- Deployed in multiple settings. - Perfect for real-time and embedded systems. Used for interoperable data exchange	- Too heavyweight to be used in embedded systems. - Does not interface with web services
MQTT (message queueing telemetry transport) [41]	Features a publisher-subscriber messaging model	Simple data flow between different devices	- Very lightweight Ensures message delivery Battery friendly	- Does not support streaming - Not 'developer friendly' - Latency issues
Wi-Fi protocol [44]	The most well-known IoT protocol. Allows adjacent devices within a specific range to connect to the Internet via a hotspot.	Wi-Fi relies on radio waves to send data at specific frequencies.	- Easy to install.	- Affected by the environment and whether. - Range and speed.
HTTP (Hypertext Transfer Protocol) [45]	It is outdated compared to the other IoT protocols.	It assigns IP addresses with recognizable names.	- Addressing the capability of processing large amounts of data, Flexibility	- Excessive electrical consumption
Bluetooth Low Energy (BLE) [46]	Personal area network (WLAN) technology	Radio waves in the 2.4 GHz ISM band are used.	- Integration into modern mobile devices	- Shorter range
HTTP+Nabto [47]	HTTP paired with Nabto Edge	Allows secure remote access to your existing HTTP service	- Built-in security to protect data integrity. - Resolving any data privacy concerns of HTTP - Nabto Edge requires minimal code changes.	- Heavy power consumption.
Z-Wave [48]	A wireless communication protocol largely utilized in smart home applications.	A mesh network that communicates from an appliance to an appliance using low-energy radio waves.	- Can be monitored from a smart device over the Internet	- Coverage is limited. - Requires knowledge to keep it secure from unauthorized people
LoraWan [49]	A Media Access Control (MAC) IoT protocol.	Communicate directly with internet-connected applications	- Use long-range wireless connection	- Large data payloads continuous monitoring. - Not ideal for real-time applications
COAP+Nabto [41]	Nabto Edge supports COAP using the Nabto Edge Direct protocol	Develop request/response clients via COAP	- Increases the reliability of the message. - Privacy is ensured capability to be mapped to both the 2nd and 3rd layers of the OSI model	

Table 3. Comparison of the features of smart home IoT-based security protocols

Protocols	Transport	Low Latency	Data discovery	Messaging Type	Binary Payload Support	Lightweight	Build-in Security	Easy to Build on	Encrypted
COAP [41]	UDP	√	Manual and registration	Sync	√		X	X	X
AMQP [42]		X	Manual	Sync	√	X	X	X	
DDS [43]		√	Automatic		√	√	√	√	
MQTT [41]	TCP	X	Manual	Async	√	√	X	X	X
Wi-Fi protocol [44]	TCP	X	Automatic	√	√	X	X	√	X
HTTP [45]	TCP	√	Manual	Sync	X	X	X	√	X
BLE [46]		√		Async	√	√	√	√	X
HTTP+Nabto [47]	UDP+TCP	√		Sync	√		√	√	√
Z-Wave [48]		√	Automatic	Sync	√	√	√	X	√
LoraWan [49]		X	Automatic	Async	√	√	√	X	√
COAP+Nabto[41]	UDP	√	Automatic	Synchronous	√		√	√	√

5. Smart Home security countermeasure

Implementing safe smart home device authentication and authorization best practices has numerous advantages for the security and privacy of smart home devices. Building a cyber resilience ecosystem and creating scalable solutions that will speed the adoption of best practices and boost cyber resilience will remain challenging. These are a few countermeasures towards better security in smart home devices. The first one is "Never trust; always verify". Malicious actors are always looking for new ways to break into an ecosystem. Monitoring smart home devices to ensure that they are secure and not a gateway for hijackers. Persistent verification of data and devices on the network is a critical component of a zero-trust security strategy. The "Never trust; always verify" part of zero-trust security requires constantly testing the devices and services on a network to ensure that they are functioning correctly. Monitoring devices prevent IoT sprawl, while proper maintenance allows to track how data flows and who interacts with it. The second countermeasure is using an Ethernet cable instead of WiFi to connect devices. In addition, using strong and unique passwords will resist brute force attacks. Moreover, after installing a WiFi network, it is essential to modify the default name. Moreover, using two-step verification is a crucial step in gaining more security. It is recommended to keep the smart home devices up-to-date and turn them off when not in use.

