Implementation of A Zero-Trust Approach in Smart Home Among the Houseowners in Kota Kinabalu, Sabah

Andrew Johanes[a], Nabilah Filzah Mohd Radzuan*[a], Zuraini Hayati Abdullah[a]

[a] *Centre for Emerging Technologies in Computing (CETC), Faculty of Information Technology, INTI International University*

Abstract

As smart home technology is becoming pervasive, smart home automation devices are increasingly being used by many users including those non-technical who may have little understanding of the technology or knowledge to properly mitigate privacy and security risks. However, smart home development and adoption is still a new phenomenon and trend and also relatively limited in Malaysia. Smart home technologies become easier in monitoring home and control access for the homeowners from anywhere and anytime with connecting to the Internet of Things (IoT) principle. Therefore, the purpose of this study is to identify the issue of smart home and zero-trust approach in IoT integration, to develop interface modules to communicate with sensor and actuators that use wireless technology and to examine the prospective user perceives the specific benefits of Zero-trust in current smart home technology. This is a quantitative study and involves a small number of respondents among smart homeowners in Kota Kinabalu, Sabah. Quantitative data will be analyzed by using the IBM SPSS version 22. While the qualitative data gathered from the respective respondents, then the data were transcribed into text for the data analysis stage and the analysis was conducted by using thematic analysis. This paper proposes an implementation of a zero-trust approach in a security system of smart homes to further increase the security of the system for the smart home network. This research review will analyze smart home approaches, challenges, and the suggestion of using the zero-trust approach as a possible solution and illustrate open issues that still need to be addressed.

Keywords: *zero-trust, smart home, houseowner, IoT*

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

INTRODUCTION

As smart home technology is becoming pervasive, smart home automation devices are increasingly being used by many users including those non-technical who may have little understanding of the technology or knowledge to properly mitigate privacy and security risks. However, smart home development and adoption is still a new phenomenon and trend and also relatively limited in Malaysia, let alone in Sabah.

Smart home technologies become easier in monitoring home and control access for the homeowners from anywhere and anytime with connecting to the Internet of Things (IoT) principle. Therefore, the purpose of this study is to identify the issue of smart home and zero-trust approach in IoT integration, to develop interface modules to communicate with sensor and actuators that use wireless technology and to examine the prospective user perceives the specific benefits of Zero-trust in current smart home technology.

This is a quantitative study and involves a small number of respondents among smart homeowners in Kota Kinabalu, Sabah. Quantitative data will be analyzed by using the IBM SPSS version 22. While the qualitative data gathered from the respective respondents, then the data were transcribed into text for the data analysis stage and the analysis was conducted by using thematic analysis. This paper proposes an implementation of a zero-trust approach in a security system of smart homes to further increase the security of the system for the smart home network, and the suggestion of using the zero-trust approach as a possible solution and illustrate open issues that still need to be addressed.

Problem Statement

Smart home system faces a lot of challenges when it comes to the security of the system to the outside world and thus making some customer relucted to transition to the smart home and go back to the traditional was using a lock and key security style.mPast studies in Malaysia have found that Malaysians are reluctant to adopt the concept of smart homes and the Internet of Things (IoT), even though they agree on the importance of a home that is safe and can be monitored remotely. There were cases where potential

[*] Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

home buyers who are unaware of the existence of smart home technology, thus hinder its adoption and further development (Rasyidah, et al., 2019)

The design of a smart home depends on the needs and lifestyle of the user. In general smart homes offer comfort, security, remote control and even energy savings (Muhammad Raisul Alam., et al., 2012). Nevertheless, smart homeowners face some ethical issues related to user privacy. Smart homes need to take into account customer satisfaction, especially when it comes to data and also the personal lives of users of smart home technology. More research needs to be done especially from the aspects of lifestyle, satisfaction, needs, consumer adaptation to smart home technology. Smart home technology networks need to optimize the connection of appliances in the home using different media and protocols. Algorithms and data processing methods can support the introduction and development of smart home technology services (Muhammad Raisul Alam., et al., 2012).

