IJICTR
International Journal of Information & Communication Technology Research

Volume 12- Number 1 – Winter 2020 (11 -19)

Security Framework of IoT-Based Smart Home

Shahrouz Sotoudeh
ICT Research Institute
Tehran, Iran
Sotoudeh@itrc.ac.ir

Sattar Hashemi
Department of Computer and Electronic
University of Shiraz
Iran
s_hashemi@shirazu.ac.ir

Hossein Gharaee Garakani*
ICT Research Institute
Tehran, Iran
gharaee@itrc.ac.ir

Received: 7 September 2019 - Accepted: 2 December 2019

***Abstract*—Internet of Things (IoT) security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Smart home is considered one of the rather prominent applications of the Internet of Things (IoT), integrating high-levels of efficiency, home security, energy & cost saving to everyone's life. In spite of all the benefits this technology provides, privacy and security are highly concerning issues that require more considerations. IoT-A reference architecture was established with the purpose of evaluating current sources and protocols, ensuring the compliance of things and protocols, and providing a comprehensive solution for different applications of IoT. This study was performed with the purpose of providing a general framework for improving security at all levels of design, implementation, and application of equipment and protocols using the IoT-A reference architecture by addressing the challenge of security in the Internet of Things and smart homes. This paper employs the term Security Framework to refer to a method for applying all technologies, procedures, software, and other components to provide security in smart homes. This research seeks to outline all the reference architecture's vulnerabilities and threats, following which an improved model for the reference architecture is proposed to meet all security requirements. Considering the theoretical evaluations performed in this study, the proposed framework, which was created by adding two components of threat and vulnerability management and field management while making some alterations to the licensing component, satisfies to an acceptable level the security requirements of the smart home and enhances the privacy of the IoT-based smart home.**

***Keywords*—Smart home; IoT; security and privacy; security architecture**

I. INTRODUCTION

As an important component of the Internet of Things (IoT), smart homes serve users effectively by communicating with various digital devices based on IoT. In the ideal version of a wired future, all smart homes' devices communicate with one another seamlessly. Smart home technology based on IoT has changed human life by providing connectivity to everyone regardless of time and place [1], [2]. Home automation systems have become increasingly sophisticated in recent years. These systems provide infrastructure and methods to exchange all types of appliance information and services [3]. A smart home is a IoT domain, a network of physical devices that provide electronic, sensor, software, and network connectivity inside a home. Smart homes are automated buildings with installed detection and control devices, such as air conditioning and heating, ventilation, lighting, hardware, and security systems. These modern systems, which include switches and sensors that communicate with a central axis, are sometimes called "gateways." These "gateways" are control systems with a user

* Corresponding Author

interface that interacts with a tablet, mobile phone, or computer; these systems' network connectivity is managed by IoT [4]. Since 2010, researchers have analyzed IoT-based smart home applications using several approaches. Regardless of their category, existing research articles focus on the challenges that hinder smart home IoT applications' full utilization and provide recommendations to mitigate these problems. Research on smart home applications is dynamic and diverse. This survey aims to provide valuable insights into technological environments and support researchers by understanding the available options and gaps in this research line. It aims to shed light on researchers' efforts in response to new and disruptive technology, map the research landscape into a coherent taxonomy, and determine the features that characterize this emerging line of research in smart home technology. Another set of problems are more social and organizational rather than technical, physical or material. These types' problems are associated with multiple and diverse stakeholders, high levels of interdependence, competing objectives and values, and social and political complexity. In this sense, city problems become wicked and tangled [16,31,39]. Ensuring livable conditions within the context of such rapid urban population growth worldwide requires a deeper understanding of the smart city concept. The urgency around these challenges is triggering many cities worldwide to find more ingenious ways to manage them. These cities are increasingly described with the label smart city. One way to conceptualize a smart city is as an icon of a sustainable and livable city.

Internet of Things (IoT) consists of devices that generate, process, and vast exchange amounts of security and safety-critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber-attacks [1]. Many new networkable devices, which constitute the IoT, are low energy and lightweight. These devices must devote most of their available energy and computation to executing core application functionality, making the task of affordably supporting security and privacy quite challenging. Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead. Moreover, many state-of-the-art security frameworks are highly centralized and are thus not necessarily well-suited for IoT due to the difficulty of scale, the many-to-one nature of the traffic, and a single point of failure [2]. To protect user privacy, existing methods often either reveal noisy data or incomplete data, potentially hindering some IoT applications from offering personalized services [3]. Consequently, IoT demands a lightweight, scalable, and distributed security and privacy safeguard. The Blockchain (BC) technology that underpins Bitcoin the first cyptocurrency system [4] has the potential to overcome the aforementioned challenges due to the potential to overcome the aforementioned challenges its distributed, secure, and private nature.

