IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 3, 2022, accepted January 14, 2022, date of publication January 31, 2022, date of current version February 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3148140

Ranking Security of IoT-Based Smart Home Consumer Devices

NABA M. ALLIFAH[1] AND IMRAN A. ZUALKERNAN[2], (Member, IEEE)

[1]Department of Engineering Systems Management, American University of Sharjah, Sharjah, United Arab Emirates
[2]Department of Computer Science and Engineering, American University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Imran A. Zualkernan (izualkernan@aus.edu)

This work was supported in part by the Open Access Program from the American University of Sharjah.

ABSTRACT Manufacturers of smart home consumer devices like home theatres, music players, voice-based assistants, smart lighting, and security cameras have widely adopted the Internet of Things (IoT). These devices pose a significant security risk to consumers because the devices are exposed to mobile applications and cloud-based services with known security vulnerabilities. Most current home consumer devices provide little or no information about the level of security they afford. Since most consumers are not tech-savvy, it is currently difficult for a consumer to make an informed decision about which consumer device model (e.g., smart television model) has the best security. Hence, consumers need an objective security ranking of each type (e.g., security cameras) of home consumer devices. This paper proposes a novel methodology to systematically build such security rankings for home consumer devices. The proposed methodology can be applied by utilizing data from any security assessment study. The paper discusses previous efforts in applying Analytic Hierarchy Process (AHP) to rank security risks in general. The paper also presents a systematic survey of security vulnerabilities of smart home consumer devices when viewed from an IoT lens. Using the proposed methodology, a case study, employing an AHP model for ranking commonly used home consumer devices including home theatres, security cameras, smart lighting, smart speakers, video surveillance, smart switches, home automation systems, home security systems, smart routers, wireless doorbell cameras, and home audio systems, was developed. Relative security rankings for each type of consumer device were derived from the AHP model. According to the AHP model, network security was the primary driver of smart home device security with a priority of 0.6893 while application security had the least priority of 0.0591. Critical Vulnerabilities were the most important for device security (priority=0.4397), Man-in-The-Middle attacks for network security (priority=0.2019), exploitable services for cloud security (priority=0.26), and sensitive data for application security (0.7626). The AHP model was internally consistent (Consistency Ratio < 0.1). Sensitivity analysis showed that the AHP model was robust against pairing assumptions.

INDEX TERMS AHP, consumer applications, cloud computing, home consumer devices, Internet of Things, network security, smart home.

I. INTRODUCTION

Smart home automation goes back to at least 1985 [1]. Recently, manufacturers of many smart home automation systems and associated devices like surveillance cameras, home voice assistants (e.g., Alexa), and appliances (e.g., fridge) have embraced the Internet of Things (IoT) [2]. Exposing a smart home and devices to the internet raised security concerns as early as 2006 [3]. Smart home security is about protecting privacy of information embedded in a home environment, preserving confidentiality and integrity of consumer's data, and ensuring 24/7 availability of smart home services [4]. A recent study showed that 40.3% of smart homes worldwide had five or more devices connected to the internet, and that 40.8% of homes had at least one vulnerable device that puts the entire home at risk [5]. Similarly, Williams *et al.* [6], Notra *et al.* [7], and Ling *et al.* [8] demonstrated that security of webcams, televisions, home printers, smart lightbulbs, smart plugs, smart power switches and smoke-alarms could be easily compromised. Celik *et al.* [9] identified security issues in a number of IoT programming platforms. Software development

The associate editor coordinating the review of this manuscript and approving it for publication was Zhenhui Yuan.

kits for smart home applications (Apps) also have security issues [10]. Mare *et al.* [11] exposed security flaws in commercially available consumer smart home hubs. The security challenges to smart homes and smart grid have also been explored in [12]–[15].

Consumers are generally aware of security risks associated with consumer devices and are willing to pay for security labeling of such devices [16]. While consumers tend to trust IoT device manufacturers to protect their privacy, neither do they verify nor are they aware of the various privacy risks posed by these devices [17]. Consequently, security labels for IoT consumer devices clearly indicating security mechanisms (e.g., security updates, access control, encryption), data practices (e.g., whether the data is stored on the device or on the cloud), and additional information (e.g., physical actuation) have been proposed [18]. Simplified consumer security indexes for such security-awareness labels have been proposed to inform consumers [19]. Even if these labels were available, as have been proposed in UK, Netherlands and Singapore, the proposed security labels are not easily interpretable by a typical consumer. For example, it is unreasonable to assume that a layperson can intelligently compare two encryption standards stated on labels of competing electronic music players.

Determining the relative security of a type of consumer device is a complex Multi-Criteria Decision-Making (MCDM) problem because a host of interacting factors based on device hardware, networking, middleware, etc., and types of potential security vulnerabilities contribute towards making this decision [20]. Mardani *et al.* [21] conducted an extensive survey of techniques for solving MCDM problems and found that Analytic Hierarchy Process (AHP) [22] was the top method for solving MCDM problems. One key advantage of using AHP is that the technique can easily incorporate both numeric and qualitative, or judgment-based inputs, and is flexible to incorporate both types of data. Furthermore, AHP can be applied transparently and easily by conducting pair-wise comparisons against individual criterion. Finally, the AHP also provides a mathematical formula to measure the internal consistency in the how the data is being used to make decisions, and hence providing a measure of the quality of goodness of the decision model.

This paper proposes an AHP-based methodology of how to develop a simplified security ranking for various types of consumer devices (e.g., smart televisions). The ranking thus developed can be used by consumers to easily assess the relative security of competing device choices. For example, when selecting which smart television set to buy, a consumer can refer to the relative security rankings of smart television sets available, and make an informed choice. The paper makes the following contributions.

- The paper presents a comprehensive survey of use of AHP to rank security aspects of computer-related systems.
- The paper presents a systematic survey of security vulnerabilities of smart home consumer devices.
- The paper presents a novel methodology for applying AHP that relies on a systematic literature review and on empirical data from security assessment studies.
- The paper presents a case study to build and validate an AHP model to determine the relative importance of key factors that have an impact on security of smart home devices today. To our knowledge this has not been done before.

The rest of the paper is organized as follows. Previous work on using AHP to assess security in a variety of computer-related domains is presented first. A systematic survey of consumer device security vulnerabilities is presented next. This is followed by an example and a description of a novel AHP methodology utilizing systematic literature review and empirical data from a security study. The methodology is then applied to many consumer devices, and the resulting AHP model is presented and discussed. Paper ends with limitations and conclusions.

II. PREVIOUS WORK

A. USING AHP TO ASSESS SECURITY

AHP is a well-known technique for solving MCDM problems [22], [23]. AHP is briefly described below followed by a discussion of previous work in applying AHP to assess security is various computer-related domains.

AHP begins by defining the problem and determining a goal. For example, for this paper the goal was to assess the relative security of a type of smart home consumer device (e.g., Which personal assistant is more secure?). The goal for AHP can be very general like "assessing cybersecurity," or be very specific like "assessing security of nuclear plants." Based on the goal, an AHP hierarchy is developed where levels of the hierarchy represent criteria and sub-criteria. For example, information security criteria like integrity, access control, authentication, availability, etc. are potential top-level AHP criteria. The next step in AHP requires a pairwise comparison of each criterion and sub-criteria. For example, if confidentiality and availability were the two chosen criteria, then a relative importance of one versus the other needs to be established; an expert could indicate that confidentiality was significantly more important than availability in a specific situation. Based on pairwise comparisons, a comparison matrix is then constructed for each level. Subsequently, the AHP algorithm assigns relative priority to each criterion and sub-criteria in the hierarchy. Higher priority means more contribution towards the goal. Relative priorities of the various criteria can then be used to rank any decision alternatives. For example, Syamsuddin and Hawng [24] used AHP to determine, that for information security, cultural elements had the highest priority, followed by economy, management, and technology. The final step in the AHP methodology is to determine internal consistency of the pairwise comparisons. Previous work in applying AHP to assess security in various computer-related and information technology domains is presented next.

Maček *et al.* [25] used AHP to assess cyber security risks and used top-level criteria like attacks, vulnerabilities, and penetration testing, etc. AHP comparison relied on expert opinions after being provided with a systematic literature review. The results show that AHP facilitated fine-tuning of the cybersecurity risk assessment procedures. Similarly, Bhol *et al.* [26] presented a taxonomy of cyber security criteria of vulnerabilities, threats, users, protection mechanism and encounter outcomes. The primary goal was to evaluate cyber security strength. The process of pairwise comparisons was not specified. Zhao *et al.* [27] proposed a methodology for evaluating system security using the criteria of host security, network security, and vulnerability security. They showed that by using AHP and grey relational analysis theory, it was possible to effectively quantify the comprehensive security of the network while avoiding the subjectivity and one-sidedness of traditional security assessment methods through experimental verification. Sohime *et al.* [28] used AHP to rank the relative importance of various cyber security skills required in the job market. The criteria used were soft skills (e.g., analytical skills), technical skills (e.g., ability to identify potential risks) and certifications (e.g., related security technical/management certifications).

In the information security domain, Zaburko and Szulżyk-Cieplak [29] used AHP to evaluate the risk of information loss among employees. The criteria used were human dependent (e.g., procedural violation), technical (e.g., hardware failure) and random (e.g., consumption wear). Using expert opinions for comparisons, more information was found to be lost based more on human factors than others. Similarly, Bodin *et al.* [30] used AHP with criteria of confidentiality, data integrity and availability, and emphasized the utility of AHP to assist and organize the ideas of an organization's chief information security officer (CISO).

In the IoT domain, Wang *et al.* [31] used AHP to determine the security of identity resolutions based on two primary criteria of trust and user experience. For trust, sub-criteria included historical trust, leakage rate, and malicious resolution rate. For user experience, average resolution delay, resolution conscience, and integrity were used as sub-criteria. All AHP comparisons were based on expert opinions. Similarly, Siboni *et al.* [32] used AHP to determine the relative security of IoT devices. The AHP model was implemented using a device-centric method that considered both device-specific and domain-related features. The criteria used were known vulnerabilities (e.g., software, hardware, and firmware), sensor capabilities (e.g., movement and position, environmental, multimedia, connectivity, and health monitoring), and the operational context (e.g., mobility, time, and location). Varma and Chandra [33] used Fuzzy AHP (FAHP) to assess security of fog-IoT systems. The primary criteria included authentication, access control, intrusion detection, trust and integrity, and the sub-criteria included legitimacy, identification, rapid response, accountability, and credibility. The comparisons were based on expert opinions. Ogundoyin and Kamil [34] used AHP to assess the level of trust in fog computing and sub-criteria included latency and reliability. They used quality of service, quality of security as the two primary criteria. Expert opinions were used for pairwise comparisons. Wang *et al.* [35] used AHP and another MCDM technique called Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to rank the security of IoT devices in the healthcare environment. The thirteen criteria included confidentiality, authentication, access control, and integrity, etc. Expert opinion along with the Delphi technique [36] was used for doing comparisons. Ly *et al.* [37] used fuzzy set theory and AHP to build a rule-based decision support mechanism to evaluate enterprise IoT security and used the criteria of connectivity, telepresence, intelligence, security, and value. Expert opinions were used for comparisons. The tangible variables (e.g., security, value, and connectivity) were found to be more essential for security than the intangible factors (e.g., telepresence and intelligence). Zhang *et al.* [38] evaluated security of IoT systems using FAHP as early as 2011. They used perceptual, transport, application, and cloud security as the primary criteria. Perceptual layer included sub-criteria like intelligent node security and node's information control certificates, etc. Similarly, the transport security criteria included the sub-criteria of network security, risks of Internet Protocol version 6 (IPV6), etc. The application security criteria included role identification efficiency, normal working hours, and software disaster control capability, etc. Finally, the cloud security criteria included sub-criteria like cloud computing platform security, user access control capability, information application security, etc. Expert judgments were used for comparisons. Security concerns related to perceptual layer were found to be the most important in 2011.

In the web applications domain, Kumar *et al.* [39] used FAHP-TOPSIS to assess usable-security. They used criteria of security and usability where security included the sub-criteria of confidentiality, integrity, accountability, authentication, and durability, while usability included appropriateness recognizability, operability, user error protection, user interface aesthetics, and accessibility. Expert opinion was used for pairwise comparisons. Agrawal *et al.* [40] used FAHP and Fuzzy TOPSIS for assessing the sustainable security of web applications. Expert opinions were used with the criteria of confidentiality, integrity, availability, and durability. The evaluation was based on two case studies and six projects. Lai *et al.* [41] used AHP to assess security threats to websites. They used the two criteria of accidental threat (e.g., hardware/software failure, ineffective management, operational error) and malicious threat (e.g., physical attack, malicious code attack, network attack, ultra vires or abuse, information leakage).