The purpose of the algorithm is to provide intelligence to create an interactive home environment. Location-detection algorithms are derived to gather information about user location-based activities (Gopalratnam & Cook, 2007). Instead of aiding people in household tasks, the algorithms implemented may irritate the user, thus alienating people from this technology. Although researchers are using various algorithms and methods for smart homes, smart homes are still partially dependent on human interaction for accurate decision making. Apart from that, the algorithm used is supposed to facilitate and help users, but there are issues where it becomes a confusing distraction, causing some users who are less proficient with the technology refuse to use it. Past research has shown that there are various algorithms used in smart homes yet ultimately smart home technology still relies on human interaction in making the right decisions (Yamazaki, 2006).

Due to the issues discussed above then the researcher is interested to make a study on the issues related to a smart home network and Zero-trust in the integration of the Internet of Things (IoT). Apart from that the researcher also wanted to get the perspective of smart home technology users on the specific benefits of zero-trust in current smart home technology. And finally, develop to develop interface modules to

[*]Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

communicate with sensors and actuators that use wireless technology. To overcome this and gain the trust of the user for using smart house is the way forward in making the house secure is the implementation of Zero-trust algorithm in the smart home network.

Project Objective

RO1: to determine the issue on smart home and Zero-trust network in IoT integration.
RO2: to identify the prospective user perceives the specific benefits of Zero-trust in current smart home technology.
RO3: to develop interface modules to communicate with sensor and actuators that use wireless technology.

Project Question

RQ1: What is the issue on smart home and Zero-trust network in IoT integration?
RQ2: What is the prospective user perceives the specific benefits of Zero-trust in current smart home technology?
RQ3: How to develop interface modules to communicate with sensor and actuators that use wireless technology?

Project Scope

Limitations are elements outside researcher control and cannot do in this study and delimitations are elements outside of the boundary's researcher have set and will not do. In this context of the study, the targeted respondents are only those smart home house owners in Kota Kinabalu, Sabah. This is because not many houses fitted with smart home and researcher need respondents with knowledge of smart home technology.

This study also aims to get feedback on the issue of smart home and zero-trust network in IoT integration among respondents and perceptions of smart homeowners about the specific benefits of zero trust in current smart home technology. And last but not least is to develop interface modules to communicate with sensor and actuators that use wireless technology.

[*]Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Target Audience

The target audience would be the Smart home houseowners in Kota Kinabalu Sabah. Due to the high price of smart home installation, only homeowners from the upper M40 and T20 groups can afford to own smart homes. The estimated minimum price for a home fitted with a basic smart home system can reach RM30,000 (Smartruma, 2021; Smart zone, 2021). For that reason, a small survey study will be conducted on smart homeowners in Kota Kinabalu with an expected 50 respondents as a sample. Sample size needed to make inferences about the population. Some researchers do, however, support a rule of thumb when using the sample size, many researchers say that there should be at least 10 observations per variable, and for three independent variables, then a clear rule would be to have a minimum sample size of 30 (Statistic Solution, 2021). Some researchers usually follow statistical formulas to calculate the sample size. With that believe, the researcher will choose a small number of respondents to admin the questionnaire to get their response.

LITERATURE REVIEW

In Malaysia's context, the market for the smart home will be widespread and it is predicted to exceed US$ 235 Million by the year 2025. There is a high demand in the Malaysian market for a more safe and secure living environment, especially the safety functionalities and discrete monitoring of security purposes. The smart home market in Malaysia has significantly advanced with the growth of the IoT market, reduction cost measures enabled by home automation systems, manufacturers expanding their product portfolios, and the importance of home monitoring from far away location. The increasing demand for smart home devices, security and privacy breach will also increase as many of the house appliances is controlled by technology. The issues about privacy and security breach are restraining the growth of the smart home market.

In recent years, the concept of smart homes has become one of the reflections of future life in the housing sector. The built house is equipped with smart home technology that allows the exchange of information between users and the building in real-time by connecting and coordinating all devices installed in the system. The Smart Home Concept is very closely related to energy efficiency and security in buildings (Nasrul Arif Ahmad Mahmud., et al., 2020).

[*]Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Smart home technology is generally devices, appliances, or systems that are connected to a network that can be independently and remotely controlled. The smart home is where the home setup is suitable to use appliance and devices that can be controlled automatically from a distance with a connection to the internet using our mobile devices. A device connected through the internet and can regulate functions such as security access to the house, temperature, lighting, and home theatre are usually the main base for a smart house for the customer.