II. Related Works

Recently, IoT has been applied in numerous applications, including smart home monitoring systems for assisted living to predict residents' wellness through the monitoring of several home appliances [4]. building management framework to support energy-saving applications [18], and human activity patterns monitoring [19,20]. As the Internet communications infrastructure develops to include sensing objects, suitable mechanisms are needed to secure communications with such entities in IoT applications. In real-world IoT applications, security threats and attacks are becoming a major issue for data transmission. Hence, the IoT-based system must include security mechanisms that could resist possible security threats and attacks in data modification, impersonation, and eavesdropping, among others. One solution for efficient key generation and management in 6LoWPAN is Lightweight IKEv2: but it requires more resources and energy for its implementation [23,24]; (2) It is not an appropriate standard for smart homes, since it does not facilitate communication among a large number of IoT nodes and it also does not have a wide coverage range [17]. The first issue can be resolved by developing an energy-efficient security algorithm based on an efficient key generation mechanism for secure data transmission in IoT applications. To resolve the second problem, recently, low-power Wi-Fi systems optimized for sensing applications are available due to the growing industry requirements for smart objects having IP connectivity [25]. According to [17], the latest Wi-Fi standard fills this gap by combining the advantages of Wi-Fi and low-power sensor network communication technologies. The emerging Wi-Fi standard is a promising communication standard that supports many heterogeneous devices in the IoT. A comparison between the latest 802.11 ah and 802.15.4 standards is described in detail in [17]; 802.11 ah performs better in association time, throughput, delay, and coverage range. Wi-Fi is the preferred standard over 6LoWPAN for several IoT applications such as smart cities and smart homes due to all these advantages. Therefore, along with the low-power Wi-Fi module to support the large number of IoT nodes and increase coverage range, security algorithms for data encryption based on efficient key generation mechanisms need to be included in WSNs with the internet novel secured IoT based smart home. Since home appliances have wireless network function -in, the smart home has provided many services for users. Through wireless network, a user can control home appliances, lighting, and cooling and heating devices and receive services regardless of time and space. A smart home provides more convenient and valuable services, for all home appliances get automated and smart. For useful services, a diversity of sensor information customized personal information (hobbies, habits, medical service, etc.), and financial information are used. For this reason, security technology should be applied [7, 9–11]. This section describes smart home devices' structure and security matters and the previous studies related to smart home security.

Several IoT-based systems are developed, including integrating security mechanisms within WSNs to provide efficient security for different applications [26–28]. Generally, hash functions, symmetric and asymmetric encryption algorithms are utilized to offer data security. The asymmetric algorithms are not suitable for implementing sensor networks' security due to the tiny sensor nodes' limited computational power [6]. Thus, hash functions, symmetric algorithms including message digest 4 (MD4) [29], message digest 5 (MD5) [30], secure hash algorithm 1 (SHA-1) [31], hash message authentication code (HMAC) [32], Data Encryption Standard (DES) [33], Advanced Encryption Standard (AES) [34], Rivest Cipher 4 (RC4) [35], blowfish [36], are utilized to

secure the sensor networks. Since these mentioned techniques are not precisely developed by keeping in view the specification of WSNs, these networks require more energy for their implementation. Therefore, security mechanisms specifically designed for WSNs could be the optimal solution for IoT applications. Mandal et al. developed a hybrid scheme of both symmetric-key and asymmetric-key-based cryptographic functions for securing WSNs. However, their scheme has not considered all the major security requirements [16]. Proposed a novel hybrid lightweight security method, PRESENT-GRP for secure data transmission in IoT-based applications and implemented on an Intel Galileo Gen 2 board. It follows a complex permutation boxes-based strategy, which requires more processing time and resources [26].

III. Threats for IoT in the Smart-Home

Smart home appliances of all varieties are emerging in the market, and Cisco VNI predicts that Internet-of-Things (IoT) connections will grow by 43% each year, rising from 341 million globally in 2013 to 2 billion by 2018. We procured several such devices and studied their behavior in our lab – we have previously revealed some of these devices' vulnerabilities in our earlier work [4]. We briefly elaborate on these to provide the context for the defense techniques that will be presented later. The Philips Hue Connected bulb allows the user to control the lighting system in the home wirelessly. It consists of an Ethernet enabled bridge that accepts commands from the user app and communicates these to the bulbs using the ZigBee-Light link protocol. The data exchange between the app and the bridge is via HTTP commands and is not encrypted, so an eavesdropper can easily deduce the user's operations on the bulb. Further, even though the device implements access control in the form of a white-listed set of users, any attacker can extract this list, who can then masquerade as a legitimate user, thereby gaining control over the bulb.

The Nest smoke-alarm sends reports and alerts to the user's mobile app, giving them peace-of-mind that their house is safe no matter where they are. However, it comes equipped with sensors that detect motion and light – this can potentially let it detect when the user is in the same room or if he/she has turned on/off the lights. These capabilities immediately raise a privacy concern for the user who may feel that they are being monitored and tracked within their home. We do note that all data exchanges with the Nest smoke-alarm are encrypted, so eavesdroppers cannot read into the communications.