In applications domain Alharbi *et al.* [42] used AHP and TOPSIS to provide rankings for security of a healthcare applications. Criteria included integrity, access control, confidentiality, and authentication. Expert opinions were used for doing comparisons. Kumar *et al.* [43] used Hesitant FAHP-TOPSIS approach to assess usability-security. They used security and usability as the top-level criteria. The sub-criteria were confidentiality, accountability, authentication, and durability. For usability, they used the sub-criteria of appropriateness recognizability, operability, error-protection and comprehensibility, and user-interface aesthetics. Expert practitioners were asked to do the pairwise comparisons. Kim *et al.* [44] used AHP to examine cyber-attack taxonomy in Nuclear Power Plants. The primary criteria were divided into attacker related variables with sub-criteria like attack skill and intensity, and target related variables that included the sub-criteria of physical access, logical access, and attack surface. Questionnaires and expert views were used to determine relative significance. Attack skill and physical access, logical access, and attack surface were found to be the most important criteria. Phudphad *et al.* [45] used AHP to assess the impact of security aspects of Human Resource Information Systems (HRIS) on the work climate. They used confidentiality, integrity, non-repudiation, privacy, and availability as the key criteria. Expert opinion was used for comparisons and the results suggest that the most crucial factor was confidentiality, followed by non-repudiation and privacy. Zhang *et al.* [46] proposed a three-layer AHP evaluation model for E-Commerce security. Primary criteria were technical criterion with sub-criteria of network and system security, environmental criterion with sub-criteria of legal and cultural security, and managerial criterion with sub-criteria of personnel and equipment security. Experts were used for comparisons, and the Dempster–Shafer (DS) theory of evidence was applied. The model was shown to be capable of handling both qualitative and quantitative data. Syamsuddin and Hawng [24] utilized AHP to assist banking decision-makers in analysing information on security areas such as management, technology, economy, and culture. The AHP model was derived from questionnaire responses and expert evaluations. According to the findings, the top priority in terms of information security was cultural elements, followed by economy, management, and technology.

In the cloud domain, Tariq *et al.* [47] used FAHP to prioritize and select the most appropriate collection of information security controls to meet the organization's information security requirements for cloud and sensor networks. Criteria like effectiveness, risk, budgetary constraints, exploitation, maintenance, and mitigation time were used. Expert opinions were used for comparison. The use of FAHP resulted in a more efficient and cost-effective evaluation and assessment of information security controls within an organization, allowing the most appropriate one to be selected based on the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). Ruo-Xin *et al.* [48] used AHP to determine Cloud Security. The primary criteria were technical requirements and administrative requirements. The technical requirements criterion included the sub-criteria of physical security, network security, host system security, application security, data security, and safety management systems. Administrative criterion included safety management institution, safety management, system construction management, system operational management, and service level agreement management. Expert opinions using the Delphi method were used for comparisons. Finally, Taha *et al.* [49] used AHP to assess and benchmark security provided by a Cloud Service Provider based on its Security Service Level Agreement (sSLA). Compliance, data governance and information security were used at the top-level criteria. Compliance criterion included the sub-criteria of audit-planning, independent audits and third-party. Data handling and governance policy were the sub-criteria used for governance criterion, and baseline acquirements and policy reviews were used as sub-criteria for information security criterion.

In the networking domain, Li *et al.* [50] used an improved AHP based on D-S evidence and Gray Theory to assess network security risks. The top-level criteria included assets (e.g., tangible and intangible), access control (e.g., user access management), and communication (e.g., computer network management). Expert opinions were used for pairwise comparisons. The results showed that the proposed technique could potentially increase the reliability of network security risk assessments. Dong *et al.* [51] used a modified AHP called D-AHP to evaluate security of smart grids. The top-level criteria used included smart terminal, wireless communication channel, password security, application code and the embedded system. Similarly, Yan and Qiao [52] used AHP to assess network security. Top-level criteria used included hardware risk, software risk, and information risks. Sub-criteria for hardware risk criterion were circuit security, network equipment security and computer security. Software security risk criterion included application, database, and operating system security. Information risk criterion included data backup, access control, encryption, and confidentiality strategy. Communication risk criterion included encryption, anti-virus, intrusion detection and firewall. Sub-criteria for organization management risk criterion were security education, management systems, and organization. Physical environment sub-criteria were security power supply, physical equipment protection, physical monitoring, and physical access control. Expert opinion using the Delphi technique was used for pairwise comparisons. Finally, Zhang *et al.* [53] used a combination of FAHP and variable weight theory to assess wireless network security using the top-level criteria of authenticity, availability, confidentiality, and integrity. A case study suggested that the FAHP variable-weight technique for assessing wireless network security was both efficient and practical.

In summary, as Table 1 shows, many variants of AHP models were developed in a variety of security domains. However, in most cases, the pairwise comparisons were based on expert opinions. In one case, experts were provided with a literature review as background information before seeking their opinions. A word cloud for the top-level criteria from Table 1 is shown in FIGURE 1. The word cloud shows that many previous studies used the traditional security dimensions of confidentiality, integrity, authentication, availability,

TABLE 1. Previous work in applying AHP to assess security in various domains.

Domain	Year	Ref.	AHP Security Goal	Top-Level Criteria
Cyber Security	2021	[25]	Cyber Security	Attacks, vulnerabilities, and penetration testing
	2021	[26]	Cyber Security	Vulnerabilities, threats, users, protection mechanisms. encounters
	2020	[28]	Cyber Security Skills	Soft skills, technical skills, certifications
	2020	[27]	System Security Controls	Effectiveness, risk, budgetary constraints, exploitation, maintenance, mitigation time
Information Security	2019	[29]	Information Loss Security	Human dependent, technical, random
	2005	[30]	Security Investments	Confidentiality, data integrity, availability
IoT Security	2021	[31]	Identity Resolution Security	Trust, user experience
	2020	[32]	IoT Device Security	Known vulnerabilities, sensor capabilities, operational context
	2020	[33]	Fog-IoT Security	Authentication, access control, intrusion detection, trust, integrity
	2020	[34]	Level of Trust in Fog	Quality of service, quality of security
	2020	[35]	Internet of Health Security	Confidentiality, authentication, access control, and integrity
	2018	[37]	IoT in the Enterprise	Tangible factors, intangible factors
	2011	[38]	IoT Security	Perceptual, transport, application, and cloud security
Web Application Security	2020	[39]	Website Usability-Security	Confidentiality, integrity, accountability, authentication, durability, usability
	2019	[40]	Sustainable Security	Confidentiality, integrity, availability, per-durability
	2016	[41]	Website Security	Accidental threat, malicious threat, physical attach, malicious code, or virus
Application Security	2021	[42]	Software Security	Integrity, access control, confidentiality, and authentication
	2020	[43]	Usability Security	Confidentiality, integrity, accountability, authentication, durability, usability
	2020	[44]	Nuclear Plant Security	Attacker's skill, physical access, logical access, and attack surface
	2017	[45]	HRIS Security	Confidentiality, integrity, non-repudiation, privacy, and availability
	2012	[46]	E-Commerce Security	Technical, environmental, managerial
	2009	[24]	E-Banking Security	Management, technology, economy, and culture
Cloud Security	2020	[47]	Information Security Control	Effectiveness, risk, budgetary constraints, exploitation time, maintenance time
	2014	[48]	Cloud Security	Technical (physical security, etc.), management (safety management, etc.)
	2014	[49]	Security Level Agreements	Compliance, data governance, information security
Network Security	2021	[50]	Network Security	Assets, access control, communication
	2020	[51]	Smart Grid Security	Smart terminal, wireless channel, password security, app. code, embedded system
	2012	[52]	Network Security	Software, hardware, information, communication, organization, physical environment
	2010	[53]	Wireless Security	Authenticity, availability, confidentiality, integrity, non-repudiation

FIGURE 1. Word cloud of the top-level AHP criteria used for security.

etc. as the primary top-level criteria. Further, most studies required experts and assumed that experts could meaningfully judge the relative weights of each criterion. A final observation is that AHP criteria were developed based on the goal and the ability to conduct meaningful pairwise comparisons using either experts or some other means. Consequently, the goal and availability of opinions or data to make pairwise comparison dictated the design of the actual AHP hierarchy used.

B. SURVEY OF SMART HOME SECURITY

A typical smart home today contains a variety of consumer devices including surveillance cameras, voice-assistants, thermostats, smart televisions, music streamers, smart lighting, etc. As FIGURE 2 shows, smart homes often utilize heterogenous networks. For example, the three signal symbols in FIGURE 2 refer to different wireless technologies; purple signals refer to ZigBee networking, blue signals refer to Bluetooth networking, and green signals refer to Wi-Fi networking. Some consumer devices may also be connected to a smart home management system using a home area network. Many smart home devices interact with a consumer's mobile phone and use internet gateways to communicate with remotely hosted services offered by various commercial providers [54]. For example, most home security cameras store video on remote servers that can be accessed by consumers anytime anywhere. Similarly, smart assistants like Alexa also leverage cloud-based services. Recently, there is also a trend to move computation from the cloud to the edge devices [55], [56] within smart homes to enact some services locally partially contributing to better network security.

Efforts are also underway to broadly characterize security risks and vulnerabilities of smart home consumer devices [57]. Reference architectures for implementing smart home security at the system level have been proposed as well [58]. There are many ways to conceptualize smart home security [59], [60]. However, this paper uses an IoT lens where smart home security is viewed from the four perspectives of device security, network security, cloud security and application security [20], [38]. Using this lens, consumer devices in a smart home are considered IoT edge devices that can sense, record, and communicate data. A security camera or a voice-based home assistant like Alexa, for example, senses and connects to the outside world through a gateway which could be a home router. The IoT gateways collect data from sensing devices, and transmit the data to cloud-hosted servers that, in turn, provide consumer services. For example, when motion is detected by a security camera, a recording of the associated video is optionally saved locally, and also transmitted remotely to the cloud for storage or further analysis. Finally, most smart home devices provide mobile Apps to allow a consumer to configure and interact with the smart home device. For example, in the case of a security camera, a mobile App lets consumers configure the camera, and connect to servers on the cloud to access the recorded videos.

Based on the IoT lens of a smart home, a survey of recent work in smart home security since 2016 was conducted to answer the following four research questions.

RQ1: What are the common vulnerabilities of smart home consumer devices when viewed as IoT edge devices?

RQ2: What are the common vulnerabilities of networking when used with smart home devices?

RQ3: What are the common vulnerabilities of cloud when used with smart home devices?

RQ4: What are the common vulnerabilities of applications when used with smart home devices?

Table 2 shows the results of searching in the four commonly used digital libraries by using the most frequently used keywords used in the highest cited papers in the area. The keywords used included IoT security, Cybersecurity, Smart Device, Privacy, Information Security, Attack Surface, Communication, Cloud Security, Security of Data, Heterogeneity, Ontology, Home Automation, etc.

The papers were filtered to include only the relevant papers for smart home security. Survey results based on the filtered papers are described below.