Smart home technology connects sensors, devices, and appliances through a communication network to monitor, access, and operate the home environment remotely. In addition, these smart home systems also provide services that meet the needs of users using websites to provide remote service access. Using web services is the most open and interoperable way to provide remote service access or allow applications to communicate with each other. Internet of Thing (IoT) is classified as a system that can be used as connectors such as internet television, sensors and movers to the internet to any device intelligently linked to forming a new communication among users (Fabi, et al., 2017).

The system is the integration of housing automation and services through a home network to enable a better quality of life. Recently, there are so many technologies related to Smart Home Concept has emerged which help occupants to be more connected and more control towards their own home. The term 'Smart' and 'Intelligent' is related to home control that often referred to the home energy management system (HEMS) which is used by the adaptation of Smart Home System (Nacer, et al., 2017).

Based on the literature review there are a few benefits of Smart home automation such as;

a. Manage all devices connected from a one-stop centre, so that all technologies at home connected through one interface (Bahshm & Aldhaibani, 2020) .

b. Smart home systems are more flexible for new devices and appliances.

[*] Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

c. Incorporate security and surveillance features in smart home networks to maximize home security (Horwitz, 2020).

d. The function of home appliances can be controlled remotely (Bahshm & Aldhaibani, 2020).

e. Increased energy efficiency to make space more energy-efficient (Robles & Kim, 2010).

f. Enhance the appliance function (Nasrul Arif Ahmad Mahmud., et al., 2020).

g. Home management insights to analyse daily habits and behaviours and to adjust live the desired lifestyle (Jabbar, et al., 2018).

Security Goal of Smart Home

However, due to its internet-connected, dynamic, and heterogeneous nature, a smart home creates new security issues and challenges. The literature review describes five of the most important security goals of the smart home such as:

a. Authentication: the verification about communicating parties or user, who is using and what he claimed, what data send by claim author and message sent.

b. Authorization: it is to ensure that every user access right is defined for the system's resources utilization (Horwitz, 2020).

c. Confidentiality: ensures that only authorized users can access the private data withina system (Nacer, et al., 2017).

d. Integration: the assurance that data is maintained inconsistency and in an accurate way. Modification and losses of data will be under notice (Schiefer, 2015).

e. Availability: assure that for any authorized user, all services will always be available, and these resources are protected against any type of threat (Ali, et al., 2017)

Security Challenge in Smart Home

Although smart home in use is convenient and able to controls all home appliances but smart home has challenges in security issues. This is due to the nature of the smart home environment that is always connected to the outside world through the internet has opened security back doors and this has raised many security concerns among smart homeowners (Mantas, et al., 2010). Internet communication may threaten system security due to the increasing order of cyber-attacks. In this case, there is data exchange among the home appliances and the smartphone, so user information and confidentiality

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

will be transmitted via the Internet, a thing that defines a threat to the privacy of the user (Mantas, et al., 2010; Ali, et al., 2017; Tanwar, et al., 2017; Karimi & Krit, 2019). Some of the threats identified in this study are.

a. Confidential Data leakage. By using smartphone apps, users exchange data with home devices In the case of an unsecured mechanism, it is may cause a data leakage inthe network that increases the cybersecurity threats (Ali, et al., 2017; Asmah Laili Yeon., et al., 2018; Karimi & Krit, 2019).
b. Denial Of Service (DoS). Denial of service (DoS) and Distributed Denial of service (DDoS) attack are used to deny system availability and communication resources (Karimi & Krit, 2019).
c. Malicious codes injection. Malicious codes are scripts (software programmed) that can be injected into the smart home apps and allow attackers to exploit the system's vulnerability and manages authorization by allowing access for unauthorized entities to the system (Karimi & Krit, 2019).
d. Eavesdropping Attack. Eavesdropping attack also called sniffing attack is realtime getting information that smart home devices, microcontroller and smartphone transmit through a network (Bluetooth, WSNs, etc.). This attack allows hackers to intercept user privacy and data confidentiality by sniffing data exchanged. It aims to steal transmit data over the network without disturbing the transmission process which makes the detection of these types of attacks being difficult (Ali, et al., 2017; Ng, et al., 2019).

The findings of Wilson, et al., 2017, reported that homeowners in the UK (n = 1025) showed a positive perception of various functions of smart home technology including energy management. However, the study report also states that the measures to convince users on security and data storage are not very convincing for smart homeowners.