The Withings Smart Baby Monitor comes with an IP camera that allows the user to monitor their baby at home via an App on their phone. We captured and WiFi packets to/from the baby monitor and found all the data exchange to be in plain-text; however, access to the camera requires obtaining a one-time access token from the server. We created a "man-in-the-middle" attack in which we allow the victim's app to authenticate itself to the server and obtain the session id, but then hijack the connection using ARP poisoning, allowing the attacker to replace the source IP address to his own to gain access to the camera feed

IV. Smart Home Security

This section provides the theoretical foundations of research on the security challenges and threats of the IoT-based smart home.

Today, homes are highly automated using intelligent technologies and thus can meet the demands of all residents, among which are comfort, security and privacy, while being sensitive and responsive to the needs of the modern human and the living environment [20, 21]. The main automation applications in smart home environments are luminosity control, heating and air conditioning, monitoring, maintaining security and protection, telemedicine, energy consumption levels, control of environmental factors, and access to the required information. The introduction of smart home to the realm of Internet of Things is associated with the delegation of storage, processing, and data analysis to the facilities offered in cyberspace further security challenges [22-25].

Security and privacy are the most important challenges of deploying IoT in smart homes. Proper security architecture is responsible for covering the life cycle and IoT capabilities in this field [26, 27]. Various studies have been performed to improve the overall security of the Internet of Things. Yet, issues such as appropriate mechanisms for encryption, network protocols, data and identifier management, user privacy, and reliable architectures are still debatable [28-30]. According to the literature on smart home security, privacy, trust, security, and communication are among the major challenges facing smart homes, and communication is among the smart homes' major challenges [25].

Vulnerabilities in the Internet of Things and the smart home pose a variety of threats. A number of these threats are based on the research presented in Table 2.

Various research centers have provided comprehensive solutions called reference architectures to address the challenges in IoT. Wso2 architecture was proposed with the aim of providing cloud services, Korean reference architecture was developed to embed this technology to the industry, while the Chinese reference architecture was introduced to standardize this technology in China [31].

The IoT-A Reference Architecture was established to examine existing protocols and resources, ensure the compatibility of objects and communication protocols, and provide a comprehensive solution for IoT's various applications in the European Union. It is consisted of several sub-models, among which the functional model is employed for the purposes of this research. The functional model is an abstract-level framework for understanding the main application groups and their interactions in the IoT-A environment, which in turn defines common notions used in the development of IoT-A compatible functional perspectives [32].

The IoT-A functional model includes seven vertical capabilities and two horizontal performance groups, namely management and security. The security framework in the functional model is consisted of 5 components that needs to be optimized to improve the level of protection in the architecture. Fig. 1 shows the components of the functional model [32].

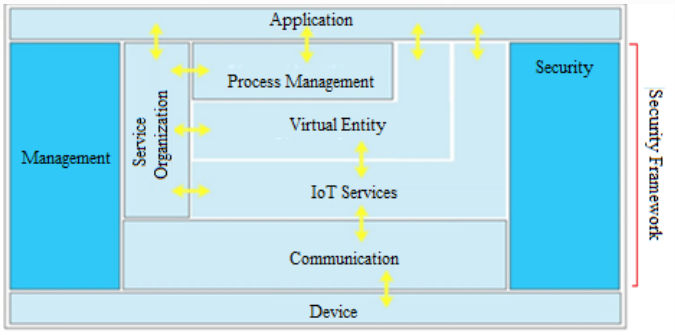

Fig. 1. Functional model and components of the security framework of IoT-A [32].

For the purpose of providing a suitable architecture and considering the comparison and approach of the introduced architectures, it can be concluded that the model and architecture presented in IoT-A is far more comprehensive than the other architectures in terms of purpose, diversity of documents, scope of the research group and its geographical area, namely European Union. Moreover, according to previous research results, offered in Table 1, it is evident that compared to other architectures, the IoT-A architecture simultaneously meets the two functional needs sought-after in this research [33]. Hence, considering the comprehensiveness of the IoT-A architecture and the necessity to meet various functional requirements, it is employed as the reference architecture in this study.

TABLE I. APPLICATION REQUIREMENTS OF REFRENCE ARCHITECTURES[33].

	Architecture		***IoT-A ARM***	***WSO2***	***Korean ARM***	***Chinese ARM***
Functional need	Application support requirements	Reliable and secure services connected to the human body	√	-	-	√
	Security and privacy requirements	Security audit	√	√	-	-

V. SECURITY REQUIREMENTS OF THE SMART HOME

After examining the threats and vulnerabilities and mapping them into architectural components, recognizing the needs for improving the overall security situation becomes priority. The security requirements for a safe smart home service, including integrity, availability, and authentication, are discussed. To this end, the smart home's security needs were studied and identified, the results of which are presented in Table 2. Applying or improving the performance of security mechanisms in each component leads to the smart home's overall improvement. Hence, this article's main purpose was to provide solutions for satisfying the security requirement mentioned in reference architecture security component's security component.

A. Integrity

A smart device can be accessed over wireless network, so that it needs security system. An attacker can insert a malignant software application and change a service purpose through a malicious code. For the reason, without integrity, the whole smart home system can be infected with a malicious code by an attacker and thereby the availability of smart home service can fall. Therefore, the integrity of smart home service is required. To ensure smart devices' integrity, it is essential to use a hash function and a digital signature for critical data or module codes [16–18].