1) RQ1: SMART HOME DEVICE SECURITY

IoT edge devices suffer from many vulnerabilities. For example, one vulnerability is eavesdropping where an attacker listens in to the data being transferred to and from a device [61], [62]. The physical device can also be compromised by node capture attacks, replay attacks and sleep deprivation attacks [63], [64]. For example, the Mirai Botnet [65] attack consisted primarily of compromising embedded IoT devices and using these devices for a Distributed Denial-of-Service (DDoS) attack. There are several reasons why devices are susceptible to attacks. Internet connectivity and telepresence are the obvious enablers [66]. There are more particular problems as well like undocumented Secure Shell (SSH) and default passwords [67]. For example, Antonakakis *et al.* [65] showed that even an unsophisticated dictionary attack could compromise hundreds of thousands of internet-connected devices. Further, device authentication might not be practical for IoT security because securing routing protocols at the network layer may potentially suffer from unacceptable end-to-end delays [68]. Legacy authentication mechanisms may

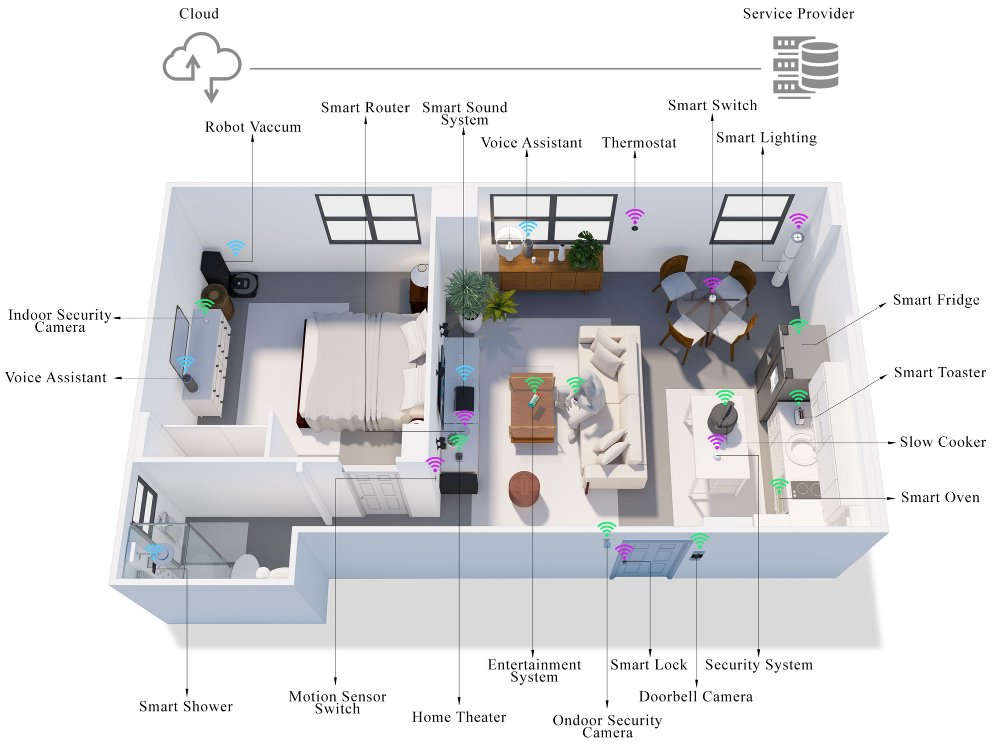

FIGURE 2. A typical smart home including many smart consumer devices and heterogenous networks.

also not be suitable IoT devices because many IoT devices are resource-constrained [69]. Astaburuaga *et al.* [70] analyzed weakness in an embedded Operating System (OS) often utilized in smart home devices and found that pairing mode feature could be easily bypassed which made the OS vulnerable to attacks such as DDoS and takeover. Some devices are also vulnerable by virtue of the hub they connect to [71].

Another common reason for device vulnerability is implicit trust and overprivileged design of the connecting Apps [72]. For example, over 55% of Apps on a popular IoT App store were overprivileged [73]. Over the air update of firmware and Apps also makes these devices vulnerable [74]. For example, Hernandez *et al.* [75] showed that firmware verification of a commonly used IoT-enabled thermostat could be bypassed, providing the means to completely change the unit's behavior. The compromised thermostat could then act as a beachhead or malicious node to attack other nodes within the local network, and any information stored within the unit was now available to the attacker who no longer needed physical access to the device. Voice is becoming a standard interface for many smart homes. Voice-spoofing has emerged as a recent threat where inaudible voice commands that cannot be understood or heard by the human, but can still be understood by the system, are injected to control the smart home [13].

Some consumer devices are borrowed, rented, gifted, resold, or retired which raises privacy violation concerns for the data stored on these devices [76]. A related issues pointed out by Özkan and Bulkan [77] is that increasingly sub-systems in modern software and devices may have been developed by an ad-hoc team that is no longer available to maintain and fix security risks. Sometimes, the company that developed a sub-system discontinues support for a product,

TABLE 2. Digital libraries used to search for papers on smart home security.

Research Quest.	Digital Library	Number of Papers
RQ1: Device Security	IEEE Xplore	652
	Science Direct	5,465
	Engineering Village	840
	ACM Digital Library	1,965
RQ2: Network Security in Smart Homes	IEEE Xplore	627
	Science Direct	6,585
	Engineering Village	1,081
	ACM Digital Library	3,021
RQ3: Cloud Security in Smart Homes	IEEE Xplore	179
	Science Direct	2,686
	Engineering Village	280
	ACM	1,454
RQ4: Application Security in Smart Homes	IEEE Xplore	136
	Science Direct	3,787
	Engineering Village	215
	ACM Digital Library	4,686

and stops issuing security updates. In a government or enterprise context, such obsolescence security risks can be handled through governance and management level mitigation policies that ensure that either such obsolete products are replaced, or the obsolete parts are isolated [77]. However, the situation is much more complex for consumer devices because even a simple consumer device may contain hardware, firmware and software from different vendors who may not adhere to the same product life-cycle governance policies. Hence, this type of obsolescence security risk remains a big challenge for consumer devices. Consumer devices with longer shelf life like televisions are particularly susceptible to this risk. One possible solution is to periodically subject such devices to rigorous security testing, and to publish the vulnerabilities to warn the consumers. Another option could be introducing legislation to ensure the that the original equipment manufacturers (OEMs) agree to provide some minimum level of extended security support for obsolete consumer devices.

Finally, consumer devices are also susceptible to a variety of attacks at the hardware level [78]. These include architectural and system threats (e.g., secure boot attacks, firmware attacks, etc.), covert and side channels attacks (e.g., timing, electromagnetic channels, etc.), intellectual property theft and counterfeiting threats, and hardware trojans.

Several countermeasures have been proposed for device security. For example, a provenance-based framework called ProvThings by Wang *et al.* [79] detected errors and malicious activates within deployment, such as weak authentication and misconfiguration. ProvThings was able to provide complete provenance for twenty-six known IoT attacks like side channel, spyware, and backdoor pin code injection. Tian *et al.* [80] proposed SmartAuth that is implemented by device vendors, where users can specify which third-party applications have permissions, and thus, obviating over privileged Apps. Santoso and Vun [81] proposed public key mutual authentication protocol for devices as a possible solution for authentication vulnerabilities. Han *et al.* [82] argued that confidentiality, access control and data integrity required a secure trustworthy smart home service in the back end as well. Meng *et al.* [13] showed that it was possible to use channel state information (CSI) to thwart voice-spoofing in a device-free manner. For hardware attacks, a variety of counter measures including true random number generators (TRNG), physical unclonable functions (PUF), system and architectural protection techniques, trusted execution environments, side channel protection techniques, and intellectual property protection techniques like hardware watermarking and steganography have been proposed [81].

2) RQ2: SMART HOME NETWORK SECURITY

Home routers have poor protection against internet-based attacks [83]. Hussain *et al.* [84] showed that various vulnerabilities like default passwords, infrequent password changes, and the absence of system updates could be reduced by accessing the home automation system using a single network. Lounis and Zulkernine [85] provided a taxonomy of attacks in Wi-Fi, Bluetooth, ZigBee, and Radio Frequency Identification (RFID) infrastructures, as well as a survey of assaults on each network technology. Their findings revealed that most attacks were caused by vulnerabilities in the authentication protocol. This is important because many smart homes utilize wireless heterogenous networks including Bluetooth Low Energy (BLE), ZigBee, Z-Wave, and Transmission Control Protocol / Internet Protocol (TCP/IP) [86]. Alrawi *et al.* [20] argued that most of the IoT devices depended on insecure protocols and that confidentiality and integrity were missing. For example, some motion sensor and home-surveillance cameras send plain text information which makes it comparatively simple for hackers to deduce when a user is at home based on the motion sensors' state [87]. Even well-known protocols like TCP/IP with Transmission Layer Security (TLS) are not entirely safe [88]. For example, Aviram *et al.* [89] presented a novel cross-protocol attack on TLS called DROWN which used a server supporting Secure Socket Layer (SSL) v2 as an oracle to decrypt modern TLS connections. Results showed that 26% of Hypertext Transfer Protocol Secure (HTTPS) servers were vulnerable to Man-in-the-Middle (MITM) attack, and that SSL was weak and damaged the TLS ecosystem. Similarly, Apthorpe *et al.* [90] examined smart home devices and showed that network traffic rate for devices revealed user activities, showing that encryption alone was not sufficient for privacy protection in smart homes. Adrian *et al.* [91] identified Logjam as a novel flaw of TLS that allows MITM to downgrade connections export grade Diffie-Hellman key exchange. Wi-Fi networks remain a key vulnerability for smart homes. For example, Godwin *et al.* [92] showed that it was challenging to break into a common voice-based home assistant using the Bluetooth protocol, but the internal Wi-Fi network could be compromised during device setup. The heterogenous nature of networks inside a home also exacerbates the situation. For example, Ho *et al.* [93] showed how it was possible to have relay attacks against Bluetooth Low Energy (BLE) protocols by serializing the BLE packets and relying on them over IP. Lounis and Zulkernine [94] discussed Bluetooth Low Energy (BLE) security and how the "Just Works" pairing option could be used to render a device inoperable. They showed a practical case study of three different Bluetooth smart gadgets. The conclusion was that people should be advised about the risk of purchasing unsecure gadgets and prioritizing convenience over security, privacy, and safety. Oren and Keromytis [95] examined network-level security weaknesses on smart televisions where a number of attacks such as DDoS, authenticated and unauthenticated request forgery, and phishing had taken place. Various types of social engineering attacks can also be used to penetrate the network security of smart homes [96]. Finally, Wood *et al.* [97] monitored home networks and disclosed multiple vulnerabilities within IoT devices highest of which was due to sharing of sensitive data.

Many approaches have been proposed for intrusion detection in smart homes. For example, Gajewski *et al.* [98] proposed a two-tier intrusion detection mechanism that used machine learning to combine anomaly detection at local level in each home combined with global anomaly detection across homes conducted by the network service provider. Likewise, deep learning approaches to detect IoT device anomalies have been proposed [99]–[102]. Similarly, Pan *et al.* [103] implemented a context aware intrusion detection framework that could accurately find and classify various kinds of Building Automation and Control Networking protocol (BacNet) attacks.

Better alternatives to TLS for resource-constrained devices have been proposed [104], [105]. Beurdouche *et al.* [106] proposed a programming approach for protocol implementation that included a systematic testing of unexpected sequences of messages. Peter and Gopal [107] introduced a multi-level smart home network authentication system that offered multiple security features. Huang *et al.* [108] proposed a security framework called SecIoT which provided important authentication and guaranteed secure communications to support authorized users with risk notification through Fifth Generation (5G) network to operate device-to-device communications at any time. Serror *et al.* [109] proposed a rule-based approach that automatically complements existing smart home network to provide protection for heterogeneous IoT devices and protocols. Apthorpe *et al.* [110] evaluated four strategies to protect the home network from threats including blocking traffic, concealing Domain Name System (DNS), and shaping traffic, and showed how traffic shaping on the home network could prevent side-channel snooping. Kim and Keum [111] provided a trusted gateway system architecture that built an IoT trust domain which could safely protect IoT devices from malicious attacks without making any changes to IP-based devices. Finally, Gill *et al.* [112] proposed a Quality of Service-aware (QoS-aware) resource management technique using fog-assisted cloud computing providing better security for smart homes.

3) RQ3: SMART HOME CLOUD SECURITY

In many instances, consumer data from a smart home device needs to be securely communicated to cloud-based back-end services [113], [114]. However, security is sometimes compromised in such transactions [115]. For example, many home surveillance cameras used cloud-based services that had issues with authentication and verification [90], [116]. Cloud-based IoT platforms are also susceptible to security flaws. For example, Surbatovich *et al.* [117] showed that some IoT recipes on a popular IoT platform could allow attackers to distribute malware and perform Denial of Service (DoS) attack. Platforms for cloud integration can also be compromised, and may expose the OAuth tokens of the user to the public. Analysis of event trigger rules in another popular open-source home automation system showed that 80% of the rules had less triggers than needed, and hence could lead to unexpected security holes that could be exploited [118].

Various countermeasures have been proposed to address cloud-based security for smart homes. For example, Alsadi and Mohan [119] proposed a method to increase secrecy rate by letting the legitimate transmitter find an alternative route to the fusion center in case of an eavesdropper located in between the information passed. Similarly, Tao *et al.* [120] proposed a new multi-layer architectural cloud model to enable efficient and seamless interactions on heterogeneous devices/services provided by various IoT-based smart home vendors. Another way to empower IoT users who trust their private data to the vendors is Transport Layer Security-Rotate and Release (TLS-RaR) that can be jointly deployed by vendors and users or trusted third parties. Device vendor can also mitigate their exposure by diversifying and subscribing to different cloud providers [121].

Finally, Fernandes *et al.* [122] proposed using a decentralized framework for trigger-action programmable platforms called Decentralized Trigger-Action Platform (DTAP) that acts as a shim between the IoT cloud platform and the users' local network. In this scenario, broker access to IoT devices was based on transfer tokens (XTokens) where attackers could not misuse the tokens.