6. Open Problems

With the smart home becoming more mainstream, cybersecurity issues have become a fundamental concern. Smart home devices being accessible via the internet makes them very vulnerable as they can be reached from anywhere and attacked. Furthermore, specific smart home gadgets enabled by the Internet of Things are insecure, putting the privacy and security of user data at risk. Although IoT-based smart home applications have significant advantages, cybersecurity is the main problem that must be addressed before its full benefits can be fully realized. Residents of the smart home can access the smart home equipment remotely via the Internet using any compatible device, such as a smartphone. Remote access to smart home devices and appliances via the Internet requires more effective authentication and authorization mechanisms than static authentication methods can provide. As a result, designing an effective access control system for smart homes is required to ensure their security protection. Although mutual authentication and key agreement are the initial steps to prevent unauthorized use of smart home products and systems, there remains a significant gap in creating an appropriate access control mechanism for the smart home environment. [3].

As homes become more competent and more reliant on technology, the need for a reliable security system that requires minimal human interaction is growing. In a smart home context, standard access control measures are ineffective. Human interventions through password and/or biometric usages are the key emphasis of traditional authentication techniques. In a smart home context, however, the authentication mechanism must be activated automatically by the devices (for example, sensors, appliances, actuators, and so on), with no human input required. Existing smart home access control systems do not take into account the security concerns posed by various devices and apps. Smart home devices are rarely offered effective security solutions due to their limited resources (computation, connectivity, etc.). As a result, most proposed solutions have a significant level of verification overhead, making them unsuitable for use in smart homes. The proposed study must aim to create a lightweight authentication ecosystem and session-key distribution module that is resistant to man-in-the-middle, wiretapped secret-key, and replay attacks. Developing a lightweight access control mechanism for a smart home environment is a challenging problem. With remote access to the smart home with devices such as smartphones, the smart home faces the challenge of being accessed securely over the Internet. This requires mechanisms that confine access to the smart home only to the legitimate user while disallowing malicious activities. Furthermore, because there are now multiple smart home technologies in use, any access control system must consider compatibility.

In addition, there is a need to develop a lightweight scheme to separate smart home devices from the primary or active home network, controlling the data flow, monitoring where these data come from and where it goes all the way down to the port level. Include network monitoring tools that are constantly on the lookout for unusual activities, strange traffic flow demands, traffic requests at odd times, or inappropriate packet sizes

7. Conclusion

The smart home devices being accessible via the internet makes them very vulnerable as they can be reached from anywhere and attacked. Furthermore, specific IoT-enabled smart home gadgets are insecure, putting the privacy and security of users' data in danger. Smart home gadgets are typically diverse in design and limited in resources. Furthermore, such devices communicate with one another using low-power and lossy networks. As a result, many customers' main fear is cybersecurity, which is the key reason why they are hesitant to use smart home technology. As a result, rather than being a tacked-on feature, smart home security should be the primary goal. This article addressed the issues facing the smart home environment. It showed how smart home devices work and the type of security and privacy threats of the smart home. This article can help raise public awareness of the dangers of connected devices and help people make informed decisions about their adoption and use. It also highlighted the various authentication techniques that can be utilized with smart home devices. It also contrasted the various smart home IoT-based security protocols as well as a security countermeasure that can be utilized in a smart home ecosystem.

Acknowledgment

The authors gratefully acknowledge the approval and the support of this research study by grant no. SAT-2018-3-9-F-7828 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

References

[1] Y., X. Dong, Sun, and W. Chang, "Influence of characteristics of the Internet of Things on consumer purchase intention", *Social Behavior and Personality: an international journal*, vol. 42, no. 2, pp. 321-330, 2014

[2] M. Noack, "Optimization of Two-Way Authentication Protocol in Internet of Things", 2014.

[3] Pardeep Kumar, An Braeken, Andrei Gurtov, Jari Iinatti, and Phuong Hoai Ha, Anonymous Secure Framework in Connected Smart Home Environments, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 12, NO. 4, APRIL 2017

[4] Bogdan-Cosmin Chifora Ion Bica, Victor-Valeriu Patriciua, Florin Pop, A security authorization scheme for smart home Internet of Things devices, Future Generation Computer Systems, Volume 86, September 2018, Pages 740-749

[5] Tao, M.; Ota, K.; Dong, M. Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes. Future Gener. Comput. Syst. 2017, 76, 528–539.

[6] Qu, C.; Tao, M.; Yuan, R. A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes. *Sensors* 2018, *18*, 2784.