B. Availability

A smart device sends and receives data to and from the outside over a wireless network. If an attacker steals data, it is possible to fabricate and modify the data. The fabricated data can cause a malfunction of a smart device that deteriorates a user's smart device availability. The deteriorated availability can lead to devise overload that triggers a fire. The malfunction can bring about financial losses like a rise in electric rate and the risk of life. To secure availability, it is required to limit other actions than essential functions and grant rights for functional access by making strong access control [7, 11, 16, 19].

C. Authentication

There are many devices whose security is not taken into account. If an attacker insert a copied module or a malignant code in a smart device, it is possible to contaminate a smart home service environment and make the device used for malicious purposes, such as distributed denial of service (DDoS), denial of service (DoS), and personal information leakage. Moreover, if an attacker disguises a modified module as a normal module, the module can serve as the secret backdoor for malicious action which can lower the function of the normal module and thereby deteriorate availability. Therefore, it is required to provide authentication of a smart device. For the authentication, it is possible to use a certificate [18–20].

TABLE II. SECURITY REQUIREMENTS OF THE SMART HOME

Requirement	**References**
Authentication	[34]
Identity management	[35]

Privacy	[34, 35]
Availability	[34, 35]
Resistance	[34-36]
Information security	[34]
Access control	[34]
Delegation	[34]
Trust	[35]

VI. Proposed Solution for Improving Security

The functional model of the IoT-A ARM provides a set of components with a certain degree of abstraction as a security framework. The aforementioned model allows developers to have access to a variety of approaches to implementation depending on the application. As a result, this study seeks to complement the above abstract model such that the security of smart home applications is enhanced based on the mentioned security requirements. To this end, the context management component was embedded to other existing security components with the purpose of collecting, updating and properly managing information about existing objects while providing accurate and up-to-date information. Furthermore, the component of vulnerabilities and threat management was integrated to the 5 components of the architectural security framework for maximum monitoring, detection and handling of threats and vulnerabilities. The licensing component has been altered to provide access to smart home information resources with maximum compliance with privacy and security of residents, thus leading to safer grounds for other applications, including remote health, to access the smart home. The components of the proposed framework are compared with those of the standard IoT-A framework in Table 3.

TABLE III. Comparison of the Components of the Propoes Framework with the Components of IoT-A Reference Architecture

Current components	Proposed components
Authentication	Authentication
Identity management	Identity management
Access permission	Distributed access permission
Key exchange and management	Key exchange and management
Trust and credibility	Trust and credibility
	Vulnerability and threat management
	Context management

As shown in Table 3, two components, namely vulnerability and threat management, and context management are added to the reference framework while alterations have been made to the licensing method, which are explained below.

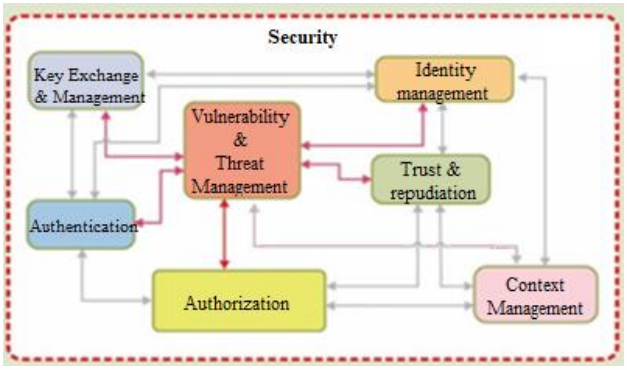

Fig. 2. Components of the proposed framework.

This component is responsible for identifying and preserving information that is continuously generated and exchanged by and between users and devices. This information may include the properties of objects, services, and entities in the work area. The proposed mechanism is designed to identify and record existing smart objects and services using the discovery service and a set of repositories in the directory level. Following discovery, the information is recorded in the source directory and stored in the repository. These services are distributed and connected to their main centers in the service provider and transfer each directory's information to the central system according to the level of privilege and necessity. This method readily offers the capability to integrate intelligent objects under different technologies and protocols [34]. In addition, this component will provide up-to-date information for other security components. The interaction of this component with other components is shown in Fig. 2.

Implementing policies for controlling access requires a comprehensive yet scalable decision-making mechanism, which should have features such as the ability to perform various assessments, facilitate the management of the systems, and background support of requirements. It also should be able to expand and decide on access control as a partnership in several nodes in a so-called distributed manner. The method of distributed licensing under the proposed security framework was devised having in mind the interaction of the smart home with other areas of the Internet of Things. The combination of the authentication process and access permissions can be seen in Fig. 3.