4) RQ4: SMART HOME APPLICATION SECURITY

Hu *et al.* [125] examined mechanisms for testing the security of third-party Apps for smart home assistants. Mobile Apps used to configure or access smart home devices provide a convenient attack surface [124]. It is difficult to maintain security at the application layer because of lack of sufficient protocol security services, incorrect configuration, and resource limitations [125]. For example, Liu *et al.* [126] showed that it was possible to emulate a commercial edge device using software and then fooling the associated mobile App to uncover home Wi-Fi passphrases, and to trap the user into disclosing personal information. Similarly, Margulies [127] argued that linking garage door openers to the internet network using mobile Apps might easily pose a security threat. Fernandes *et al.* [128] found that many IoT programming frameworks only support permission-based access control on sensitive data, and hence making it possible for malicious Apps to abuse the permissions and to leak data. Sivaraman *et al.* [83] demonstrated a smart phone attack on a home network using a doctored smart phone App by scouting for vulnerable IoT devices within the home and then reporting them back to an external entity where they modify the firewall to allow the external entity to directly attack IoT devices. Demetriou *et al.* [129] proposed HanGuard that allowed the router to enforce access control policies to home area network using mobile phones and IoT devices. Chen *et al.* [130] suggested that to ensure proper deployment, IoT vendors and developers should follow platform development guidelines and leverage the in-built security features. Finally, Yamauchi *et al.* [131] proposed a unique intrusion detection mechanism that used Hidden Markov Machines (HMM) to learn the behavior of homeowners. App commands that were not congruent with this behavior were marked as anomalies.

TABLE 3. Common vulnerabilities of smart homes.

Security Question	Common Vulnerabilities
RQ1: Device	Eavesdropping [63-64] Node capture and replay attacks [63] Sleep deprivation attack [64] DDoS attack [65] Internet pairing default password [67] Configuration and device authentication [68], [81] Legacy authentication mechanism [69] Exposed services [72] Overprivileged configuration Apps [73], [80] Insecure hardware interfaces [70] OTA Updates and upgradeability weakness [74-75] Critical vulnerabilities: side channel, spyware, and backdoor pin code injection [79] Voice spoofing [13] Communal acts like renting, lending, etc. [76] Hardware-level attacks [78] COTS obsolescence risk [77]
RQ2: Network	Authentication and communication [83], [85] Default password [81-82] Insecure protocols [20], [87] Susceptibility to MITM attack [84-85], [91] Inappropriate use of encryption [90] Protocol attacks [92], [103] Relay attack [93] Sensitive data [97] Prospective attacks [95-96] Social engineering [96]
RQ3: Cloud	Information disclosure and access control [113-114] Authentication and verification [116], [90] Exploitable services [109-110] Eavesdropping [119]
RQ4: Application	Incorrect configuration and resource limitations [125] Leakage of sensitive Data [126] Excess permissions [128] Programming issues [83] Weak password protection [127]

Table 3 shows the key security vulnerabilities for each research question posed in the survey. Table 3 suggests that each component of a smart home device viewed from the IoT lens leads to related but potentially different set of vulnerabilities.

III. AHP METHODOLOGY FOR SMART HOME DEVICE SECURITY

The previous section showed that a variety of task-specific criteria have been used to build AHP hierarchies to assess security in various computer-related domains. In most cases, the generic security criteria of confidentiality, integrity, authentication, availability, etc were used at the top-level in developing these AHP hierarchies. A second common characteristic of most pervious work discussed in the last section was a reliance on expert judgement when comparing alternatives. The previous section also showed that a large number of security vulnerabilities at various levels (e.g., device, network, etc.) have been identified in the literature, and that new vulnerabilities continue to emerge and hence represent a moving target.

The AHP methodology proposed in this paper removes the subjective component of the expert judgements used in previous work by systematically using the extensive literature review on computer security presented earlier in conjunction with current empirical security studies of consumer devices. Hence the proposed methodology relies on the latest empirical data mediated by the collective judgement of experts represented in the research literature as opposed to using individual expert opinions. Further, unlike most previous work, the top-level criteria of the AHP hierarchy in the proposed methodology are not based on generic security concepts, but on the dimensions used by a specific empirical study. Combining literature review systematically with data derived from empirical studies to automatically conduct AHP analysis is unique has not been done before to our knowledge.

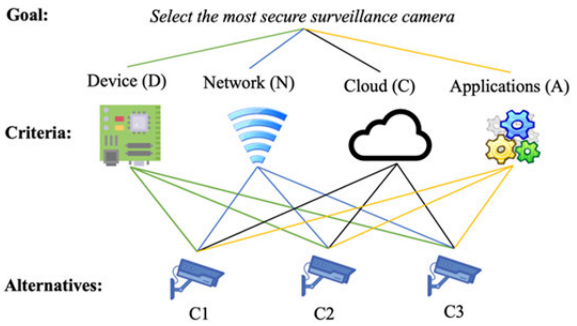

FIGURE 3. A simplified AHP model for selecting the most secure surveillance camera.

This section proposes a novel methodology for applying AHP to create smart home device security rankings. A simplified example of how AHP can be used to rank device security using the IoT lens with the four top-level criteria of device, network, cloud and application security is presented first. The simplified example shows in detail all the steps and the calculations required for each step of the generic AHP methodology. The example is followed by a description of the proposed methodology for applying AHP for smart home security domain. The proposed methodology is then demonstrated by using an existing empirical study, and all the steps and calculations are subsequently described in detail.

A. A SIMPLE EXAMPLE OF APPLYING AHP

This section presents as simple example of using an AHP based on device, network, cloud, and application security criteria. Lower-level sub-criteria are excluded for simplicity.

The first step in AHP is to build a decision hierarchy like the one shown in FIGURE 3. This hierarchy assumes that AHP has the goal of selecting the most secure surveillance camera. This goal can be achieved by evaluating each candidate camera with respect to Device (D), Network (N), Cloud (C) and Application (A) security. The model in FIGURE 3 shows that three alternative camera models (C1-C3) are to be compared.

The second step in applying AHP is to determine the priority or importance of each criterion (e.g., Network Security) in achieving the said goal. This is done by first constructing a pairwise comparison matrix A^G for the four criteria.

The matrix A^G encodes the relative importance of these criteria towards achieving the goal. This example uses arbitrary pairwise comparison numbers. Equation (1) shows an example matrix A^G where each $a_{ij} \in$A^G represents a symmetric pairwise comparison of importance between the i_{th} and j_{th} criterion based on the AHP fundamental scale [26]. For example, $a_{14} = 9$ in (1) shows the assumption that Device (D) security is much more important than the Application (A) security in determining the security of a surveillance camera.

$$\boldsymbol{A^G} = \begin{array}{c} \begin{array}{cccc} D & N & C & A \end{array} \\ \begin{pmatrix} 1 & 1 & 3 & 9 \\ 1 & 1 & 1 & 3 \\ \frac{1}{3} & 1 & 1 & 5 \\ \frac{1}{3} & \frac{1}{9} & \frac{1}{5} & 1 \end{pmatrix} \end{array} \tag{1}$$

w^G is a vector representing the relative priority of each criterion with respect to the top goal and is calculated by solving a system of equations given in (2) and (3) for any pairwise comparison matrix A and priority vector w [26]

$$A\boldsymbol{w} = \lambda_{max}\boldsymbol{w} \tag{2}$$

$$\boldsymbol{w^T 1} = 1 \tag{3}$$

λ_{max} is the maximum eigenvalue of A, and $\boldsymbol{1} = (1 \ldots 1)$T. w^G calculated using (2) and (3) in (4) shows that according to A^G, Device has the highest priority for achieving the goal of determining the most secure camera (i.e., $w_D^G = 0.455$).

$$\boldsymbol{w^G} = \begin{pmatrix} w_D^G \\ w_N^G \\ w_C^G \\ w_A^G \end{pmatrix} = \begin{pmatrix} 0.455 \\ 0.266 \\ 0.221 \\ 0.058 \end{pmatrix} \tag{4}$$

The internal consistency of an $n \times n$ pairwise comparison matrix A is given by (5) where RI_n is empirically determined for each n. Matrices with $CR(A) < 0.1$ are acceptable while those with $CR(A) > 0.1$ are rejected as being inconsistent [26].

$$CR\,(A) = \frac{\lambda_{max} - n}{(n-1) \times RI_n} \tag{5}$$

$CR\left(A^G\right) = 0.069(n = 4)$ which means that pairwise comparisons in matrix A^G are internally consistent.

Once the relative priority of each criterion (e.g., Network) with respect to the goal is determined, the same process is repeated for each criterion by creating a pairwise comparison matrix for each criterion (e.g., Network) with respect to each alternative. For example, A^D in (6) shows the pairwise comparison of each of the three camera alternatives with respect to Device (D) security criterion. For example, (6) shows that with respect to device security, camera C1 is less secure than camera C2 ($a_{12} = 0.5$), and more secure than camera C3 ($a_{13} = 3$).

$$\boldsymbol{A^D} = \begin{array}{c} \begin{array}{ccc} C1 & C2 & C3 \end{array} \\ \begin{pmatrix} 1 & \frac{1}{2} & 3 \\ 2 & 1 & 3 \\ \frac{1}{3} & \frac{1}{3} & 1 \end{pmatrix} \end{array} \tag{6}$$

w^D in (7) shows that overall priority vector for A^D calculated using (2) and (3). Equation (7) shows that camera C2 was the most preferred with respect to device security ($w_{C2}^D = 0.528$).

$$\boldsymbol{w^D} = \begin{pmatrix} w_{C1}^D \\ w_{C2}^D \\ w_{C3}^D \end{pmatrix} = \begin{pmatrix} 0.333 \\ 0.528 \\ 0.140 \end{pmatrix} \tag{7}$$

Finally, goal level priority and the criteria level priority vectors can be combined into a single priority vector $\boldsymbol{w^{cameras}}$ using (8) [26].

$$\boldsymbol{w^{cameras}} = w_D^G\boldsymbol{w^D} + w_N^G\boldsymbol{w^N} + w_C^G\boldsymbol{w^C} + w_A^G\boldsymbol{w^A} \tag{8}$$

where $\boldsymbol{w^N}$, $\boldsymbol{w^C}$, $\boldsymbol{w^A}$ represent the priority vectors with respect to Networking, Cloud and Application layers respectively calculated in a similar fashion as w^D.

$\boldsymbol{w^{cameras}}$ in (9) shows the relative priority of each camera alternative calculated using (8).

$$\boldsymbol{w^{cameras}} = \begin{pmatrix} w_{C1} \\ w_{C2} \\ w_{C3} \end{pmatrix} = \begin{pmatrix} 0.242 \\ 0.469 \\ 0.289 \end{pmatrix} \tag{9}$$

Equation (9) shows that $\boldsymbol{w_{C1} w_{C3} w_{C2}}$ which means that in this example, camera C2 was the best overall choice for a surveillance camera.

B. PROPOSED AHP METHODOLOGY

A methodology of conducting the pairwise comparisons for each level of the AHP model is described next.

1) TOP-LEVEL PAIRWISE COMPARISON

At the top-level, relative importance of various security criteria like Device Security versus Network Security must be determined. The methodology proposed a pairwise comparison scheme based on the literature review for smart home security. Specifically, the number of words discussing issues related to each security criteria were counted for each paper and used as a proxy for relative importance of each security criterion.

Table 4 shows an example of how a normalized percentage with respect to each paper's total word count was derived. Each Security column in Table 4 represents the overall importance of each criterion for four sample papers.

An effect size using Rank biserial correlation (r) [133] was used to then calculate the magnitude of difference between

TABLE 4. Sample of systematic review results.

Paper	Word Count	Device Security	Network Security	Cloud Security	Applic. Security
Noor *et al.* [68]	10,809	0%	23%	0%	0%
Alrawi *et al.* [20]	17,465	7%	9%	7%	5%
Liu *et al.* [10]	5,810	0%	20%	0%	16%
Mohammad *et al.* [61]	5,071	4%	13%	0%	4%

TABLE 5. Top level pairwise comparison matrix for top-level comparision.

Security Criteria	Value	Device	Network	Cloud	Application
	r		0.28	-0.17	-0.20
Device	$\hat{r}$	1	0.57	-0.34	-0.41
	ahp_scale		**1/6**	**4**	**4**
	r	-0.28		-0.44	-0.49
Network	$\hat{r}$	-0.57	1	-0.88	-1.00
	ahp_scale	**6**		**8**	**9**
	r	0.17	0.44		-0.03
Cloud	$\hat{r}$	0.34	0.88	1	-0.06
	ahp_scale	**1/4**	**1/8**		**1**
	r	0.20	0.49	0.03	
Application	$\hat{r}$	0.41	1.00	0.06	1
	ahp_scale	**1/4**	**1/9**	**1**	

the compared pairs (e.g., Device vs. Network Security column in Table 4). The effect size value (r) was then mapped to the AHP scale [26] by using (10) and (11).

$$\hat{r} = \frac{r}{max\left(max\left(r\right) - min\left(r\right)\right)} \tag{10}$$

$$ahp\_scale = 8\times\left(\hat{r}\right) + 1 \tag{11}$$

Table 5 shows the resulting pairwise comparisons among the various security criteria based on all the papers reviewed earlier. For example, Table 5 shows that Device security was much less important than Network security (ahp_scale =1/6) and much more important than Cloud or Application security (ahp_scale = 4).