Zero-Trust Approach

Smart home helps to automate the house by making it smart and interconnected. However, at the same time, it raises a great concern of the privacy and security for the users due to its capability to be controlled remotely. With this, our house can be targeted with hacks for other people to gain access to our house because the way security for smart housework is as long as the person can gain the access code, they can enter

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

without validating the device used to gain access with, thus implementing Zero-trusts into the network will help a lot in making our smart house more secure and well protected. The implementation of the Zero-trust approach in the smart house system where it functions by verifying the user, the user device and cross-reference them to a database that is stored in a server for the system to make sure that the user and their devices used to access the house is a registered one in the database (Rose, et al., 2019).

Zero-trust is a network security model, based on a strict identity verification process. The framework dictates that only authenticated and authorized users and devices can access applications and data. At the same time, it protects those applications and users from advanced threats on the Internet. Zero-trust Model ensures each node is responsible for the approval of the transaction before it gets committed. The data owners can track their data while it is shared amongst the various data custodians ensuring data security (Campbell, 2020). The consensus algorithm enables the users to trust the network as malicious nodes fail to get approval from all nodes, thereby causing the transaction to be aborted. In conclusion, Zero-trust is a systemic approach to information security that trusts no user, transaction, or network traffic unless verified (Campbell, 2020).

Security benefits of zero-trust. The zero-trust approach to security is widely regarded as best practice by analysts and governments. The Zero-trust model centres on the concept that users inside a network are no more trustworthy than users outside a network (Barry Scott., 2018). To make it a reality, organisations must focus on four key areas: verifying the user; verifying the device; restricting access and privilege; and ensuring that systems are intelligent enough to learn and adapt over time. In practice, this translates to using multi-factor authentication (MFA) everywhere; extending identity controls to the endpoint via a risk score-based system; enforcing privileged access management, and behavioural analytics to constantly update those risk scores. Zero-trust policies help prevent successful data breaches by eliminating unauthorized access to networks. A zero-trust security policy thus requires that devices and users wanting access to the network must always verify their identity. This principle of “Never trust; always verify” enables security administrators to constantly verify the nature of an IoT device before it accesses a network (Horwitz, 2020).

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Meanwhile, the Zero-trust architecture strategy does not show the implied trust found in the system based on physical location or network (local area networks versus the Internet). Authentication (users and devices) is performed before a connection is made and access to the data source is granted when the source is required. Zero-trust architecture is a response to enterprise network trends that include remote users and cloud-based assets that are not located within an enterprise-owned network boundary. It emphasizes resource protection because a network location is not a key component of resource security (Rose, et al., 2019).

Zero-Trust Towards Smart Home

Stand-alone smart home - An isolated application that does not necessarily use a central control unit, serves a single purpose, and can be directly controlled (via a router) from a smart device. Included are all smart homes that use devices from only one segment. The proposed system requires two components and one of them is a server to store the data of the component ID and the registered ID of the user to access the Smart Home, to manage, control, and monitor the user's home activity. The administrator of this system can be locally and remotely control and manage the system. There will be a hardware interface that provides the sensors and actuator to automate the home through the application. The proposed system will advance with the implementation of the Zero-trust approach where it will verify every user, validate their device, and limit the access of the user that is not given a time-limited code to enter the house.

In this study, researchers explore the concept of security in Zero Trust applications as a security measure in IoT networks (Samaniego & Deters, 2018). The idea of zero trust is based on network segmentation and the network concept of 'micro cores and perimeters' (Kindervag, 2010). In a typical Information Technology network, .defies the concept of a trusted domain and champions the "never trust, always verify" principle (Samaniego and Deters 2018). IoT networks extend beyond the perimeter of the organization. This makes Zero Trust an ideal way to provide security to IoT networks. Zero Trust is a comprehensive approach to securing access across your networks, applications, and infrastructure (including access from users, computers,

[*]Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

phones, IoT devices, cloud applications). The Zero Trust architecture eliminates the idea of trusted/untrusted devices, network, and users (Kindervag, 2010).