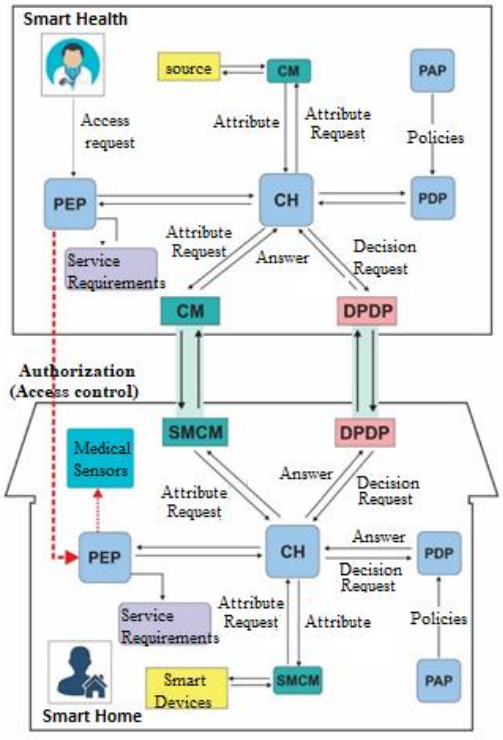

Fig. 3. Distributed mechanisms of evaluation and licensing between the smart home and the smart health.

Based on the above figure, the requester sends the access request to the policy enforcement point (PEP). The PEP sends a request for information to the context handler (CH). Since the decision-making function is in another area, i.e. the smart home, the context handler sends a request to the context management (CM) to complete information on the requested resourcrequested resource attribute attribute. It also sends a message to the distributed decision point (DPDP) to make the appropriate decision. The CM requests information from its counterpoint, the context management of the smart home. The DPDP also requests a decision from its counterpart in the smart home. The context handler in the smart home is responsible for receiving all the requests.

The policy administration point (PAP) provides policies and policy sets to the policy decision point (PDP). Based on existing policies and the characteristics of the requested resource, the PDP sends the necessary conclusion response to the CH, which submits the decisions to the DPDP and. Also, it provides the requested features to the CM. The CH delivers the information sent from the smart home to the PEP, where the requirements are reviewed and, if approved, grants access to the resource, otherwise denies access.

Vulnerability and threat management, which somehow plays the role of security operation center for the smart home, was proposed for centralized management to monitor, detect vulnerabilities and deal with threats. It is consisted of monitoring, data collection, analysis and response services [35]. To function properly and collect new and reliable information from the objects and services available in the smart home, it needs to be linked to context management. After analyzing the security information, the appropriate diagnosis and response to the potential threat are made. It is also used to fix and address vulnerabilities in objects. due to the high costs of designing, implementing and maintaining, it is recommended to be deployed as a cloud service provider and IoT service provider.

VII. Analysis of the Proposed Solution

In this research, the security requirements and needs of IoT-based smart home were outlined. In the functional model of IoT-A architecture, a general security framework with a certain degree of abstraction was considered to establish security. Moreover, a novel framework was proposed for improving security in smart home applications as a new solution and making alterations to the aforementioned security model. These changes included the addition of two components of context management and management of vulnerabilities and threats, and the application of assessment and licensing in a distributed manner. The purpose of the new framework was to maximize the security needs of the smart home. The results are presented theoretically and from integrating successful solutions of previous research with a degree of abstraction. Therefore, analysis and comparison methods are used to evaluate the proposed theoretical model.

In the following section, each of the proposed components is analyzed based on its functions and security purpose. Table 4 shows the functions of the component and the intended security objectives provided by each component.

A. *Comparison of results*

In the following, the proposed model is compared with existing solutions. First, the proposed model is compared with the functional model and then with the existing security frameworks in this field.

B. *Comparison with the security framework in the IoT-A architecture*

The framework provided in the IoT-A reference architecture has five standard components for providing the security of the components. These components are designed and implemented according to the needs of the security standard. Table 5 provides a comparison between the security objectives met by the two basic security architectural frameworks and the proposed framework.

TABLE IV. Components of the Proposed Solution Along with its Functions and Security Purpose

Proposed component	**Function of the component**	**Intended security objectives**
Identity management	Management of identities, aliases, and relevant access policies	User privacy Service privacy
Authentication	Authentication of entities	Authentication Responsibility
Licensing	Controlling access to services	Service access control Data privacy Data integrity
	Controlling access over infrastructure control	Service privacy Service availability
Key management and exchange	Managing and exchanging encryption keys	Confidentiality of communications Accuracy of communication non-denial forward and backward secrecy
Vulnerability and threat management	Discovering vulnerabilities and threats	Confidentiality Information integrity Accuracy of information Privacy Communication security
Trust and credibility	Collecting user credit points and calculating service trust level	Service credit Service trust Privacy
Context management	Gathering information on objects, resources and services	Novelty and accuracy of information Privacy Availability

TABLE V. SECURITY COMPONENTS OF THE ARCHITECTURE AND PROPOSED FRAMEWORK [25,32]

Security component	Desired security goals	Architecture	Proposed
Identity management	Privacy of users	✓	✓
	Service Privacy	✓	✓
	Responsibility	✓	✓
Licensing	Service access control	✓	✓
	Data privacy	✓	✓
	Data accuracy	✓	✓
	Service privacy	✓	✓
	Service availability	✓	✓
	Privacy of the functional domain	✓	✓
Key management and exchange	Confidentiality of communications	✓	✓
	Communication integrity	✓	✓
	Non-denial	✓	✓
	Forward and backward secrecy	✓	✓
Vulnerability and threat management	Hardening	-	✓
	Confidentiality	-	✓
	Information integrity	-	✓
	Accuracy of information	-	✓
	Privacy	-	✓
	Communication security	-	✓
	Application security	-	✓
Trust and credibility	Service credit	✓	✓
	Service trust	✓	✓
	Privacy	✓	✓
Context management	Novelty and accuracy of information	-	✓
	Confidentiality of information in the scope of application	-	✓
	Availability of information	-	✓

VIII. COMPARISON FRAMEWORK

In this section, we discussed another related framework, which is utilized for the smart home.