2) LOWER-LEVEL PAIRWISE COMPARISON SCHEME

A second key contribution of this paper is the idea of using empirical data on security assessment of home devices for the low-level AHP comparisons. Empirical security assessment data from a security study conducted by Alrawi *et al.* [20] was used in this paper. Like most such studies, this study also used pragmatic lower-level criteria for each of the device, network, cloud and application-level security. For example, device security criteria contained the sub-criteria of internet pairing, configuration, upgradability, exposed services, and Common Vulnerability Scoring System (CVSS) [132]. This is different than the general dimensions of security like confidentiality, integrity, etc. being used by many AHP studies in the past as shown in FIGURE 1. Data published by Alrawi *et al.* [134] based on this study was used to automatically generate pairwise comparisons for the lower level. Since the original study used a ratio scale to represent relative security risk, the ratio scale was first converted to an ordinal scale for AHP. For example, the overall security risk for Application security in the original study was 16. For one consumer device model (e.g., camera model C1), the security risk due to 'sensitive data' with respect to Application security was (7/16), while security risk due to 'programming issues' with respect to Application security was (5/16). This meant that for camera model C1, 'programming issues' was less of a security risk with respect to Application security. Given each such ratio (a/b), (12) was first used to calculate the angle of the vector < a, b > in radians for each reviewed device.

TABLE 6. An example of application security pairwise comparison.

Security Factor	Value	Sensitive Data	Program. Issues	Excess Permissions
	$\Delta\theta$		-0.11	-0.17
Sensitive Data	$\Delta\hat{\theta}$	1	-0.65	-1
	ahp_scale		6	9
	$\Delta\theta$	0.11		-0.06
Program. Issues	$\Delta\hat{\theta}$	0.65	1	-0.35
	ahp_scale	1/6		4
	$\Delta\theta$	0.17	0.06	
Excess Permissions	$\Delta\hat{\theta}$	1	0.35	1
	ahp_scale	1/9	1/4	

$$\theta = cos^{-1}\left(\frac{a}{\sqrt{a^2 + b^2}}\right) \tag{12}$$

All reviewed devices of a particular type (e.g., security cameras) were then compared in pairs by taking the difference between their respective θs calculated using (12) and subsequently using (13) and (14) to map the difference of $\theta's$ to the AHP scale.

$$\Delta\hat{\theta} = \frac{\Delta\theta}{max\left(max\left(\Delta\theta\right) - min\left(\Delta\theta\right)\right)} \tag{13}$$

$$ahp\_scale = 8\times\left(\Delta\hat{\theta}\right) + 1 \tag{14}$$

Table 6 shows an example of the pairwise comparison matrix for Application security which depends on Sensitive Data, Programming Issues and Excess Permissions.

IV. CASE STUDY

Using the methodology described in the previous section, an AHP analysis was conducted using the pairwise comparison matrices as shown in the previous section. A total of 41 devices (e.g., Alexa) within 11 device types including home theatres, security cameras, smart lighting, smart speakers, video surveillance, smart switches, home automation systems, home security systems, smart routers, wireless doorbell cameras, and home audio systems were considered based on security assessment data published by Alrawi *et. al* [134].

A. THE AHP MODEL

FIGURE 4 shows the resulting AHP model based on applying the proposed methodology. The calculated priority or relative weight of each security criterion is shown in parentheses.

As FIGURE 4 shows, at the top level, Network security had the highest priority (0.6893) which implies that network

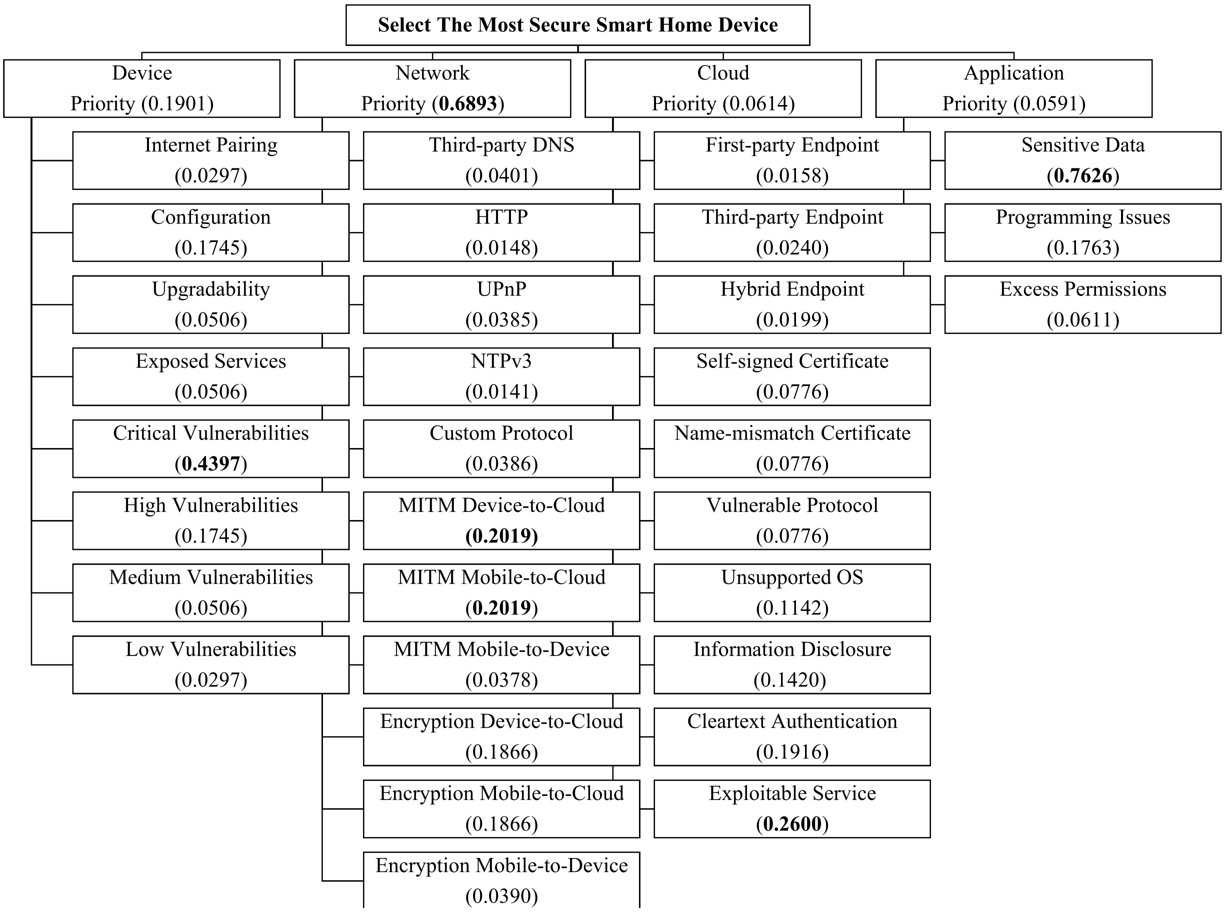
Select The Most Secure Smart Home Device
Device Priority (0.1901)
Network Priority (**0.6893**)
Cloud Priority (0.0614)
Application Priority (0.0591)
Internet Pairing (0.0297)
Configuration (0.1745)
Upgradability (0.0506)
Exposed Services (0.0506)
Critical Vulnerabilities (**0.4397**)
High Vulnerabilities (0.1745)
Medium Vulnerabilities (0.0506)
Low Vulnerabilities (0.0297)
Third-party DNS (0.0401)
HTTP (0.0148)
UPnP (0.0385)
NTPv3 (0.0141)
Custom Protocol (0.0386)
MITM Device-to-Cloud (**0.2019**)
MITM Mobile-to-Cloud (**0.2019**)
MITM Mobile-to-Device (0.0378)
Encryption Device-to-Cloud (0.1866)
Encryption Mobile-to-Cloud (0.1866)
Encryption Mobile-to-Device (0.0390)
First-party Endpoint (0.0158)
Third-party Endpoint (0.0240)
Hybrid Endpoint (0.0199)
Self-signed Certificate (0.0776)
Name-mismatch Certificate (0.0776)
Vulnerable Protocol (0.0776)
Unsupported OS (0.1142)
Information Disclosure (0.1420)
Cleartext Authentication (0.1916)
Exploitable Service (**0.2600**)
Sensitive Data (**0.7626**)
Programming Issues (0.1763)
Excess Permissions (0.0611)

FIGURE 4. A graphical representation of the AHP assessment model and priorities assigned to each criterion.

security was by far the most important security criteria for smart home devices. Application (0.059) and Cloud securities (0.0614) each had much lower priority. At the lower level, for Device security, predictably, 'critical vulnerabilities' had the highest priority of 0.4397. Second position was tied between high vulnerabilities and configuration with a priority of 0.1745. Internet pairing, and low vulnerabilities were the least important with a priority of 0.0297 each. Similarly, for Network security, two types of MITM attacks had the highest priority of 0.201. Interestingly, Mobile-to-Device MITM had a low priority of 0.0378. For Cloud security, exploitable services had the highest priority of 0.260. Finally, for Application security, sensitive data had the highest priority of 0.7626, while the least important was excess permissions with a priority of 0.0611.

B. INTERNAL VALIDATION

1) CONSISTENCY RATIOS

It should be emphasized that in this paper, the pairwise comparisons were based on quantitative measures taken directly from a combination of a literature review and on data from an empirical security assessment study. Therefore, it was important to ensure that these automatically derived pairwise comparisons were mathematically consistent. In AHP, internal consistency of judgments of pairwise comparisons is measured by the Consistency Ratio (*CR*) [135]. The pairwise comparisons are considered unreliable if the *CR* value is higher than 0.1 and must be revisited [136].

The consistency ratios for all top-level comparisons for the AHP model were mostly within bounds ($CR<0.1$). The only exception was Application security where the *CR* value was a bit higher than 0.1 ($CR=0.1037$) which is acceptable. Mean *CR* values for all device types (e.g., surveillance cameras) were well within bounds with the highest mean being 0.0140 for the video surveillance equipment. In more than 50% of the cases, the median *CR* values were zero, and the standard deviations were small. In summary, it is reasonable to assume that the model was internally consistent at all levels of comparisons.

2) SENSITIVITY ANALYSIS

The goal of sensitivity analysis was to determine how sensitive the ranking outcomes were to the pairwise comparisons. Sensitivity analysis was conducted by varying top-level priorities 10% above and below their respective values and determining the impact on the relative ranking of various devices.

TABLE 7. A sample scorecard rank for video surveillance equipment.

Video S. Device	Original Work: Scorecard Percentage Score [134]			
	Device	Network	Cloud	Application
VSD1	86%	57%	52%	85%
VSD2	93%	96%	84%	54%
VSD3	62%	71%	88%	69%
VSD4	95%	93%	63%	69%

Most devices with the topmost ranking within each device type were not sensitive to priority changes. Priority thresholds of 0.01 and 0.05 were used to determine if the rank changed for each device type. For example, if the priority of two alternative devices differed by more than 1% (threshold=0.01), then the rank was considered different based on a threshold of 0.01. For the threshold of 0.05, top rankings changed only twice across all 11 device types. Similarly, for a threshold of 0.01, the ranking changed for 4 device types only. This suggests that although the AHP model was sensitive to some device types, overall, the model was robust with respect to the pairwise comparisons.

3) COMPARISON WITH ORIGINAL SECURITY SCORES

It is instructive to compare the security ranks given to each consumer device with those from the original security scorecards from Alrawi *et. al* [134]. Table 7 shows an example of original scorecard percentage scores for four video surveillance devices; higher percentages meant better security. For example, Video Surveillance Device 1 (VSD1) was most secure with respect to Device security (86%) as opposed to Network, Cloud or Application security. It is clear from Table 7 that while useful for a researcher, a typical consumer cannot directly interpret this information to determine which device is the most secure. For example, from Table 7, it is not clear whether Video Surveillance Device 2 (VSD2) was better than Video Surveillance Device 4 (VSD4). This is because both devices were similar with respect to Device (93% and 95% respectively) and Network (96% and 93% respectively) security. However, VSD2 was better in Cloud security (84% vs. 63%) while VSD4 was better in Application security (69% vs. 54%). It is not possible for a typical consumer to decide which of the Application or Cloud security is more important for video surveillance devices in making this decision. What the consumers require is a simple ranking as proposed in this paper.