[7] Bertino, E. Data security and privacy in the IoT. In Proceedings of the 19th International Conference on Extending Database Technology, Bordeaux, France, 15–18 March 2016; pp. 1–3.

[8] Ala Al-Fuqaha ; Mohsen Guizani ; Mehdi Mohammadi ; Mohammed Aledhari ; Moussa Ayyash, Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, IEEE Communications Surveys & Tutorials, 2015, Volume: 17 , Issue: 4, 2347 – 2376.

[9] Mussab Alaa, A.A. Zaidan, B.B. Zaidan, Mohammed Talal, and M.L.M. Kiah, A review of smart home applications based on Internet of Things, Journal of Network and Computer Applications, Volume 97, 1 November 2017, Pages 48-65.

[10] Barnana Baruah, Subhasish Dhal, A two-factor authentication scheme against FDM attack in IFTTT based Smart Home System, Computers & Security, Volume 77, August 2018, Pages 21-35

[11] Kuen-Min Lee ; Wei-Guang Teng ; Ting-Wei Hou, Point-n-Press: An Intelligent Universal Remote Control System for Home Appliances, IEEE Transactions on Automation Science and Engineering, July 2016, (Volume: 13 , Issue: 3, Page(s): 1308 – 1317.

[12] Fernandes, Rahmati, Jung, & Prakash Fernandes E, Rahmati A, Jung J, Prakash A. Decoupled-IFTTT: Constraining privilege in trigger-action platforms forthe internet of things, 2017, arXiv:1707.00405 [cs.CR].

[13] Min, and Varadharajan, B. Min, V. Varadharajan, Design and analysis of a new feature-distributed malware, Proceedings of the IEEE thirteenth international conference on trust, security and privacy in computing and communications (2014), pp. 457-464.

[14] K. Bhargavan, A.D. Lavaud, C. Fournet, A. Pironti, P.Y. Strub, Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS Proceedings of the IEEE symposium on security and privacy (2014), pp. 98-113

[15] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: 2007 IEEE Symposium on Security and Privacy (SP'07), IEEE, 2007, pp. 321–334.

[16] F. Stajano, Pico: No more passwords!, in: International Workshop on Security Protocols, Springer, 2011, pp. 49–81.

[17] Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H., Wei, H.W., 2011. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography.Sensors 11 (5), 4767–4779.

[18] Z. Shelby, K. Hartke, and C. Bormann, The constrained application protocol (CoAP), 2014, https://tools.ietf.org/html/rfc7252.

[19] M. Sethi, E. Oat, M. Di Francesco, T. Aura, Secure bootstrapping of cloudmanaged ubiquitous displays, in: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, in: UbiComp'14, ACM, New York, NY, USA, 2014, pp. 739–750.

[20] M. Yoon, J. Baek, A study on framework for developing secure IoT service, in: Advances in Computer Science and Ubiquitous Computing, Springer, 2015, pp. 289–294.

[21] L. Barreto, A. Celesti, M. Villari, M. Fazio, A. Puliafito, An authentication model for IoT clouds, in: Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2015, ACM, 2015, pp. 1032–1035.

[22] H. Tschofenig, Fixing user authentication for the internet of things (IoT), Datenschutz und Datensicherheit-DuD 40 (4) (2016) 222–224.

[23] A.F.A. Rahman, M. Daud, M.Z. Mohamad, Securing sensor to cloud ecosystem using internet of things (IoT) security framework, in: Proceedings of the International Conference on Internet of Things and Cloud Computing, ACM, 2016, p. 79.

[24] T. Abera, N. Asokan, L. Davi, F. Koushanfar, A. Paverd, A.-R. Sadeghi, G. Tsudik, Invited-things, trouble, trust: on building trust in IoT systems, in: Proceedings of the 53rd Annual Design Automation Conference, ACM, 2016, p. 121.

[25] G. Alpár, L. Batina, L. Batten, V. Moonsamy, A. Krasnova, A. Guellier, I. Natgunanathan, New directions in IoT privacy using attribute-based authentication, in: Proceedings of the ACM International Conference on Computing Frontiers, ACM, 2016, pp. 461–466

[26] Amin, R., Biswas, G.P., 2016. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad HocNetw. 36, 58–80.

[27] Das, A.K., Sutrala, A.K., Kumari, S., Odelu, V., Wazid, M., Li, X., 2016. An efficientmulti-gateway-based three-factor user authentication and key agreementscheme in hierarchical wireless sensor networks. Secur. Commun. Networks 9(13), 2070–2092.