- Complete design and implementation of an innovative, efficient, and low-cost smart house system is introduced by [39]. Under the guidance of IoT technologies, the system can act and effectively automates remote environments. This research project motivated mainly to compare the applicability and the cost limitation of NETPI and BLYNK network platforms. NETPI confirmed that many specifications could be fulfilled using several modules under the main primary supervisor's supervision. However, BLYNK offered restrictions regarding projects' design in a unique sole GUI, mainly when more than one microcontroller is used. Besides, the cost is considered expensive due to energy-based limits exist in BLYNK that constrain users to fulfill their design specifications. On the other hand, the BLYNK platform is friendly, helpful, and easy to design considerable projects in less time, unlike the NETPI platform that needs great effort to deal with the programming manner's complexity [39].

- Generic frameworkhas been proposed by [4] supported by a three-level data management model composed of dew computing, fog computing, and cloud computing for efficient data flow in IoT-based home care systems. We examine the proposed model through a real case scenario of an early fire detection system using a distributed fuzzy logic approach[40].

- An approach to incorporate strong security in deploying the Internet of Things (IoT) is presented by [41] for a smart home system, together with due consideration given to user convenience in operating the system. The IoT smart home system runs on a conventional wifi network implemented based on the AllJoyn framework, using an asymmetric Elliptic Curve Cryptography to perform the authentications during system operation. A wifi gateway is used as the center node of the system to perform the system initial configuration. It is then responsible for authenticating the communication between the IoT devices and providing a means for the user to setup, access, and control the system through an Android-based mobile device running appropriate application program[41].

- Secure IoT-based smart home automation system has been developed by [42]. To facilitate energy-efficient data encryption, a method, namely Triangle Based Security Algorithm (TBSA) based on an efficient key generation mechanism was proposed. The proposed TBSA in integrating the low power Wi-Fi was included in WSNs with the Internet to develop a novel IoT-based smart home that could provide secure data transmission among several associated sensor nodes in the network over a long converge range[42].

- Choi et al. [43] is offer The firmware validation and update scheme. performs based authentication between devices in a smart home environment and uses the key derivation algorithm for firmware image distribution. To verify the integrity of the firmware image, it uses a hash chain. The firmware image is used as an input of the hash chain and is fragmented. The scheme transmits the pieces fragmented by firmware fragmentation and put the transmitted pieces into the hash chain for verification.

- By Lee et al. [44] proposes user privacy-enhanced security architecture applied in a smart home environment. The architecture has a defense against such attacks as personal information hijacking and burst attacks between an attacker and devices in a smart home environment. The study proposed a security framework applicable to a smart home environment, including encryption, access control, digital signature, authentication, and logging.

- Abdallah et al. proposd The lightweight lattice-based homomorphic privacy-preserving aggregation scheme [45] uses the authentication process of smart devices and lightweight lattice-based homomorphic cryptosystem to encrypt a message. It is divided into initialization phase and the reading aggregation phase. Since the scheme makes it possible to monitor authentication between smart devices,

control center, smart meters, and communication between APs, the control center can decrypt an encrypted message to improve confidentiality and privacy of devices.

- Framework based on the open source framework 'AllJoyn' was proposed by Tomanek et al. [46 . It is comprised of device, AllJoyn Core, permission module, and ACLs and policy certificate trust anchor. In the framework, critical data are transmitted after authentication between devices. End-user's security manager provides security provisioning and maintenance service for devices. A session is established between the applications of devices for data transmission. Authentication is performed with the use of a group key and a certificate. Authenticated devices transmit the messages encrypted with a given policy.

- To authenticate smartphones and send messages safely in a smart home environment, Mantoro et al. [47] uses an encryption algorithm and a hash function. The algorithm applies AES256, ephemeral Diffie-Hellman key exchange, and RC4-based hash function. With the use of a central hub, all messages to transmit are monitored, and the messages sent by smartphones pass the central hub for transmission. A message to share is encrypted with three algorithms, and a hash value is generated.

In this paper, we proposed a new framework according to the identified needs for use in smart home application. This framework complements the reference architecture's security components and is proposed with a security enhancement approach in smart home applications. Examining existing research, we find that previous research has specifically addressed topics such as the smart home, the Internet of Things, and their security. While current research has provided a specific security framework with an IoT-based smart home approach, using a reference architecture.