To facilitate a comparison with our approach, percentage scores of the type shown in Table 7 were first normalized using the SoftMax [137] function shown in (15).

$$score_{dl} = \frac{e^{a_{dl}}}{\sum_{i=1}^{n} e^{a_{il}}} \tag{15}$$

In (15), $score_{dl}$ represents the normalized score of a device d (e.g., VSD1) with respect to security criteria l (e.g., Device)and n is the number of alternative devices in the group. The original percentage score as shown in Table 7 is represented by a_{dl} (e.g., $a_{VSD1-Network} = 57\%$). For a particular criterion l (e.g., Network), the normalized scores add up to 1 for the n device alternatives. By definition, $score_{dl} \leq 1$ because each device has four such scores, one for each security criterion, (16) was used to calculate the overall rank for each alternative device where i represents each security criterion (e.g., Cloud).

$$rank(d) = \frac{\sum_{i=1}^{4} score_{di}}{4} \tag{16}$$

Levenshtein or Edit distance [138] was subsequently used to calculate the distance between the ranks derived from the original score cards and the proposed AHP model. Edit distance of zero means that ranks are the same. For example, the ranks of five smart lights (L1-L5) using the original scorecard [134] were $L1 \preceq L2 \preceq L3 \preceq L4 \preceq L5$ (i.e., $L5$ was the most secure) while the AHP model's ranks were $L1 \preceq L3 \preceq L2 \preceq L5 \preceq L4$ (i.e., $L4$ was the most secure), showing that the ranks were different because the edit distance between the two ranks was 4.

Overall, the ranks based on the proposed AHP approach were significantly different than the original scorecard ranks with a total Levenshtein distance of 20 across all device types. Since the lower-level empirical data was common for both the scorecard and the proposed AHP model, this discrepancy between the two approaches can perhaps be explained by the fact that the original scorecard did not explicitly incorporate any top-level assumptions. This speaks to the importance of the more holistic view of the AHP model for a more informed decision.

V. CONCLUSION AND LIMITATIONS

This paper presented a systematic survey, a methodology and a case study to rank the security of home consumer devices. An IoT lens based on the current state-of-the-art research in security of smart home devices was used to propose a novel methodology. The proposed methodology was then used and evaluated in the context of one empirical security assessment study. The key contribution of the methodology is systematically combining the current wisdom behind smart home device security research with empirical on the ground results from security vulnerability studies. The case study showed that even though the AHP model was based on empirical data, remarkably, the resulting AHP model was internally consistent and robust with respect to pairing assumptions and sensitivity analysis. The derived AHP model also showed the importance of various security factors in current home consumer devices in an explicit and quantitative manner. In addition to ranking consumer devices, the AHP model can also be used to inform future research because it incorporates empirical security studies as well. For example, under network security, Third Party DNS and MITM Device-to-Cloud were found to be most significant from a security perspective, and therefore, more research could be directed towards determining and deploying counter measures for these two vulnerabilities.

Although the proposed methodology and approach is general, the proposed methodology has only been applied to one empirical security assessment study. However, the methodology can be easily adapted to any of the many vulnerability assessment studies being conducted today. In addition, as the research focus on smart home device security changes, the current top-level priorities may change as well. For example, network may no longer be the primary weak point in the future. In this case, the proposed methodology can be used to simply recalculate the priorities. Finally, it would also be interesting to compare these device rankings with those based on an AHP built using expert opinions. However, the advantage of the proposed methodology over an expert-based approach is that the methodology can be mostly automated and applied whenever the underlying information changes.

ACKNOWLEDGMENT

This paper represents the opinions of the authors and does not mean to represent the position or opinions of the American University of Sharjah.

REFERENCES

[1] M. Inoue, K. Uemura, Y. Minagawa, M. Esaki, and Y. Honda, "A home automation system," *IEEE Trans. Consum. Electron.*, vol. CE-31, no. 3, pp. 516–527, Aug. 1985, doi: 10.1109/TCE.1985.289966.

[2] D. Kumar. *All Things Considered: An Analysis of IoT Devices on Home Networks*. Accessed: Oct. 1, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-deepak

[3] D. Pishva and K. Takeda, "A product based security model for smart home appliances," in *Proc. 40th Annu. Int. Carnahan Conf. Secur. Technol.*, Lexington, KY, USA, 2006, pp. 234–242, doi: 10.1109/CCST.2006.313456.

[4] C. Lee, L. Zappaterra, K. Choi, and H. A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Proc. Conf. Commun. Netw. Secur.*, 2014, pp. 67–72, doi: 10.1109/CNS.2014.6997467.

[5] (2019). *Avast Smart Home Report 2019*. Accessed: Jan. 15, 2022. [Online]. Available: https://press.avast.com/press-kits/avast-smart-home-report-2019

[6] R. Williams, E. McMahon, S. Samtani, M. Patton, and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Beijing, China, Jul. 2017, pp. 179–181, doi: 10.1109/ISI.2017.8004904.

[7] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerging household appliances," in *Proc. IEEE Conf. Commu. Netw. Secur.*, San Francisco, CA, USA, Oct. 2014, pp. 79–84, doi: 10.1109/CNS.2014.6997469.

[8] Z. Ling, J. Luo, Y. Xu, C. Gao, K. Wu, and X. Fu, "Security vulnerabilities of Internet of Things: A case study of the smart plug system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1899–1909, Dec. 2017, doi: 10.1109/JIOT.2017.2707465.

[9] Z. Celik, E. Fernandes, E. Pauley, and G. Tan, "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–30, 2019, doi: 10.1145/3333501.

[10] H. Liu, C. Li, X. Jin, J. Li, Y. Zhang, and D. Gu, "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices," in *Proc. Workshop Internet Things Secur. Privacy*, New York, NY, USA, Nov. 2017, pp. 13–18, doi: 10.1145/3139937.3139948.

[11] S. Mare, L. Girvin, F. Roesner, and T. Kohno, "Consumer smart homes: Where we are and where we need to go," in *Proc. 20th Int. Workshop Mobile Compu, Sys. Appl.*, Santa Cruz, CA, USA, Feb. 2019, pp. 117–122, doi: 10.1145/3301293.3302371.

[12] J. M. Batalla, A. Vasilakos, and M. Gajewski, "Secure smart homes: Opportunities and challenges," *ACM Comput. Surv.*, vol. 50, no. 5, pp. 1–32, 2017, doi: 10.1145/3122816.

[13] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 53–59, Dec. 2018, doi: 10.1109/MWC.2017.1800100.

[14] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017, doi: 10.1109/COMST.2017.2720195.

[15] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1933–1954, 4th Quart., 2014, doi: 10.1109/COMST.2014.2320093.

[16] S. D. Johnson, J. M. Blythe, M. Manning, and G. T. W. Wong, "The impact of IoT security labelling on consumer product choice and willingness to pay," *PLoS ONE*, vol. 15, no. 1, pp. 33–48, Jan. 2020, doi: 10.1371/journal.pone.0227800.

[17] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," in *Proc. ACM Hum. Comput. Interact.*, vol. 2, pp. 1–20, Nov. 2018, doi: 10.1145/3274469.

[18] P. Emami-Naeini, Y. Agarwal, L. F. Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?" in *Proc. IEEE Symp. Secur. Priv. (SP)*, San Francisco, CA, USA, May 2020, pp. 447–464, doi: 10.1109/SP40000.2020.00043.

[19] J. M. Blythe and S. D. Johnson, "The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices," in *Proc. Living Internet Things, Cybersecurity*, London, U.K., 2018, pp. 4–7, doi: 10.1049/cp.2018.0004.

[20] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. IEEE Symp. Secur. Priv.*, vol. 1, San Francisco, CA, USA, May 20-22, 2019, pp. 1362–1380, doi: 10.1109/SP.2019.00013.

[21] A. Mardani, A. Jusoh, K. MD Nor, Z. Khalifah, N. Zakwan, and A. Valipour, "Multiple criteria decision-making techniques and their applications—A review of the literature from 2000 to 2014," *Econ. Res. Ekonomska Istraivanja*, vol. 28, no. 1, pp. 516–571, Jan. 2015, doi: 10.1080/1331677X.2015.1075139.

[22] T. L. Saaty, "Decision making with the analytic hierarchy process," *Int. J. Serv. Sci.*, vol. 1, no. 1, pp. 1–16, 2008. [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJSSCI.2008.017590, doi: 10.1504/IJSSCI.2008.017590.

[23] T. L. Saaty and L. G. Vargas, "How to make a decision," in *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. Boston, MA, USA: Springer, 2012, pp. 1–21.

[24] I. Syamsuddin and J. Hwang, "The application of AHP model to guide decision makers: A case study of E-banking security," in *Proc. 4th Int. Conf. Comput. Sci. Converg. Inf. Technol.*, Nov. 2009, pp. 1469–1473, doi: 10.1109/ICCIT.2009.251.

[25] D. Maáek, I. Magdaleni, and N. Reáep, "A systematic literature review on the application of multicriteria decision making methods for information security risk assessment," *Int. J. Saf. Secur. Eng.*, vol. 10, no. 2, pp. 161–174, Apr. 2020, doi: 10.18280/ijsse.100202.

[26] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Mater. Today, Proc.*, Jun. 2021. [Online]. Available: https://www-sciencedirect-com.aus.idm.oclc.org/science/article/pii/S2214785321046009?via%3Dihub, doi: 10.1016/j.matpr.2021.06.228.

[27] X. Zhao, H. Xu, T. Wang, X. Jiang, and J. Zhao, "Research on multidimensional system security assessment based on AHP and gray correlation," in *Proc. Trusted Comput. Inf. Secur.*, Singapore, 2020, pp. 177–192, doi: 10.1007/978-981-15-3418-8_13.

[28] F. H. Sohime, R. Ramli, F. A. Rahim, and A. A. Bakar, "Exploration study of skillsets needed in cyber security field," in *Proc. 8th Int. Conf. Inf. Technol. Multimedia (ICIMU)*, Aug. 2020, pp. 68–72, doi: 10.1109/ICIMU49871.2020.9243448.

[29] J. Zaburko and J. Szuláyk-Cieplak, "Information security risk assessment using the AHP method," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 710, no. 1, Dec. 2019, Art. no. 012036, doi: 10.1088/1757-899X/710/1/012036.

[30] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Commun. ACM*, vol. 48, no. 2, pp. 78–83, Feb. 2005, doi: 10.1145/1042091.1042094.

[31] H. Wang, Z. Sun, H. Wang, and Z. Sun, "Research on multi decision making security performance of IoT identity resolution server based on AHP," *Math. Biosci. Eng.*, vol. 18, no. 4, pp. 3977–3992, 2021, doi: 10.3934/mbe.2021199.

[32] S. Siboni, C. Glezer, R. Puzis, A. Shabtai, and Y. Elovici, "Security ranking of IoT devices using an AHP model," in *Cyber Security Cryptography and Machine Learning*. Cham, Switzerland: Springer, 2020, pp. 29–44, doi: 10.1007/978-3-030-49785-9_3.

[33] R. Verma and S. Chandra, "A fuzzy AHP approach for ranking security attributes in fog-IoT environment," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–5, doi: 10.1109/ICCCNT49239.2020.9225513.

[34] S. O. Ogundoyin and I. A. Kamil, "A fuzzy-AHP based prioritization of trust criteria in fog computing services," *Appl. Soft Comput.*, vol. 97, Dec. 2020, Art. no. 106789, doi: 10.1016/j.asoc.2020.106789.

[35] L. Wang, Y. Ali, S. Nazir, and M. Niazi, "ISA evaluation framework for security of Internet of Health Things system using AHP-TOPSIS methods," *IEEE Access*, vol. 8, pp. 152316–152332, 2020, doi: 10.1109/ACCESS.2020.3017221.

[36] C.-C. Hsu and B. Sandford, "The Delphi technique: Making sense of consensus," *Practical Assessment, Res., Eval.*, vol. 12, no. 1, p. 10, 2007, doi: 10.7275/PDZ9-TH90.

[37] P. T. M. Ly, W.-H. Lai, C.-W. Hsu, and F.-Y. Shih, "Fuzzy AHP analysis of Internet of Things (IoT) in enterprises," *Technol. Forecasting Social Change*, vol. 136, pp. 1–13, Nov. 2018, doi: 10.1016/j.techfore.2018.08.016.

[38] B. Zhang, Z. Zou, and M. Liu, "Evaluation on security system of Internet of Things based on Fuzzy-AHP method," in *Proc. Int. Conf. E-Bus. E-Government (ICEE)*, Shanghai, China, May 2011, pp. 1–5, doi: 10.1109/ICEBEG.2011.5881939.

[39] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, pp. 50944–50957, 2020, doi: 10.1109/ACCESS.2020.2970245.

[40] A. Agrawal, M. Alenezi, R. Kumar, and R. A. Khan, "Measuring the sustainable-security of web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019, doi: 10.1109/ACCESS.2019.2946776.