Zero Trust Concepts

Zero trust is not a product but a systematic approach to information security that does not trust any user, transaction or network stream unless it has been verified. Zero Trust ensures that access is granted not only on the perimeter but at every layer, network, application and data access point (Samaniego & Deters, 2018; Suparna Dhar. & Indramil Bose., 2020). No one has trusted whether it is an insider or an outsider. Zero Trust is characterized by segmented, parallelized, and centralized network. It is based on three key concepts that empower secure networking:

a. Easy to manage segmented networks: Zero Trust recommends new ways of segmenting networks by addressing segmentation at the core of the network.
b. Built with multiple parallel switching cores: Zero Trust recommends distributed processing by breaking the core switch into multiple smaller and less expensive cores. By using the concept of parallelization, Zero Trust segregates network traffic into smaller network segments.
c. Centrally managed from a single console: Central management of all networking elements is a key feature of Zero Trust. It recommends a platform to centrally manage the network components and segment network traffic (Suparna Dhar. & Indramil Bose., 2020).

Zero Trust System Design

In the Zero Trust architecture, all network traffic is untrusted irrespective of the source (Samaniego & Deters, 2018). Zero Trust covers security rules for seven stacks – networks, devices, data, people, workloads, automation and orchestration, and visibility and analytics (Checkpoint, 2019). It applies security protocols and policies on all network entities to secure all resources, limits and enforces access control, and inspects and logs network traffic (Kindervag, 2010). This reduces the threat of abuse and misuse of data and the network from entities within and outside the network.

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Zero Trust Components

Zero Trust network architecture professes explicit security as a part of a layered, defence-in-depth approach. This eliminates single points of failure and security compromise. The key concepts and components of the Zero Trust architecture are as follows;

a. Segmentation Gateway (SG) forms the nucleus of the network in Zero Trust. The SG provides all security functions (firewall, network access control, data loss prevention, intrusion prevention, intrusion detection, VPN gateway, and others). It implements all global network and security policies. The SG segregates network traffic to secure and parallel network segments. Segmentation improves management visibility and allows early detection and containment of security incidents.

b. Microcore and perimeter (MCAP) offers fine gained parallel segmentation and isolation of critical network resources. MCAP has a microcore switch that connects to the SG. The network segment, managed by the microcore switch, becomes the microperimeter. Network resources in each microcore share the same set of functionalities and network policy attributes.

c. Centralized unified and transparent management of the MCAPs is a key feature of Zero Trust. In effect, Zero Trust shifts the paradigm of network management from managing network components individually to a centralized network management system.