IX. Conclusions and Suggestions

The purpose of this study was to provide a security framework by modifying and adding the necessary components to the existing security framework of the IoT-A reference architecture for increased security in IoT-based smart homes. The addition of context management to the security framework components contributes to identifying and collecting data from smart resources and objects and information about smart home communication protocols. In the proposed framework, various alterations have been applied to controlling evaluation and licensing task, the anticipated result of which is the optimal operation of this mechanism in a distributed manner using field management. The vulnerability and threat management component is also embedded in the framework, posing as a step towards a centralized security management. Based on previous research and comparisons and evaluations tables in this study, the proposed model is theoretically able to meet the security needs of the IoT-A-based smart home

The review performed before this research indicate a significant lack of standard and typical architecture for this technology. Considering the breadth of activities and studies on proposing novel methods or standardization in this field, more comprehensive study projects are highly recommended. The component of identity management and authentication is implemented in the framework provided using the reference architecture's mechanisms. Due to the emergence of cloud mechanisms and their ever-increasing deployment in this field, it is suggested to use cloud identity management or identity as a service to focus on management and improve security in this field and reduce costs.

References

[1] J. Zheng, C. D. S. R. Bisdikian, and H. Mouftah, "The internet of Things," IEEE Commun. Mag., vol. 49, no. 11, pp. 30-31, 2011.
[2] T. Fan, and Y. Chen, "A scheme of data management in the Internet of Things," in 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, IEEE, 2010, pp. 110-114.
[3] Y. Yu, J. Wang, and G. Zhou, "The exploration in the education of professionals in applied internet of things engineering," in 2010 4th International Conference on Distance Learning and Education, IEEE, 2010, pp. 74-77.
[4] Y. Huang, and G. Li, "Descriptive models for Internet of Things," in Intelligent Control and Information Processing (ICICIP), 2010 International Conference on, 2010.
[5] K. Ashton, "That 'internet of things' thing," RFID J., vol. 22, no. 7, pp. 97-114, 2009.
[6] G. T. Ferguson, "Have your objects call my objects," Harv. Bus. Rev., vol. 80, no. 6, pp. 138-144, 2002.
[7] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787-2805, 2010.
[8] G. Lawton, "Machine-to-machine technology gears up for growth," Computer, vol. 9, pp. 12-15, 2004.
[9] Gandomi, and M. Haider, "Beyond the hype: Big data concepts, methods, and analytics," Int. J. Inf. Manag., vol. 35, no. 2, pp. 137-144, 2015.
[10] S. Zhang, S. Zhang, X. Chen, and X. Huo, "Cloud computing research and development trend," in Paper presented at the Future Networks. ICFN'10. Second International Conference on., 2010.
[11] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Commun. Surv. Tutor., vol. 17, no. 4, pp. 2374-2376, 2015.
[12] S. Pirbhulal, O.W. Amuel, W. Wu, A.K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," Future Gener Comput Syst., vol. 95, pp. 382-391, 2019.
[13] Vinodhan, and A. Vinnarasi, "IOT Based Smart Home," Int. J. Innov. Res. Sci. Eng. Technol., vol. 5, pp. 35-38, 2016.
[14] M. O'Neill, "Insecurity by design: Today's IoT device security problem," Engin., vol. 21, no. 1, pp. 48-49, 2016.
[15] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Netw., vol. 20, no. 8, pp. 2481-2501, 2014.
[16] Nimmermark, and A. Larsson, "Comparison of IoT frameworks for the smart home," MSc thesis, Department of Electrical and Information Technology, Faculty of Engineering, LTH, Lund University, 2016.
[17] Lobaccaro, S. Carlucci, and E. Löfström, "A review of systems and technologies for smart homes and smart grids," Energies, vol. 9, no. 5, p. 348, 2016.
[18] K. Jonnalagadda, "Secure Communication Scheme in Smart Home Environment," MSc thesis, University of South Florida, 2016.
[19] F. Johari, The security of communication protocols used for Internet of Things, LU-CS-EX 2015-42, 2015.