[41] Z. Lai, Y. Shen, and G. Zhang, "A security risk assessment method of website based on threat analysis combined with AHP and entropy weight," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2016, pp. 481–484, doi: 10.1109/ICSESS.2016.7883113.

[42] A. Alharbi, W. Alosaimi, and H. Alyami, "Managing software security risks through an integrated computational method," *Intell. Autom. Soft Comput.*, vol. 28, pp. 179–194, Mar. 2021, doi: 10.32604/iasc.2021.016646.

[43] R. Kumar, A. Baz, and H. Alhakami, "A hybrid model of hesitant fuzzy decision-making analysis for estimating usable-security of software," *IEEE Access*, vol. 8, pp. 72694–72712, 2020, doi: 10.1109/ACCESS.2020.2987941.

[44] Y. S. Kim, M. K. Choi, S. M. Han, C. Lee, and P. H. Seong, "Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP," *Ann. Nucl. Energy*, vol. 149, Dec. 2020, Art. no. 107790, doi: 10.1016/j.anucene.2020.107790.

[45] K. Phudphad, B. Watanapa, W. Krathu, and S. Funilkul, "Rankings of the security factors of human resources information system (HRIS) influencing the open climate of work: Using analytic hierarchy process (AHP)," *Proc. Comput. Sci.*, vol. 111, pp. 287–293, Oct. 2017, doi: 10.1016/j.procs.2017.06.065.

[46] Y. Zhang, X. Deng, D. Wei, and Y. Deng, "Assessment of E-commerce security using AHP and evidential reasoning," *Expert Syst. Appl.*, vol. 39, no. 3, pp. 3611–3623, Feb. 2012, doi: 10.1016/j.eswa.2011.09.051.

[47] M. Tariq, S. Ahmed, N. Memon, and S. Tayyaba, "Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks," *Sensors*, vol. 20, no. 5, Jan. 2020, Art. no. 5, doi: 10.3390/s20051310.

[48] Z. Ruo-xin, X. Cui, S. Gong, H. Ren, and K. Chen, "Model for cloud computing security assessment based on AHP and FCE," in *Proc. 9th Int. Conf. Comput. Sci. Educ.*, Aug. 2014, pp. 197–204, doi: 10.1109/ICCSE.2014.6926454.

[49] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-based quantitative approach for assessing and comparing cloud security," in *Proc. IEEE 13th Int. Conf. Trust, Secur. Priv. Comput. Commun.*, Sep. 2014, pp. 284–291, doi: 10.1109/TrustCom.2014.39.

[50] J. Li, L. Yan, J. Wang, and T. Fu, "Research on network security risk assessment method based on improved AHP," *J. Phys., Conf. Ser.*, vol. 1828, no. 1, Feb. 2021, Art. no. 012115, doi: 10.1088/1742-6596/1828/1/012115.

[51] H. Dong, J. Zhao, X. Yang, and K. Yang, "Combination of D-AHP and grey theory for the assessment of the information security risks of smart grids," *Math. Problems Eng.*, vol. 2020, Oct. 2020, Art. no. e3517104, doi: 10.1155/2020/3517104.

[52] C. Yan and B. Qiao, "Study and application of risk evaluation on network security based on AHP," in *Proc. Conf. Commun. Inf. Process.*, Berlin, Germany, 2012, pp. 198–205, doi: 10.1007/978-3-642-31968-6_24.

[53] R. Zhang, L. Huang, and M. Xiao, "Security evaluation for wireless network based on fuzzy-AHP with variable weight," in *Proc. 2nd Int. Conf. Netw. Secur., Wireless Commun. Trusted Comput.*, Apr. 2010, vol. 1, pp. 490–493. [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4615-1665-1_1#citeas, doi: 10.1109/NSWCTC.2010.122.

[54] M. Khawla and M. Tomader, "A survey on the security of smart homes: Issues and solutions," in *Proc. 2nd Int. Conf. Smart Digit. Environ.*, New York, NY, USA, 2018, pp. 81–87, doi: 10.1145/3289100.3289114.

[55] I. Bernabe-Sanchez, D. Diaz-Sanchez, and M. Munoz-Organero, "Specification and unattended deployment of home networks at the edge of the network," *IEEE Trans. Consum. Electron.*, vol. 66, no. 4, pp. 279–288, Nov. 2020, doi: 10.1109/TCE.2020.3018543.

[56] E. Rubio-Drosdov, D. Díaz-Sánchez, F. Almenárez, P. Arias–Cabarcos, and A. Marín, "Seamless human-device interaction in the Internet of Things," *IEEE Trans. Consum. Electron.*, vol. 63, no. 4, pp. 490–498, Nov. 2017.

[57] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, Oct. 2020, doi: 10.1109/JIOT.2020.2983983

[58] J. Augusto-Gonzalez and A. Collen, "From Internet of Threats to Internet of Things: A cyber security architecture for smart homes," in *Proc. IEEE 24th Int. Workshop Comput. Aided Modeling Des. Commun. Links Netw. (CAMAD)*, Limassol, Cyprus, Sep. 2019, pp. 1–6, doi: 10.1109/CAMAD.2019.8858493.

[59] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Hum. Centric Comput. Inf. Sci.*, vol. 7, no. 1, pp. 1–6, Mar. 2017, doi: 10.1186/s13673-017-0087-4.

[60] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consum. Electron. Mag.*, vol. 9, no. 2, pp. 17–25, Mar. 2020, doi: 10.1109/MCE.2019.2953740.

[61] Z. Mohammad, T. A. Qattam, and K. Saleh, "Security weaknesses and attacks on the Internet of Things applications," in *Proc. IEEE Jordan Int. Joint Conf. Elect. Eng. Inf. Technol. (JEEIT)*, Amman, Jordan, Apr. 2019, pp. 431–436, doi: 10.1109/JEEIT.2019.8717411.

[62] Z. Shouran, A. Ashari, and T. K. Priyambodo, "Internet of Things (IoT) of smart home: Privacy and security," *Int. J. Comput. Appl.*, vol. 182, pp. 3–8, Oct. 2019, doi: 10.5120/ijca2019918450.

[63] L. Prathibha and K. Fatima, "Exploring security and authentication issues in Internet of Things," in *Proc. 2nd Int. Conf. Intell. Comput. Control Sys. (ICICCS)*, Madurai, India, Jun. 2018, pp. 673–678, doi: 10.1109/ICCONS.2018.8663111.

[64] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019, doi: 10.1109/JIOT.2018.2869847.

[65] M. Antonakakis, "Understanding the Mirai botnet," in *Proc. 26th USENIX Secur. Symp.*, Vancouver, BC, Canada, Aug. 2017, pp. 1093–1110.

[66] P. T. M. Ly, W. H. Lai, C. W. Hsu, and F. Y. Shih, "Fuzzy AHP analysis of Internet of Things (IoT) in enterprises," *Technol. Forecast. Soc. Change*, vol. 136, pp. 1–13, Oct. 2018, doi: 10.1016/j.techfore.2018.08.016.

[67] M. Schiefer, "Smart home definition and security threats," in *Proc. 9th Int. Conf. Secur. Incident Manage. Forensics*, 2015, pp. 114–118, doi: 10.1109/IMF.2015.17.

[68] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019, doi: 10.1016/j.comnet.2018.11.025.

[69] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things security, device authentication and access control: A review," 2019, *arXiv:1901.07309*.

[70] I. Astaburuaga, A. Lombardi, B. La Torre, C. Hughes, and S. Sengupta, "Vulnerability analysis of AR. drone 2.0, an embedded Linux system," in *Proc. IEEE 9th Ann. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2019, pp. 666–672, doi: 10.1109/CCWC.2019.8666464.

[71] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," in *Proc. 40th Int. Conv. Inf. Commu. Technol., Electro. Microelectron.*, Opatija, Croatia, May 2017, pp. 1292–1297, doi: 10.23919/MIPRO.2017.7973622.

[72] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security implications of permission models in smart-home application frameworks," *IEEE Secur. Privacy*, vol. 15, no. 2, pp. 24–30, Mar. 2017, doi: 10.1109/MSP.2017.43.

[73] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symp. Secur. Priv. (SP)*, San Jose, CA, May 2016, pp. 636–654, doi: 10.1109/SP.2016.44.

[74] I. Yaqoob and E. Ahmed, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 10–16, Jun. 2017, doi: 10.1109/MWC.2017.1600421.

[75] G. Hernandez, O. Arias, D. Buentello, and Y. Jin. *Smart Nest Thermostat: A Smart Spy in Your Home*. Accessed: Jan. 15, 2022. [Online]. Available: https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf

[76] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Five acts of consumer behavior: A potential security and privacy threat to Internet of Things," in *Proc. IEEE Int. Conf. Consum. Electro. (ICCE)*, Las Vegas, NV, USA, Oct. 2018, pp. 1–3, doi: 10.1109/ICCE.2018.8326124.

[77] B. E. Ozkan and S. Bulkan, "Hidden risks to cyberspace security from obsolete COTS software," in *Proc. 11th Int. Conf. Cyber Conflict (CyCon)*, May 2019, pp. 1–19, doi: 10.23919/CYCON.2019.8756990.

[78] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures and design tools," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1010–1038, Jun. 2020, doi: 10.1109/TCAD.2020.3047976.

[79] Q. Wang, W. U. Hassan, A. Bates, and C. Gunter, "Fear and logging in the Internet of Things," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, Feb. 2018, pp. 1–16, doi: 10.14722/ndss.2018.23282.

[80] Y. Tian, "SmartAuth: User-centered authorization for the Internet of Things," in *Proc. 26th USENIX Conf. Secur. Symp.*, Vancouver, BC, Canada, Aug. 2017, pp. 361–378.

[81] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *Proc. Int. Symp. Consum. Electro.*, Madrid, Spain, Aug. 2015, pp. 1–2, doi: 10.1109/ISCE.2015.7177843.

[82] J. H. Han, Y. Jeon, and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," in *Proc. Int. Conf. ICT Converg. Innov. Towar. IoT, 5G, Smart Media Era (ICTC)*, Jeju Island, South Korea, Oct. 2015, pp. 1116–1118, 2015.

[83] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attacking smart-homes," in *Proc. 9th ACM Conf. S&P*, Darmstadt, Germany, 2016, pp. 195–200, doi: 10.1145/2939918.2939925.

[84] A. Hussain, D. M. Marcinonyte, F. Iqbal Iqbal, H. Tawfik, T. Baker, and D. Al-Jumeily, "Smart home systems security," in *IEEE 16th Int. Conf. Smart City*, Exeter, U.K., Jun. 2018, pp. 1422–1428, doi: 10.1109/HPCC/SmartCity/DSS.2018.00235.

[85] K. Lounis and M. Zulkernine, "Attacks and defenses in short-range wireless technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[86] A. AlHammadi, A. AlZaabi, B. AlMarzooqi, S. AlNeyadi, Z. AlHashmi, and M. Shatnawi, "Survey of IoT-based smart home approaches," in *Proc. Adv. Sci. Eng. Technol. Int. Conf. (ASET)*, Dubai, United Arab Emirates, Mar. 2019, pp. 1–6, doi: 10.1109/ICASET.2019.8714572.

[87] A. Sivanathan, F. Loi, H. H. Gharakheili, and V. Sivaraman, "Experimental evaluation of cybersecurity threats to the smart-home," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Bhubaneswar, India, Dec. 2017, pp. 1–6, doi: 10.1109/ANTS.2017.8384143.

[88] M. D. Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "Analysis of DDoS-capable IoT malwares," in *Proc. Federated Conf. Comput. Sci. Info. Syst. (FedCSIS)*, Prague, Czech Republic, Sep. 2017, pp. 807–816, doi: 10.15439/2017F288.

[89] N. Aviram, S. Schinzel, and J. Somorovsky, "DROWN: Breaking TLS using SSLv2," in *Proc. 25th USENIX Conf. Secur. Symp.*, Austin, TX, USA, Aug. 2016, pp. 689–706.

[90] N. Apthorpe, D. Reisman, and N. Feamster. (Jan. 2017). *A Smart Home is, no, Castle: Privacy Vulnerabilities of Encrypted IoT Traffic*. Accessed: Jan. 15, 2022. [Online]. Available: https://arxiv.org/abs/1705.06805

[91] D. Adrian, "Imperfect forward secrecy: How Diffie-Hellman fails in practice," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commu. Secur.*, Denver, CO, USA, 2015, pp. 5–17, doi: 10.1145/2810103.2813707.

[92] S. Godwin, B. Glendenning, and K. Gagneja, "Future security of smart speaker and IoT smart home devices," in *Proc. 5th Conf. Mobi. Sec. Serv. (MobiSecServ)*, Miami Beach, FL, USA, 2019, pp. 1–6, doi: 10.1109/MOBISECSERV.2019.8686545.