[28] Chifor, B.C., Bica, I., Patriciu, V.V. and Pop, F., 2018. A security authorization scheme for smart home Internet of

Things devices. Future Generation Computer Systems, 86, pp.740-749.

[29] Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, SK.H., Gope, P., 2018.Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. Multimedia Tools Appl.77(14),18295–18325.

[30] Wu, F., Li, X., Sangaiah, A.K., Xu, L., Kumari, S., Wu, L., Shen, J., 2018. A lightweightand robust two-factor authentication scheme for personalized healthcaresystems using wireless medical sensor networks. Future Generat. Comp. Syst.82, 727–737.

[31] Kazmi, S., Javaid, N., Mughal, M.J., Akbar, M., Ahmed, S.H., Alrajeh, N., 2019. Toward the optimization of metaheuristic algorithms for IoT-enabled smart homestargeting balanced demand and supply of energy. IEEE Access 7, 24267–24281.

[32] Shin, S., Kwon, T., 2019. A lightweight three-factor authentication and keyagreement scheme in wireless sensor networks for smart homes. Sensors 19(9), 2012–2036.

[33] Shidik, G., Kusuma, E., Nuraisha, S., Andono, P., 2019. Heuristic vs. Meta heuristic method: improvement of spoofed fingerprint identification in IoT devices. Int.Rev. Modell. Simul. (IREMOS) 12 (3), 168–175

[34] Alshahrani, M., Traore, I., 2019. Secure mutual authentication and automated accesscontrol for IoT smart home using cumulative keyed-hash chain. J. Inf. SecurityAppl. 45, 156–175.

[35] Khan, A.A., Kumar, V., Ahmad, M., 2019. An elliptic curve cryptography basedmutual authentication scheme for smart grid communications using biometricapproach. J. King Saud Univ.-Comp. Inf. Sci., 1–8

[36] Bae, W.I., Kwak, J., 2020. Smart card-based secure authentication protocol in multi-server IoT environment. Multimedia Tools Appl. 79 (23-24), 15793–15811.

[37] Naresh, V.S., Reddi, S., Murthy, N.V.E.S., 2020. Provable secure lightweight multiple-shared key agreement based on hyper elliptic curve Diffie-Hellman for wirelesssensor networks. Inf. Sec. J.: Global Perspective 29 (1), 1–13

[38] Santos-González, I., Rivero-García, A., Burmester, M., Munilla, J., Caballero-Gil, P.,2020. Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks. Inf. Syst. 88, 101423–101434

[39] Shahidinejad, A., Ghobaei-Arani, M., Souri, A., Shojafar, M., Kumari, S., 2021. Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloudenvironment. IEEE Consum. Electron. Mag. 1-1.

[40] Masud, M., Gaba, G.S., Choudhary, K., Hossain, M.S., Alhamid, M.F., Muhammad, G.,2021. Lightweight and anonymity-preserving user authentication scheme forIoT-based healthcare. IEEE Internet Things J. 1-1.

[41] Silva, D.; Carvalho, L.I.; Soares, J.; Sofia, R.C. A Performance Analysis of Internet of Things Networking Protocols: Evaluating MQTT, CoAP, OPC UA. Appl. Sci. 2021, 11, 4879. https://doi.org/ 10.3390/app11114879

[42] OASIS. AMQP Advanced Message Queuing Protocol. 2018. Available online: http://www.amqp.org/ (accessed on 20 Dec. 2021).

[43] OMG. DDS Data Distribution Service. Available online: http://portals.omg.org/dds/what-is-dds-3/ (accessed on 20 Dec. 2021).

[44] Hussain et al. "Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks." Journal of communications and networks 16.4 (2014): 397-406.

[45] Pettersson, William. "An Evaluation of IoT Protocol Efficiency and suitability: For smart vehicles, smart homes & industrial scenarios." (2021).

[46] Dian, F. John, Amirhossein Yousefi, and Sungjoon Lim. "A practical study on Bluetooth Low Energy (BLE) throughput." 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2018.

[47] Pettersson, William. "An Evaluation of IoT Protocol Efficiency and suitability: For smart vehicles, smart homes & industrial scenarios." (2021).

[48] Kim, Taehong. "A study of the Z-wave protocol: implementing your own smart home gateway." 2018 3rd International Conference on Computer and Communication Systems (ICCCS). IEEE, 2018.