[20] F. Kausar, E. Al Eisa, and I. Bakhsh, "Intelligent home monitoring using RSSI in wireless sensor networks," Int. J. Comput. Net. Communicat., vol. 4, no. 6, p. 33, 2012.
[21] S. Marzano, The new everyday: Views on ambient intelligence, 010 Publishers., 2003.
[22] A. Saad al-sumaiti, M. H. Ahmed, and M. M. Salama, "Smart home activities: A literature review," Electr Pow. Compo. Sys. vol. 42, no. 3-4, pp. 294-305, 2014.
[23] W. Granzer, W. Kastner, G. Neugschwandtner, and F. Praus, A modular architecture for building automation systems, na, 2006.
[24] M. A. Al-Qutayri, and J. S. Jeedella, "Integrated wireless technologies for smart homes applications," in Smart Home Systems, Intech Open, 2010.
[25] Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model for Cloud. International Journal Of Computers & Technology, 10(1), 1186-1191.
[26] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security Challenges in the IP-based Internet of Things," Wirel. Pers. Commun., vol. 61, no. 3, pp. 527-542, 2011.
[27] Gan, Z. Lu, and J. Jiang, "Internet of things security analysis," in 2011 international conference on internet technology and applications, IEEE, 2011, pp. 1-4.
[28] M. Katagi, and S. Moriai, Lightweight cryptography for the internet of things, Sony Corporation, 2008, pp. 7-10.
[29] Duan, Weihua, Rouhollah Nasiri, and Sasan Karamizadeh. "Smart City Concepts and Dimensions." In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City, pp. 488-492. 2019.
[30] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 9, pp. 51-58, 2011.
[31] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with china perspective," IEEE Internet Things J., vol. 1, no. 4, pp. 349-359, 2014.
[32] FhG, S. H. SAP, E. H. HSG, C. Jardak, A. O. CEA, A. Serbanati, and J. W. Walewski, Internet of things-architecture iot-a deliverable d1. 3–updated reference model for iot v1. 5, 2012.
[33] A. Torkaman, and M. A. Seyyedi, "Analyzing IoT reference architecture models," Int. J. Comput. Sci. Software Engin., vol. 5, no. 8, p. 154, 2016.
[34] M. M. Hossain, M. Fotouhi, R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in 2015 IEEE World Congress on Services, IEEE, 2015, pp. 21-28.
[35] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, A. Iera, "A systemic and cognitive approach for IoT security," in 2014 International Conference on Computing, Networking and Communications (ICNC), IEEE, 2014, pp. 183-188.
[36] A. Lee, L. Zappaterra, K. Choi, H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in 2014 IEEE Conference on Communications and Network Security, IEEE, 2014, pp. 67-72.
[37] L. Hernández-Ramos, M. V. Moreno, J. B. Bernabé, D. G. Carrillo, and A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings," J. Comput. Syst. Sci., vol. 81, no. 8, pp. 1452-1463, 2015.
[38] N. Miloslavskaya, and A. Tolstoy, "New SIEM System for the Internet of Things," in In World Conference on Information Systems and Technologies, Springer, Cham. April., 2019, pp. 317-327.
[39] Alani, S., Mahmood, S. N., Attaallah, S. Z., Mhmood, H. S., Khudhur, Z. A., & Dhannoon, A. A. (2021). IoT based implemented comparison analysis of two well-known network platforms for smart home automation. International Journal of Electrical & Computer Engineering (2088-8708), 11(1).
[40] Risteska Stojkoska, B., Trivodaliev, K., & Davcev, D. (2017). Internet of things framework for home care systems. Wireless Communications and Mobile Computing, 2017.
[41] Santoso, F. K., & Vun, N. C. (2015, June). Securing IoT for smart home system. In 2015 international symposium on consumer electronics (ISCE) (pp. 1-2). IEEE.
[42] Pirbhulal, S., Zhang, H., E Alahi, M. E., Ghayvat, H., Mukhopadhyay, S. C., Zhang, Y. T., & Wu, W. (2017). A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors, 17(1), 69.
[43] Choi, B. C., Lee, S. H., Na, J. C., & Lee, J. H. (2016). Secure firmware validation and update for consumer devices in home networking. IEEE Transactions on Consumer Electronics, 62(1), 39-44.
[44] Lee, S., Kim, J., & Shon, T. (2016). User privacy-enhanced security architecture for home area network of Smartgrid. Multimedia Tools and Applications, 75(20), 12749-12764.
[45] Tomanek, O., & Kencl, L. (2016, June). Security and privacy of using AllJoyn IoT framework at home and beyond. In 2016 2nd international conference on intelligent green building and smart grid (IGBSG) (pp. 1-6). IEEE.
[46] Abdallah, A., & Shen, X. S. (2016). A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid. IEEE Transactions on Smart Grid, 9(1), 396-405.
[47] Mantoro, T., Ayu, M. A., & binti Mahmod, S. M. (2014, April). Securing the authentication and message integrity for Smart Home using smart phone. In 2014 International Conference on Multimedia Computing and Systems (ICMCS) (pp. 985-989). IEEE.

Shahrouz Sotoudeh received his master's degree in Information Technology Engineering at Shiraz University in 2017. He also completed his bachelor's degree in Software Engineering at the same university. His field of research and expertise is networking, security and the Internet of Things; he is currently head of the networking and security team at ICT Research Institute.

Sattar Hashemi received Ph.D. in Artificial Intelligence at Iran University of Science and Technology (IUST) in conjunction with Monash University, Australia and M.Sc. degree in Artificial Intelligence and Robotics from IUST, and a bachelor degree in Computer Hardware Engineering at Isfahan University. He is Professor of Artificial Intelligence & Machine Learning at Shiraz University, Iran. He has excellent field experience and research, including Machine Learning, Data Sciences & Network Security.

Hossein Gharaee received B.Sc. degree in Electrical Engineering from K.N. Toosi University, of Technologhy in 1998, M.Sc. and Ph.D. degree in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2000 and 2009 respectively. Since 2009, he has been with the Department of Network Technology in ICT Research Institute (ITRC). His research interests include VLSI with emphasis on basic logic circuits for low-voltage low-power applications, DSP, crypto chip and Intrusion detection and prevention systems.