[93] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, "Smart locks: Lessons for securing commodity Internet of Things devices," in *Proc. 11th ACM Asia Conf. Comput. Commu. Secur.*, Xi'an, China, 2016, pp. 461–472, doi: 10.1145/2897845.2897886.

[94] K. Lounis and M. Zulkernine. (Oct. 2019). *Bluetooth Low Energy Makes*. Accessed: Jan. 15, 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-02528877

[95] Y. Oren and A. D. Keromytis, "Attacking the internet using broadcast digital television," *ACM Trans. Inf. Syst. Secur.*, vol. 17, no. 4, pp. 1–27, Apr. 2015, doi: 10.1145/2723159.

[96] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, pp. 80–89, 2019, doi: 10.3390/fi11040089.

[97] D. Wood, N. Apthorpe, and N. Feamster, "Cleartext data transmissions in consumer IoT medical devices," in *Proc. Workshop Internet Things Secur. Priv.*, vol. 17, Dallas, TX, USA, Nov. 2017, pp. 7–12, doi: 10.1145/3139937.3139939.

[98] M. Gajewski, J. Mongay Batalla, A. Levi, C. Togay, C. X. Mavromoustakis, and G. Mastorakis, "Two-tier anomaly detection based on traffic profiling of the home automation system," *Comput. Netw.*, vol. 158, pp. 46–60, Jul. 2019, doi: 10.1016/j.comnet.2019.04.013.

[99] R. Taheri, M. Shojafar, M. Alazab, and R. Tafazolli, "FED-IIoT: A robust federated malware detection architecture in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8442–8452, Dec. 2020, doi: 10.1109/TII.2020.3043458.

[100] A. Kuppa, S. Grzonkowski, M. R. Asghar, and N. Le-Khac, "Finding rats in cats: Detecting stealthy attacks using group anomaly detection," in *Proc. 18th IEEE Int. Conf. Trus. Secur. Priv. Comput. Commu.*, Rotorua, New Zealand, Aug. 2019, pp. 442–449, doi: 10.1109/TrustCom/BigDataSE.2019.00066.

[101] F. Xia, H. Song, and C. Xu, "Securing the wireless environment of IoT," in *Proc. IEEE Int. Conf. Saf. Produce Inf. (IICSPI)*, Chongqing, China, Dec. 2018, pp. 315–318, doi: 10.1109/IICSPI.2018.8690435.

[102] G. Spanos, "A lightweight cyber-security defense framework for smart homes," in *Proc. Int. Conf. Innov. Intell. Sys. Appl. (INISTA)*, Novi Sad, Serbia, Aug. 2020, pp. 1–7, doi: 10.1109/INISTA49547.2020.9194689.

[103] Z. Pan, S. Hariri, and J. Pacheco, "Context aware intrusion detection for building automation systems," *Comput. Secur.*, vol. 85, pp. 181–201, Aug. 2019, doi: 10.1016/j.cose.2019.04.011.

[104] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar, and S. Kumari, "Light-edge: A lightweight authentication protocol for IoT devices in an edge-cloud environment," *IEEE Consum. Electron. Mag.*, early access, Jan. 25, 2021, doi: 10.1109/MCE.2021.3053543.

[105] F. A. Mendoza, P. A. Cabarcos, and R. S. Sherratt, "TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3502–3531, 4th Quart., 2019, doi: 10.1109/COMST.2019.2914453.

[106] B. Beurdouche, "A messy state of the union: Taming the composite state machines of TLS," in *Proc. IEEE Symp. Secur. Priv.*, May 2015, pp. 535–552, doi: 10.1109/SP.2015.39.

[107] S. Peter and R. K. Gopal, "Multi-level authentication system for smart home-security analysis and implementation," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, Coimbatore, India, Aug. 2016, pp. 1–7, doi: 10.1109/INVENTIVE.2016.7824790.

[108] X. Huang, P. Craig, H. Lin, and Z. Yan, "SecIoT: A security framework for the Internet of Things," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3083–3094, 2016, doi: 10.1002/sec.1259.

[109] M. Serror, M. Henze, S. Hack, M. Schuba, and K. Wehrle, "Towards in-network security for smart homes," in *Proc. 13th Int. Conf. Availabil., Reliabil. Secur.*, Hamburg, Germany, 2018, pp. 1–8, doi: 10.1145/3230833.3232802.

[110] N. Apthorpe, D. Reisman, and N. Feamster, "Closing the blinds: Four strategies for protecting smart home privacy from network observers," 2017, *arXiv:1705.06809*.

[111] E. Kim and C. Keum, "Trustworthy gateway system providing IoT trust domain of smart home," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 551–553, doi: 10.1109/ICUFN.2017.7993848.

[112] S. S. Gill, P. Garraghan, and R. Buyya, ''ROUTER: Fog enabled cloud based intelligent resource management approach for smart home IoT devices,'' *J. Syst. Softw.*, vol. 154, pp. 125–138, Aug. 2019, doi: 10.1016/j.jss.2019.04.058.

[113] S. R. Oh and Y. G. Kim, ''Security requirements analysis for the IoT,'' in *Proc. Int. Conf. Platform Technol. Service*, Busan, South Korea, Feb. 2017, pp. 1–6, doi: 10.1109/PlatCon.2017.7883727.

[114] F. Hussain and M. Qi, ''Integrated privacy preserving framework for smart home,'' in *Proc. 14th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Huangshan, China, Jul. 2018, pp. 1246–1253, doi: 10.1109/FSKD.2018.8687201.

[115] J. Bugeja and A. Jacobsson, ''An investigation of vulnerabilities in smart connected cameras,'' in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2018, pp. 537–542, doi: 10.1109/PERCOMW.2018.8480184.

[116] J. Obermaier and M. Hutle, ''Analyzing the security and privacy of cloud-based video surveillance systems,'' in *Proc. 2nd ACM Int. Workshop IoT Priv. Trust Secur.*, Xi'an, China, 2016, pp. 22–28, doi: 10.1145/2899007.2899008.

[117] M. Surbatovich, J. Aljuraidan, L. Bauer, A. Das, and L. Jia, ''Some recipes can do more than spoil your appetite: Analyzing the security and privacy risks of IFTTT recipes,'' in *Proc. Int. Conf. World Wide Web*, Perth, WA, Australia, 2017, pp. 1501–1510, doi: 10.1145/3038912.3052709.

[118] C. Nandi and M. D. Ernst, ''Automatic trigger generation for rule-based smart homes,'' in *Proc. ACM Workshop Program. Lang. Anal. Secur.*, Vienna, Austria, 2016, pp. 97–102, doi: 10.1145/2993600.2993601.

[119] A. Alsadi and S. Mohan, ''Improving the physical layer security of the Internet of Things (IoT),'' in *Proc. IEEE Int. Smart Cities Conf. (ISC2)*, Kansas City, MI, USA, Sep. 2018, pp. 1–8, doi: 10.1109/ISC2.2018.8656679.

[120] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, ''Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes,'' *Elsevier Sci.*, vol. 78, no. 3, pp. 1040–1051, Jan. 2018, doi: 10.1016/j.future.2016.11.011.

[121] J. Wilson, R. S. Wahby, H. Corrigan-Gibbs, D. Boneh, P. Levis, and K. Winstein, ''Trust but verify: Auditing the secure Internet of Things,'' in *Proc. 15th Annu. Int. Conf. Mobile Syst. Appl. Services*, Niagara Falls, NY, USA, 2017, pp. 464–474, doi: 10.1145/3081333.3081342.

[122] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, ''Decentralized action integrity for trigger-action IoT platforms,'' in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2018, pp. 1–16, doi: 10.14722/ndss.2018.23119.

[123] H. Hu, L. Yang, S. Lin, and G. Wang, ''Security vetting process of smart-home assistant applications: A first look and case studies,'' 2020, *arXiv:2001.04520*.

[124] S. Grzonkowski, A. Mosquera, L. Aouad, and D. Morss, ''Smartphone Security: An overview of emerging threats,'' *IEEE Consum. Electron. Mag.*, vol. 3, no. 4, pp. 40–44, Oct. 2014, doi: 10.1109/MCE.2014.2340211.

[125] G. Nebbione and M. C. Calzarossa, ''Security of IoT application layer protocols: Challenges and findings,'' *Future Internet*, vol. 12, no. 3, Mar. 2020, pp. 50–55, doi: 10.3390/fi12030055.

[126] H. Liu, T. Spink, and P. Patras, ''Uncovering security vulnerabilities in the Belkin WeMo home automation ecosystem,'' in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Kyoto, Japan, Mar. 2019, pp. 894–899, doi: 10.1109/PERCOMW.2019.8730685.

[127] J. Margulies, ''Garage door openers: An Internet of Things case study,'' *IEEE Secur. Privacy*, vol. 13, no. 4, pp. 80–83, Jul. 2015, doi: 10.1109/MSP.2015.80.

[128] E. Fernandes, J. Paupore, A. Rahmati, D. Simionato, M. Conti, and A. Prakash, ''FlowFence: Practical data protection for emerging IoT application frameworks,'' in *Proc. 25th USENIX Secur. Symp.*, Austin, TX, USA, Aug. 2016, pp. 531–548. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/fernandes

[129] S. Demetriou, ''HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps,'' in *Proc. 10th ACM Conf. Secur. Priv. Wireless Mobile Netw.*, Boston, MA, USA, 2017, pp. 122–133, doi: 10.1145/3098243.3098251.

[130] J. Chen, ''IoTFuzzer: Discovering memory corruptions in IoT through app-based fuzzing,'' in *Proc. Netw. Distrib. Syst. Secur. Symp.*, San Diego, CA, USA, 2018, pp. 1–15, doi: 10.14722/ndss.2018.23159.

[131] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, and Y. Kato, ''Anomaly detection in smart home operation from user behaviors and home conditions,'' *IEEE Trans. Consum. Electron.*, vol. 66, no. 2, pp. 183–192, May 2020, doi: 10.1109/TCE.2020.2981636.

[132] (June 2019). *CVSS V3.1 Specification Document*. Accessed: Jan. 15, 2022. [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[133] E. E. Cureton, ''Rank-biserial correlation,'' *Psychometrika*, vol. 21, no. 3, pp. 287–290, Sep. 1956, doi: 10.1007/BF02289138.

[134] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose. (May 2019). *YourThings Scorecards*. Accessed: Jan. 15, 2022. [Online]. Available: https://yourthings.info/scorecards

[135] T. L. Saaty, ''Decision-making with the AHP: Why is the principal eigenvector necessary,'' *Eur. J. Oper. Res.*, vol. 145, no. 1, pp. 85–91, Feb. 2003.

[136] J. Franek and A. Kresta, ''Judgment scales and consistency measure in AHP,'' *Proc. Econ. Finance*, vol. 12, pp. 164–173, Jan. 2014, doi: 10.1016/S2212-5671(14)00332-3.

[137] D. Yu, ''Softmax function based intuitionistic fuzzy multi-criteria decision making and applications,'' *Oper. Res.*, vol. 16, no. 2, pp. 327–348, Jul. 2016, doi: 10.1007/s12351-015-0196-7.

[138] V. I. Levenshtein, ''Binary codes capable of correcting deletions, insertions and reversals,'' *Sov. Phys. Dokl.*, vol. 10, no. 8, pp. 707–710, Feb. 1966.

NABA M. ALLIFAH received the B.Sc. degree in computer science from Prince Mohammad Bin Fahd University, Saudi Arabia, in 2016, and the M.Sc. degree in engineering systems management with major concentration of IT management from the American University of Sharjah, United Arab Emirates, in 2020. Her current research interests include the Internet of Things (IoT) and smart homes.

IMRAN A. ZUALKERNAN (Member, IEEE) received the B.S. (Hons.) and Ph.D. degrees in computer science from the University of Minnesota, Minneapolis, in 1983 and 1991, respectively. He was an Assistant Professor with the Computer and Electrical Engineering Department, Pennsylvania State University, from 1992 to 1995. He was a Principal Design Engineer with AMCS Inc., Chanhassen, MN, USA, from 1995 to 1998. He was the Chief Executive Officer at Askari Information Systems, from 1998 to 2000, and the Chief Technology Officer at Knowledge Platform, Inc., Singapore, from 2000 to 2003. In 2003, he joined the American University of Sharjah, United Arab Emirates, where he is currently a Professor of computer science and engineering. He is an author or the coauthor of more than 200 peer-reviewed articles. His research interests include consumer systems, sensor-based internet applications, the IoT for consumer devices, and the Internet of Things (IoT). He has received the 2020 IEEE Consumer Electronics Society Chester Sall Award.