[49] Leonardi L, Lo Bello L, Battaglia F, Patti G. Comparative Assessment of the LoRaWAN Medium Access Control Protocols for IoT: Does Listen before Talk Perform Better than ALOHA? Electronics. 2020; 9(4):553. https://doi.org/10.3390/electronics9040553

[50] Hoyul Choi, Hyunsoo Kwon, Junbeom Hur, ‘‘A Secure OTP Algorithm Using a Smartphone Application', IEEE Seventh International Conference on Ubiquitous and Future Networks ICUFN Aug – 2015, pp. 476-481.

[51] Kaspersky Report, “Kaspersky IoT cyberattacks report 2021” retrieved from https://www.kaspersky.com/about/press-releases, accessed on 10/12/2021.

[52] Lei et al. "The insecurity of home digital voice assistants-vulnerabilities, attacks, and countermeasures." *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018.

[53] Velsquez, Ignacio, Anglica Caro, and Alfonso Rodrguez. "Authentication schemes and methods." *Information and Software Technology* 94.C (2018): 30-37.

[54] Pal, Debajyoti, Xiangmin Zhang, and Saeed Siyal. "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach." *Technology in Society* 66 (2021): 101683.

[55] Kaur, Damandeep, and Devender Kumar. "Cryptanalysis and improvement of a two-factor user authentication scheme for smart home." *Journal of Information Security and Applications* 58 (2021): 102787.

[56] Zou et al. "A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT." *IEEE Systems Journal* (2021).

[57] Yu, Sungjin, Namsu Jho, and Youngho Park. "Lightweight Three-Factor-Based Privacy-Preserving Authentication Scheme for IoT-Enabled Smart Homes." *IEEE Access* 9 (2021): 126186-126197.

[58] Shin, Sooyeon, and Taekyoung Kwon. "A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart homes." *Sensors* 19.9 (2019): 2012.

[59] Satapathy, Utkalika, et al. "An ECC based lightweight authentication protocol for mobile phone in smart home." *IEEE 13th international conference on industrial and information systems (ICIIS)*. IEEE, 2018.

[60] Liu, Yunqiang, et al. "An efficient privacy protection solution for smart home application platform." *2016 2nd IEEE International Conference on Computer and Communications (ICCC)*. IEEE, 2016.

[61] Batalla, Jordi Mongay, and Franciszek Gonciarz. "Deployment of smart home management system at the edge: mechanisms and protocols." *Neural Computing and Applications* 31.5 (2019): 1301-1315.

[62] Lu, Di, et al. "xTSeH: A trusted platform module sharing scheme towards smart IoT-eHealth devices." *IEEE Journal on Selected Areas in Communications* 39.2 (2020): 370-383.

[63] Al-Mutawa, Rihab Fahd, and Fathy Albouraey Eassa. "A smart home system based on internet of things." *arXiv preprint arXiv:2009.05328* (2020).

Abdulbasit A. Darem (Ph.D.) is an Assistant Professor at the Department of Computer Science, Northern Border University, Saudi Arabia. He completed his Ph.D. in Computer Science from University of Mysore, India in 2014. He has more than 20 years of experience in the IT field. He published more than 21 research papers in reputed international journals and conferences. His area of research includes, Cybersecurity, Web engineering, HCI, usability, E-government, and Cloud Computing.

Asma A. Alhashmi (Ph.D.) is an Assistant Professor at the Department of Computer Science, Northern Border University, Saudi Arabia. She completed her Ph.D. in Computer Science from University of Mysore, India in 2015. She has more than 10 years of experience in the IT field. She published more than 19 research papers in reputed international journals and conferences. Her area of research includes, Cybersecurity, Software engineering, E-government, and Cloud Computing.

Prof. Jemal H. Abawajy (BSE, M.Sc., Ph.D., D.Sc.) is a full Professor in the Faculty of Science, Engineering and Built Environment, Deakin University, Australia. Prof. Abawajy has delivered more than 60 keynotes worldwide and Prof. Abawajy is the author/co-author of several books and about 400 refereed papers in premier venues and supervised numerous Ph.D. students to completion. Prof. Abawajy have been actively involved in the organization of more than 350 conferences all over the world in various capacity including chair, general co-chair, vice-chair, best paper award chair, publication chair, session chair and program committee. He has also served/serving on the editorial board of numerous international journals including the IEEE Transaction on Cloud Computing.