The propose of a Zero-trust Smart home shown in Figure 2.1

[*]Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

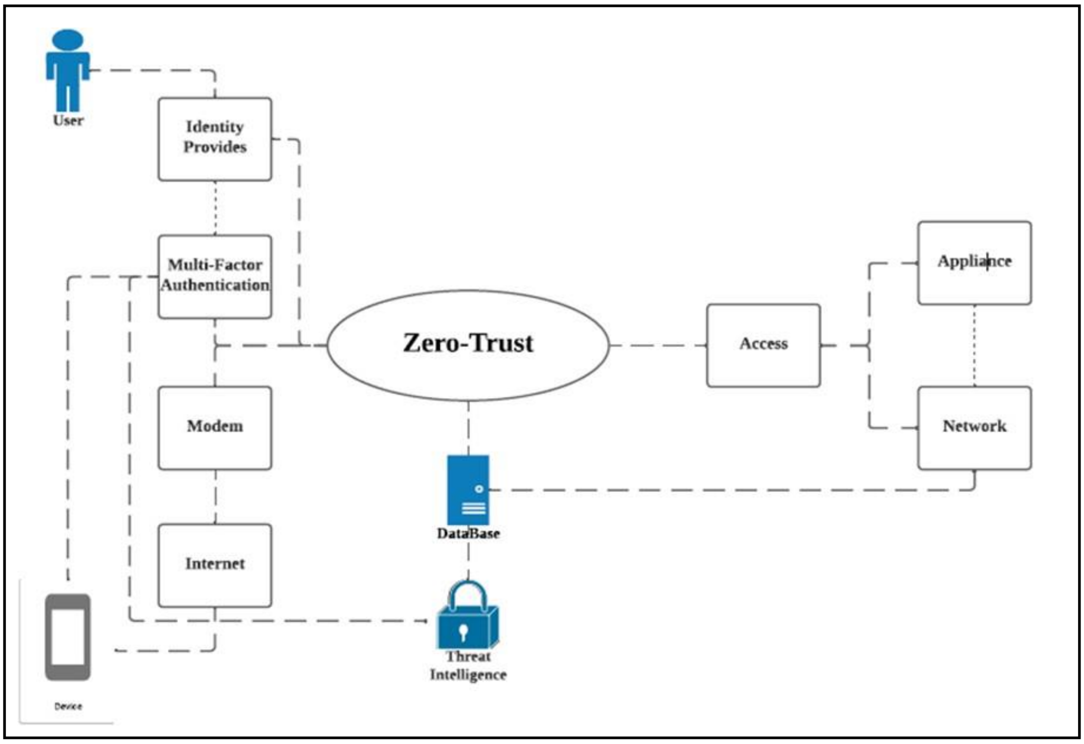

Figure 2.1: The Proposed Zero-trust Smart home

Result and Discussion

Zero trust security is an IT security model that requires strict identity verification for every person and device trying to access resources on a private network, regardless of whether they are sitting within or outside of the network perimeter. No single specific technology is associated with zero trust architecture; it is a holistic approach to network security that incorporates several different principles and technologies. Due to that, researcher intend to develop interface modules to communicate between sensor and actuators that use wireless technology to overcome all the issue discussed earlier.

The first main function is that the user will provide identity to the system by login into their account and will through multi-factor authentication to authenticate the users account from the database. As for the device side, it will connect through the internet and goes through the modem and will also pass through the multi-factor authenticate to the database to find the device and the user that it is registered too and this is the common way for a smart home security system, but with Zero-Trust this will act as a secondary authentication before giving the user access to the smart home system. Zero-Trust will authenticate not only the user's account but also the user devices where every

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

device has a special model number only specific to that specific device not counting the model of the device.

Depicts the integrating of the Smart Home, IoT and Zero-Trust main components and their interconnectivity. This enables communication among the devices and outside of it. Connected to the LAN are a server and its database. The server controls the devices, logs their activities, provides reports, answers queries and executes the appropriate commands. In addition, IoT home appliances are connected to the internet and to the LAN, and so expands smart homes to include IoT and zero trusts. The connection to the internet allows the end-user, resident, to communicate with the smart home to get current information and remotely activate tasks with peace of mind because of the zero trusts in it.

Summary

In conclusion, the problems faced by smart home technology users have led to this study to enable the identification of real issues faced by smart homeowners, as well as to get the perspective of smart home technology users on the benefits of zero-trust security. Meanwhile, the choice of zero-trust security is due to the projected size of the global zero-trust security market which increased so much especially during the pandemic and post-Covid-19 period.

It is reported that the global market size of zero-trust security had increased from USD 19.2 billion in 2020 to USD 51.6 billion in 2026. It recorded a compound annual growth rate (CAGR) of 17.4% from 2020 to 2026. The major factors driving the market include the growing frequency of target-based cyberattacks and increasing regulations for data protection and information security (Markets & Markets, 2021). An overview of the installation of smart home technology, consumer perceptions and their willingness to accept this technology. In addition, this chapter also discusses the advantages of zero trust integration in smart home technology, concepts, components and also smart home design systems as an initial preparation before the implementation of actual research.

REFERENCES

Ali, W., Dustgeer, G., Awais, M. & Shah, M., 2017. *IoT based smart home: Security challenges requirements and solution.*. Huddersfield, University of Huddersfield, pp. 1-6.

Asmah Laili Yeon., et al., 2018. Smart Home Users Perception on Sustainable Urban Living and Legal Challenges in Malaysia. *The Journal of Social Science Research,* Issue 6, pp. 807-814.

Bahshm, Y. & Aldhaibani, A., 2020. Designing a Smart Home Automation System Using Internet of Things and Mobile Application. *Journal of Network Communications and Emerging Technologies (JNCET),* 10(3), pp. 1 - 5.

Barry Scott., 2018. *Network Security.* s.l.:s.n.

Campbell, M., 2020. *Beyond Zero Trust: Trust is a Vulnerability.* 0 ed. s.l.:IEEE Computer Society.

Checkpoint, 2019. *The Ultimate Guide to Zero Trust Security.* [Online] Available at: https://resources.checkpoint.com/ [Accessed 20 March 2021].

Fabi, V., Spigliantini, G. & Corgnati, S., 2017. *Insights on Smart Home Concept and Occupants' Interaction with Building Controls.* s.l., Energy Procedia, pp. 759-769.

Gopalratnam, K. & Cook, D. J., 2007. Online Sequential Prediction via Incremental Parsing: The Active LeZi Algorithm. *IEEE Intell. Sys.,* Volume 22, pp. 62-58.

Horwitz, L., 2020. *IoT World Today.* [Online] [Accessed 22 February 2021].

Jabbar, W., Alsibai, M., Amran, N. & Mahayadin, S., 2018. *Design and Implementation of IoT-Based Automation System for Smaart Home.* s.l., s.n.

Karimi, K. & Krit, S., 2019. *Smart Home-Smartphone Systems: Threats, Security Requirements and Open Research Challenges.* s.l., s.n.

Kindervag, J., 2010. *Build Security into your Network's: The Zero Trust Netwoek Architecture.* [Online] Available at: http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf [Accessed 19 March 2021].

Mantas, G., Lymperopoulos, D. & Komninos, N., 2010. Security in Smart Home Enviroment. In: A. S. K. &. I. K. Lazakidou, ed. *Wireless Technologies for Ambient Assisted Living and Health Care: Systems and Applications.* s.l.:Medican Information Science Reference, pp. 170-191.

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Markets & Markets, 2021. *Market Research Report: Zero Trust Security Market. Report Code: TC7384*, s.l.: Markets & Markets.

Muhammad Raisul Alam., Mamun Ibne Reaz. & Mohd Alauddin Mohd Ali., 2012. A Review of Smart Homes: Past, Present and Future. *IEEE Transactions on Systems, MAn and Cybernetics - Part C: Applications & Reviews,* 42(6), pp. 1190-1203.

Nacer, A., Marhic, B. & Delahoche, L., 2017. *Smart home, Smart HEMS anda Smart Heating: An Overview on latest Products and Trend.* s.l., s.n., pp. 90 - 95.

Nasrul Arif Ahmad Mahmud., Nurul Nabila Mohamad Yusof., Izuddinshah Abd Wahab. & Nur amalina Hanapi., 2020. *The Application of Smart Home Concept into Existing Typical Malaysian Single-storey Terrace House: Device Installation.* s.l., IOP Publishing, pp. 1 - 11.

Ng, T., Ahmad Suhaimi Baharudin., Lubna, A. H. & Mohd Faiz Hilmi., 2019. Factors Affecting User's Intention to Adopt Smart Home in Malaysia. *International Journal of Interactive Mobile Technologies (iJIM),* 13(12), pp. 39-54.

Rasyidah, Z., Hariati, A., Rosadah, M. & Maryanti, M., 2019. *Perceptions on Smart Home concept Among The Millennials in Johor.* Langkawi, IOP Publishing Ltd.

Robles, R. & Kim, T., 2010. A Review on Security in Smart Home Development. *International Journal of Advanced Science and Technology,* Volume 15, pp. 13-22.

Rose, S., Borchert, O., Mitchell, S. & Connelly, S., 2019. *Zero-trust Architure,* s.l.: Computer Security Centre.

Samaniego, M. & Deters, R., 2018. *Zero Trust Hierarachical Management in IoT.* San Francisco, CA, USA., s.n., pp. 88-95.

Schiefer, M., 2015. *Smart Home Definition and Security Threats.* s.l., s.n., pp. 114-118. Smart zone, 2021. *Smart Zone.* [Online] Available at: https://www.smartzone.info/videos-smart-home-malaysia [Accessed 25 Februari 2021].

Smartruma, 2021. [Online] Available at: https://www.smartruma.com/pages/about-us [Accessed 25 February 2021].

Statistic Solution, 2021. *Sample Size Formula.* [Online] Available at: https://www.statisticssolutions.com/sample-size-formula/ [Accessed 25 February 2012].

Suparna Dhar. & Indramil Bose., 2020. Securing IoT Devices Using Zero Tr uct and Blockchain. *Journal of Organizational Computing and Electronic Commerce,* pp. 1-17.

Tanwar, S. et al., 2017. *An Advanced Internet of Thing based Security Alert for Smart Home.* s.l., s.n.

*Corresponding author. Tel.: +6-017-5999732; Fax: +6-06-798 2000
E-mail: nabilah.radzuan@newinti.edu.my

Wilson, C., Hargreavesb, T. & Hauxwell-Baldwin, R., 2017. Benefits and risks of Smarthome Technologies. *Energy Policy, Elsevier*, Issue 103, pp. 72-83.

Yamazaki, T., 2006. *Beyond the Smart Home.* s.l., Proceedings of the International Conference on Hybrid Information Technology (ICHIT), pp. 350-355.